E 7411

ASSEMBLÉE NATIONALE

TREIZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2011-2012

Reçu à la Présidence de l'Assemblée nationale
Le 14 juin 2012

Enregistré à la Présidence du Sénat
Le 14 juin 2012

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

COM (2012) 238 FINAL

CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 7 juin 2012 (08.06)
(OR. en)

10977/12

Dossier interinstitutionnel: 2012/0146 (COD)

TELECOM 122
MI 411
DATAPROTECT 73
CODEC 1576

PROPOSITION

Origine:	Commission européenne
En date du:	5 juin 2012
N° doc. Cion:	COM(2012) 238 final
Objet:	Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

Les délégations trouveront ci-joint la proposition de la Commission transmise par lettre de M. Jordi AYET PUIGARNAU, Directeur, à Monsieur Uwe CORSEPIUS, Secrétaire général du Conseil de l'Union européenne.

p.j.: COM(2012) 238 final

COMMISSION EUROPÉENNE

Bruxelles, le 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

(Texte présentant de l'intérêt pour l'EEE)

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

Le présent exposé décrit le cadre juridique qui est proposé pour susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur.

Instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique. En effet, si les consommateurs, les entreprises et les administrations n'ont pas confiance, ils hésiteront à effectuer des transactions par voie électronique et à adopter de nouveaux services.

La *stratégie numérique pour l'Europe*[1] recense les obstacles qui s'opposent actuellement au développement numérique de l'Europe et propose une législation sur les signatures électroniques (action clé 3) et la reconnaissance mutuelle de l'identification et de l'authentification électroniques (action clé 16), en établissant un cadre juridique clair afin de remédier au cloisonnement et au manque d'interopérabilité, de développer la citoyenneté numérique et de prévenir la cybercriminalité. Une législation garantissant la reconnaissance mutuelle de l'identification et de l'authentification électroniques dans l'UE et le réexamen de la directive sur les signatures électroniques constituent aussi, dans l'*Acte pour le marché unique*[2], une action clé pour la réalisation du marché unique du numérique. Enfin, la *feuille de route pour la stabilité et la croissance*[3] souligne la fonction essentielle que le futur cadre juridique commun concernant la reconnaissance et l'acceptation mutuelles de l'identification et de l'authentification électroniques au niveau transnational aura pour le développement de l'économie numérique.

Le cadre juridique proposé, consistant en un *règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*, vise à permettre des interactions électroniques sûres et sans discontinuité entre les entreprises, les particuliers et les pouvoirs publics et à accroître ainsi l'efficacité des services en ligne publics et privés et du commerce électronique dans l'UE.

La législation de l'UE existant en la matière, à savoir la directive 1999/93/CE sur un *cadre communautaire pour les signatures électroniques*[4], ne couvre, comme son nom l'indique, que les signatures électroniques. L'UE ne dispose encore d'aucun cadre transnational et intersectoriel complet pour des transactions électroniques sûres, fiables et aisées, qui recouvre l'identification, l'authentification et les signatures électroniques.

Le but est donc d'étoffer la législation actuelle et de l'étendre à la reconnaissance et à l'acceptation mutuelles, au niveau de l'UE, des systèmes d'identification électronique notifiés et des principaux autres services de confiance électroniques qui y sont associés.

---

1 COM(2010) 245 du 19.5.2010.
2 COM(2011) 206 final du 13.4.2011.
3 COM(2011) 669 du 12.10.2011.
4 JO L 13 du 19.1.2000, p. 12.

2. RÉSULTATS DES CONSULTATIONS AVEC LES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

La présente initiative est le fruit de consultations approfondies à propos du réexamen du cadre juridique actuel sur les signatures électroniques, au cours desquelles la Commission a recueilli des informations auprès des États membres, du Parlement européen et d'autres parties prenantes[5]. Une consultation publique en ligne a été complétée par un «panel de PME» chargé de faire connaître l'avis et les besoins spécifiques des PME, et par d'autres consultations ciblées avec certaines parties prenantes[6,7]. La Commission a également entrepris un certain nombre d'études relatives à l'identification, à l'authentification, aux signatures électroniques et aux services de confiance associés (eIAS).

Les consultations ont révélé qu'une grande majorité des parties prenantes reconnaissait la nécessité de réexaminer le cadre actuel pour combler les lacunes de la directive sur les signatures électroniques. Il a été estimé que cela permettrait de mieux répondre aux problèmes posés par le développement rapide des nouvelles technologies (notamment en ligne et mobiles) et par la mondialisation accrue, tout en préservant la neutralité technologique du cadre juridique.

Conformément à sa politique tendant à «mieux légiférer», la Commission a réalisé une analyse d'impact des différentes options possibles. Trois séries d'options ont été analysées, portant respectivement sur (1) le champ d'application du nouveau cadre, (2) l'instrument juridique et (3) le niveau de contrôle requis[8]. L'option privilégiée s'est avérée être celle consistant à accroître la sécurité juridique, en coordonnant davantage les mesures nationales de contrôle et en assurant la reconnaissance et l'acceptation mutuelles des systèmes d'identification électronique, et à intégrer les principaux services de confiance qui y sont associés. Il a été conclu de l'analyse d'impact que de telles mesures permettraient de réaliser des progrès considérables en matière de sécurité juridique, de sécurité et de confiance dans le domaine des transactions électroniques transnationales, et aboutiraient à un moindre cloisonnement du marché.

---

5 Pour plus de détails sur les consultations, voir http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/index_en.htm.

6 Un atelier a été organisé le 10.3.2011, qui réunissait des représentants des secteurs public et privé et du monde universitaire afin de discuter des mesures législatives nécessaires pour relever les défis annoncés. Il s'agissait d'un forum interactif permettant d'échanger des points de vue et de marquer les différentes positions concernant les questions soulevées lors de la consultation publique. Plusieurs organismes lui ont spontanément envoyé des documents exposant leur position.

7 La présidence polonaise de l'Union a, en particulier, organisé une réunion avec les États membres à Varsovie, le 9.11.2011, sur les signatures électroniques et à Poznan, le 17.11.2011, sur l'identification électronique. Le 25.1.2012, la Commission a organisé un atelier avec les États membres pour discuter de questions en suspens en matière d'identification, d'authentification et de signatures électroniques.

8 Dans la première catégorie, quatre options ont été examinées: abroger la directive sur les signatures électroniques; maintenir le *statu quo*; accroître la sécurité juridique en coordonnant davantage les mesures nationales de contrôle et en assurant la reconnaissance et l'acceptation mutuelles de l'identification électronique dans l'UE; et étendre le champ d'application pour y intégrer certains services de confiance auxiliaires. Dans la deuxième catégorie, ont été évalués les avantages respectifs que présentent les possibilités de réglementer au moyen d'un ou de deux instruments, et d'une directive plutôt que d'un règlement. Dans la troisième catégorie, ont été examinées les possibilités offertes par la mise en œuvre de systèmes de contrôle nationaux fondés sur des exigences essentielles communes par comparaison avec un système de contrôle à l'échelle de l'UE. Chaque option a été évaluée, avec l'aide d'un groupe réunissant toutes les directions générales concernées de la Commission, du point de vue de son efficacité à atteindre les objectifs politiques fixés, de ses conséquences économiques pour les parties prenantes (y compris pour le budget des institutions de l'Union), de son impact social et environnemental et de son effet sur la charge administrative.

3. ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

3.1 Base juridique

La présente proposition se fonde sur l'article 114 du TFUE, qui a trait à l'adoption de règles pour lever les obstacles au fonctionnement du marché intérieur. Les particuliers, les entreprises et les administrations pourront bénéficier de la reconnaissance et de l'acceptation mutuelles de l'identification, de l'authentification et des signatures électroniques, ainsi que d'autres services de confiance, au niveau transnational lorsque c'est nécessaire pour entamer et mener à terme une procédure ou une transaction électronique.

Le règlement est considéré comme l'instrument juridique le plus approprié. De par son applicabilité directe, conformément à l'article 288 du TFUE, un règlement limitera le morcellement juridique et fournira une plus grande sécurité juridique en instaurant un ensemble harmonisé de règles essentielles contribuant au fonctionnement du marché intérieur.

3.2 Subsidiarité et proportionnalité

Pour qu'une action de l'UE soit justifiée, il faut que le principe de subsidiarité soit respecté.

a) Dimension transnationale du problème (critère de nécessité)

La dimension transnationale des eIAS exige une action au niveau de l'UE. Une action au niveau national seulement ne suffirait pas pour atteindre les objectifs poursuivis ni ceux fixés dans la *stratégie Europe 2020*[9]. Au contraire, l'expérience a montré que les mesures nationales ont créé, *de facto*, des obstacles à l'interopérabilité des signatures électroniques au niveau de l'UE et qu'elles produisent actuellement le même effet sur l'identification et l'authentification électroniques et les services de confiance associés. Il est donc nécessaire que l'UE établisse un cadre favorable à l'interopérabilité transnationale et améliore la coordination des systèmes nationaux de contrôle. Toutefois, l'identification électronique ne peut être abordée, dans le règlement proposé, de façon générique comme les autres services de confiance électroniques car la délivrance des moyens d'identification est une prérogative nationale. La proposition est donc axée sur les aspects strictement transnationaux de l'identification électronique.

Alors que les différences existant actuellement entre les législations nationales entraînent souvent une insécurité juridique et une charge administrative supplémentaire, le règlement proposé vise à créer des conditions de concurrence équitables pour les entreprises qui fournissent des services de confiance. La sécurité juridique est considérablement accrue dès lors que les États membres sont tenus d'accepter sans ambiguïté les services de confiance qualifiés, ce qui incitera davantage les entreprises à exercer leurs activités à l'étranger. Par exemple, il sera possible à une société établie dans un État membre de répondre par voie électronique à un appel d'offres public lancé par une administration d'un autre État membre sans craindre que sa signature électronique ne soit bloquée à cause d'exigences nationales spécifiques ou de problèmes d'interopérabilité. De même, elle pourra signer des contrats par voie électronique avec un partenaire établi dans un autre État membre sans craindre que des exigences juridiques différentes ne s'appliquent aux services de confiance, qu'il s'agisse de cachets, de documents ou d'horodatage électroniques. De plus, une mise en demeure pourra être notifiée d'un État membre à un autre avec l'assurance de sa validité juridique dans les

[9] Communication de la Commission intitulée «Europe 2020. Une stratégie pour une croissance intelligente, durable et inclusive», COM(2010) 2020 du 3.3.2010.

deux États membres. Enfin, le commerce en ligne gagnera en fiabilité dès lors que les clients auront les moyens de vérifier qu'ils ont effectivement accès au site Web du commerçant de leur choix et non à un éventuel site fantôme.

La reconnaissance mutuelle des moyens d'identification électronique et la large acceptation des signatures électroniques faciliteront la fourniture transnationale de nombreux services dans le marché intérieur et permettront aux entreprises d'étendre leurs activités à l'étranger sans rencontrer d'obstacle dans leurs relations avec les pouvoirs publics. S'agissant d'effectuer des formalités administratives, cela signifiera, dans la pratique, des gains d'efficacité importants pour les entreprises comme pour les particuliers. Par exemple, il sera possible à un étudiant de s'inscrire par voie électronique dans une université à l'étranger, à un contribuable de remettre à un autre État membre une déclaration d'impôts en ligne ou à un patient d'accéder à son dossier médical en ligne. Sans reconnaissance mutuelle des moyens d'identification électronique, un médecin ne peut pas avoir accès aux informations dont il a besoin pour soigner un patient et il faut que ce dernier refasse les examens et analyses qu'il a déjà effectués.

b) Valeur ajoutée (critère d'efficacité)

La coordination volontaire entre États membres ne permet pas actuellement d'atteindre les objectifs exposés ci-dessus, et il est peu vraisemblable que cela se produise à l'avenir. Cela implique des doubles emplois, la fixation de normes différentes, des caractéristiques transnationales des retombées générées par les TIC et une complexité administrative pour mettre en place une telle coordination au moyen d'accords bilatéraux et multilatéraux.

De plus, la nécessité de surmonter des problèmes comme (a) l'absence de sécurité juridique, due aux dispositions nationales disparates résultant d'interprétations divergentes de la directive sur les signatures électroniques, et (b) le manque d'interopérabilité des systèmes de signature électronique instaurés au niveau national, dû à l'application non uniforme des normes techniques, implique un type de coordination entre États membres qui peut être plus efficacement assuré au niveau de l'UE.

3.3 Explication détaillée de la proposition

3.3.1 CHAPITRE I – DISPOSITIONS GÉNÉRALES

L'article 1er définit l'objet du règlement.

L'article 2 définit le champ d'application matériel du règlement.

L'article 3 définit les termes employés dans le règlement. Certaines définitions sont reprises de la directive 1999/93/CE, d'autres sont précisées ou complétées, ou de nouvelles sont ajoutées.

L'article 4 définit les principes du marché intérieur en ce qui concerne l'application territoriale du règlement. Il y est expressément énoncé qu'il n'y a pas de restriction à la libre prestation des services ni à la libre circulation des produits.

3.3.2 CHAPITRE II – IDENTIFICATION ÉLECTRONIQUE

L'article 5 prévoit la reconnaissance et l'acceptation mutuelles des moyens d'identification électronique relevant d'un système qui sera notifié à la Commission selon les conditions

fixées dans le règlement. En effet, la plupart des États membres ont adopté un type de système d'identification électronique, mais ces systèmes diffèrent sur de nombreux points. L'absence de base juridique commune imposant à chaque État membre de reconnaître et d'accepter les moyens d'identification électronique délivrés dans d'autres États membres pour accéder à des services en ligne, ainsi que l'insuffisante interopérabilité transnationale des identifications électroniques nationales constituent des obstacles qui empêchent les particuliers et les entreprises de profiter pleinement du marché unique du numérique. La reconnaissance et l'acceptation mutuelles de tout moyen d'identification électronique relevant d'un système notifié en vertu du présent règlement permettent de lever ces obstacles juridiques.

Le règlement ne fait pas obligation aux États membres de mettre en place ou de notifier des systèmes d'identification électronique, mais de reconnaître et d'accepter les identifications électroniques notifiées pour les services en ligne dont l'accès au niveau national exige une telle identification. L'augmentation potentielle des économies d'échelle permises par l'utilisation transnationale de moyens d'identification électronique et de systèmes d'authentification notifiés peut inciter les États membres à notifier leurs systèmes d'identification électronique. L'article 6 définit les cinq conditions auxquelles est soumise la notification des systèmes d'identification électronique.

Les États membres peuvent notifier les systèmes d'identification électronique qu'ils acceptent sous leur juridiction lorsqu'une identification électronique est exigée pour accéder à des services publics. Une exigence supplémentaire impose que le moyen d'identification électronique respectif soit délivré par l'État membre notifiant le système, en son nom ou, au moins, sous sa responsabilité.

Les États membres doivent établir un lien univoque entre les données d'identification électronique et la personne concernée. Cette obligation signifie non pas qu'une personne ne peut pas avoir plusieurs moyens d'identification électronique, mais que les moyens doivent tous renvoyer à la même personne.

La fiabilité d'une identification électronique dépend de la disponibilité des moyens d'authentification (c'est-à-dire de la possibilité de vérifier la validité des données d'identification électronique). Le règlement fait obligation aux États membres notifiants de fournir gratuitement des moyens d'authentification en ligne aux tierces parties. La possibilité d'authentification doit être offerte sans interruption. Aucune exigence technique particulière, en matière de matériel ou de logiciel, ne peut être imposée aux parties qui recourent à l'authentification. Cette disposition ne concerne pas les exigences imposées aux utilisateurs (détenteurs) du moyen d'identification électronique, tel un lecteur de carte, et qui sont techniquement nécessaires pour l'utiliser.

Les États membres doivent assumer la responsabilité de l'univocité du lien (c'est-à-dire que les données d'identification attribuées à une personne ne renvoient à aucune autre personne) et de la possibilité d'authentification (c'est-à-dire la possibilité de vérifier la validité des données d'identification électronique). La responsabilité des États membres ne couvre aucun autre aspect du processus d'identification ni aucune transaction exigeant une identification.

L'article 7 contient les règles de notification des systèmes d'identification électronique à la Commission.

L'article 8 vise à assurer l'interopérabilité technique des systèmes d'identification notifiés, selon une approche de coordination ainsi que des actes délégués.

3.3.3 CHAPITRE III – SERVICES DE CONFIANCE

3.3.3.1 Section 1 – Dispositions générales

L'article 9 pose les principes relatifs à la responsabilité des prestataires de services de confiance qualifiés et non qualifiés. Il repose sur l'article 6 de la directive 1999/93/CE et étend le droit à réparation des dommages causés par un prestataire de service de confiance qui n'a pas appliqué de bonnes pratiques de sécurité, lorsque cette négligence entraîne une atteinte à la sécurité ayant des conséquences importantes pour le service.

L'article 10 décrit le mécanisme de reconnaissance et d'acceptation des services de confiance qualifiés fournis par un prestataire établi dans un pays tiers. Il repose sur l'article 7 de la directive 1999/93/CE mais ne retient que la seule solution concrètement envisageable, à savoir permettre la reconnaissance en vertu d'un accord international entre l'Union européenne et des pays tiers ou des organisations internationales.

L'article 11 pose les principes de la protection et de la limitation des données utilisées. Il repose sur l'article 8 de la directive 1999/93/CE.

L'article 12 dispose que les services de confiance sont accessibles aux personnes handicapées.

3.3.3.2 Section 2 – Contrôle

L'article 13 fait obligation aux États membres de mettre en place des organes de contrôle, sur la base de l'article 3, paragraphe 3, de la directive 1999/93/CE, en précisant et en étendant le mandat de ces derniers en ce qui concerne les prestataires de services de confiance et les prestataires de services de confiance qualifiés.

L'article 14 instaure un mécanisme spécifique d'assistance mutuelle entre les organes de contrôle dans les États membres afin de faciliter le contrôle transnational des prestataires de services de confiance. Il instaure des règles relatives aux opérations communes et au droit des autorités de contrôle de participer à ces opérations.

L'article 15 instaure l'obligation, pour les prestataires de services de confiance qualifiés et non qualifiés, d'appliquer les mesures techniques et organisationnelles appropriées afin de garantir la sécurité de leurs activités. En outre, les organes de contrôle compétents et autres autorités concernées doivent être informés de toute atteinte à la sécurité. Le cas échéant, ils en informeront les organes de contrôle des autres États membres ainsi que, directement ou par l'intermédiaire du prestataire de service de confiance concerné, le public.

L'article 16 définit les conditions du contrôle des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent. Il fait obligation aux prestataires de services de confiance qualifiés de se soumettre tous les ans à un audit réalisé par un organisme indépendant reconnu pour confirmer à l'organe de contrôle qu'ils remplissent les obligations énoncées dans le règlement. En outre, l'article 16, paragraphe 2, confère à l'organe de contrôle le droit d'effectuer des audits sur place, à tout moment, chez les prestataires de services de confiance qualifiés. L'organe de contrôle est également habilité à donner à ces derniers des instructions contraignantes pour remédier, de façon proportionnée, à tout manquement à une obligation révélé par l'audit de sécurité.

L'article 17 concerne l'activité exercée par l'organe de contrôle à la demande d'un prestataire de service de confiance en vue de fournir un service de confiance qualifié.

L'article 18 prévoit l'établissement de listes de confiance[10] contenant des informations sur les prestataires de services de confiance qualifiés soumis à contrôle et sur les services qualifiés qu'ils offrent. Ces informations doivent être mises à la disposition du public selon un modèle commun afin d'en faciliter l'utilisation automatique et fournir un niveau de détail approprié.

L'article 19 définit les exigences auxquelles les prestataires de services de confiance qualifiés doivent satisfaire afin d'être reconnus comme tels. Il s'inspire de l'annexe II de la directive 1999/93/CE.

3.3.3.3 Section 3 – Signature électronique

L'article 20 consacre les règles relatives à l'effet juridique des signatures électroniques des personnes physiques. Il précise et développe l'article 5 de la directive 1999/93/CE en instaurant l'obligation expresse de donner aux signatures électroniques qualifiées le même effet juridique qu'aux signatures manuscrites. En outre, les États membres doivent veiller à l'acceptation transnationale des signatures électroniques qualifiées, dans le contexte de la fourniture de services publics, et ne doivent pas imposer d'exigences supplémentaires pouvant constituer des obstacles à l'utilisation de ces signatures.

L'article 21 définit les exigences applicables aux certificats de signature qualifiés. Il précise l'annexe I de la directive 1999/93/CE dont sont supprimées les dispositions qui étaient inapplicables en pratique (par exemple, les limites à la valeur des transactions).

L'article 22 définit les exigences applicables aux dispositifs de création de signature électronique qualifiés. Il précise les exigences posées à l'article 3, paragraphe 5, de la directive 1999/93/CE et applicables aux dispositifs sécurisés de création de signature qui, en vertu du présent règlement, doivent désormais être considérés comme des dispositifs de création de signature électronique qualifiés. De plus, il dispose clairement que la définition d'un dispositif de création de signature peut être beaucoup plus large et ne se limite pas à ce qui contient des données de création de signature. La Commission peut aussi établir une liste des numéros de référence des normes définissant les exigences de sécurité applicables aux dispositifs.

Se fondant sur l'article 3, paragraphe 4, de la directive 1999/93/CE, l'article 23 introduit le concept de certification des dispositifs de création de signature électronique qualifiés afin de déterminer leur conformité aux exigences de sécurité énoncées à l'annexe II. Ces dispositifs doivent être reconnus par tous les États membres comme satisfaisant aux exigences dès lors qu'une procédure de certification est appliquée par un organisme de certification désigné par un État membre. La Commission publiera une liste positive de ces dispositifs certifiés, conformément à l'article 24. La Commission peut aussi établir une liste des numéros de référence des normes pour l'évaluation de la sécurité des produits informatiques visés à l'article 23, paragraphe 1.

L'article 24 concerne la publication, par la Commission, d'une liste de dispositifs de création de signature électronique qualifiés, après notification de leur conformité par les États membres.

[10] La liste de confiance établie par la décision 2009/767/CE de la Commission, modifiée par la décision 2010/425/UE de la Commission, servira de base à une nouvelle décision de la Commission sur les listes de confiance en vertu du présent règlement.

L'article 25 repose sur les recommandations, figurant à l'annexe IV de la directive 1999/93/CE, de soumettre la validation des signatures électroniques qualifiées à des exigences contraignantes en vue d'accroître la sécurité juridique de cette validation.

L'article 26 définit les conditions applicables aux services de validation qualifiés.

L'article 27 définit les conditions de conservation à long terme des signatures électroniques qualifiées. Cela est rendu possible par le recours à des procédures et des technologies permettant d'étendre la fiabilité de la validation des signatures électroniques qualifiées au-delà de leur délai de validité technologique, lorsqu'il devient plus facile pour les cyberdélinquants de les falsifier.

3.3.3.4 Section 4 – Cachets électroniques

L'article 28 concerne l'effet juridique des cachets électroniques des personnes morales. Une présomption légale spécifique est conférée au cachet électronique qualifié qui garantit l'origine et l'intégrité des documents électroniques auxquels il est associé.

L'article 29 définit les exigences applicables aux certificats qualifiés de cachet électronique.

L'article 30 définit les exigences applicables à la certification et à la publication d'une liste des dispositifs de création de cachet électronique qualifiés.

L'article 31 définit les conditions de validation et de conservation des cachets électroniques qualifiés.

3.3.3.5 Section 5 – Horodatage électronique

L'article 32 concerne l'effet juridique des horodatages électroniques. Une présomption légale spécifique est conférée aux horodatages électroniques qualifiés en ce qui concerne l'exactitude de l'heure.

L'article 33 définit les exigences applicables aux horodatages électroniques qualifiés.

3.3.3.6 Section 6 – Documents électroniques

L'article 34 traite des effets juridiques et des conditions d'acceptation des documents électroniques. Tout document électronique signé à l'aide d'une signature électronique qualifiée ou revêtu d'un cachet électronique qualifié bénéficie d'une présomption légale d'authenticité et d'intégrité spécifique. S'agissant de l'acceptation des documents électroniques, lorsqu'il est exigé un document original ou une copie certifiée pour la fourniture d'un service public, au moins les documents électroniques délivrés par les personnes compétentes pour délivrer les documents imprimés correspondants et qui sont considérés comme des originaux ou des copies certifiées selon le droit national de l'État membre d'origine, doivent être acceptés dans d'autres États membres sans exigence supplémentaire.

3.3.3.7 Section 7 – Services de fourniture électronique

L'article 35 concerne l'effet juridique des données envoyées ou reçues à l'aide d'un service de fourniture électronique. Une présomption légale spécifique, concernant l'intégrité des données envoyées ou reçues et l'exactitude de l'heure à laquelle les données sont envoyées ou reçues,

est garantie pour les services de fourniture électronique qualifiés. Il garantit aussi la reconnaissance mutuelle des services de fourniture électronique qualifiés au niveau de l'UE.

L'article 36 définit les exigences applicables aux services de fourniture électronique qualifiés.

3.3.3.8 Section 8 – Authentification de site Web

Cette section vise à faire en sorte que l'authenticité d'un site Web soit garantie relativement au propriétaire du site.

L'article 37 définit les exigences applicables aux certificats qualifiés d'authentification de site Web, lesquels peuvent être utilisés pour garantir l'authenticité d'un site Web. Un certificat qualifié d'authentification de site Web fournira un ensemble minimal d'informations fiables sur le site et sur la personnalité juridique de son propriétaire.

3.3.4 CHAPITRE IV – ACTES DÉLÉGUÉS

L'article 38 contient les dispositions types applicables à l'exercice de la délégation, conformément à l'article 290 du TFUE (actes délégués). Celui-ci autorise le législateur à déléguer à la Commission le pouvoir d'adopter des actes non législatifs de portée générale qui complètent ou modifient certains éléments non essentiels d'un acte législatif.

3.3.5 CHAPITRE V – ACTES D'EXÉCUTION

L'article 39 contient la disposition relative à la procédure de comité nécessaire pour conférer des compétences d'exécution à la Commission dans les cas où, conformément à l'article 291 du TFUE, il est nécessaire de prévoir des conditions uniformes d'exécution d'actes de l'Union juridiquement contraignants. La procédure d'examen s'applique.

3.3.6 CHAPITRE VI – DISPOSITIONS FINALES

L'article 40 fait obligation à la Commission d'évaluer le règlement et de présenter ses conclusions.

L'article 41 abroge la directive 1999/93/CE et consacre la transition harmonieuse entre l'infrastructure de signature électronique existante et les nouvelles exigences du règlement.

L'article 42 fixe la date d'entrée en vigueur du règlement.

4. INCIDENCES BUDGÉTAIRES

Les incidences budgétaires spécifiques de la proposition concernent les missions dévolues à la Commission européenne, comme il est indiqué dans la fiche financière législative jointe à la présente proposition.

La proposition n'a pas d'incidence sur les dépenses de fonctionnement.

La fiche financière législative accompagnant la présente proposition de règlement couvre les incidences budgétaires du règlement lui-même.

2012/0146 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

(Texte présentant de l'intérêt pour l'EEE)

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[11],

après consultation du contrôleur européen de la protection des données[12],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique. En effet, si les consommateurs, les entreprises et les administrations n'ont pas confiance, 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 permettant des interactions électroniques sûres et sans discontinuité entre les entreprises, les particuliers et les pouvoirs publics et en accroissant ainsi l'efficacité des services en ligne publics et privés et de l'activité économique et du commerce électroniques dans l'Union.

(3) La directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques[13] couvrait essentiellement les signatures électroniques sans fournir de cadre transnational et intersectoriel complet pour des transactions électroniques sûres, fiables et aisées. Le présent règlement renforce et développe l'acquis que représente la directive.

---

11 JO C du …, p. ...

12 JO C du …, p. ...

13 JO L 13 du 19.1.2000, p. 12.

(4) La stratégie numérique pour l'Europe[14] de la Commission recense le cloisonnement du marché du 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, la Commission a également souligné la nécessité de «résoudre les principaux problèmes empêchant les citoyens européens de profiter des avantages d'un marché unique du numérique et des services numériques transfrontaliers»[15].

(5) Le Conseil européen a invité la Commission à créer un marché unique du numérique d'ici à 2015[16], à progresser rapidement dans les domaines clés de l'économie numérique et à favoriser la mise en place d'un marché unique du numérique pleinement intégré[17] en facilitant l'utilisation transnationale des services en ligne et, en particulier, l'identification et l'authentification électroniques sécurisées.

(6) Le Conseil a invité la Commission à contribuer à la mise en place du marché unique du numérique en créant les conditions propices à la reconnaissance mutuelle, entre les pays, d'outils clés tels que l'identification électronique, les documents électroniques, les signatures électroniques et les services de fourniture électronique, ainsi qu'à la mise au point de services interopérables d'administration en ligne dans toute l'Union européenne[18].

(7) Le Parlement européen a souligné l'importance de la sécurité des services électroniques, en particulier des signatures électroniques, et la nécessité de créer une infrastructure à clé publique au niveau paneuropéen, et a invité la Commission à mettre en place un portail des autorités européennes de validation afin d'assurer l'interopérabilité transnationale des signatures électroniques et d'accroître la sécurité des transactions réalisées au moyen de l'internet[19].

(8) La directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur[20] exige des États membres qu'ils créent des guichets uniques pour veiller à ce 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 concerné et 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 prestataires de services d'un autre État membre ne peuvent pas utiliser leur identification électronique pour accéder à ces services car les systèmes nationaux d'identification électronique dans leur pays ne sont pas reconnus ni acceptés dans d'autres États membres. Cet obstacle numérique empêche les prestataires de services de tirer tous les bénéfices du marché intérieur. La reconnaissance et

---

14 COM(2010) 245 final/2.

15 Rapport 2010 sur la citoyenneté de l'Union *Lever les obstacles à l'exercice des droits des citoyens de l'Union*, COM(2010) 603 final, point 2.2.2, page 15.

16 4/2/2011: Document EUCO 2/1/11.

17 23/10/2011: Document EUCO 52/1/11.

18 Conclusions du Conseil sur le plan d'action 2011-2015 pour l'administration en ligne, 3093e session du Conseil Transports, télécommunications et énergie, Bruxelles, le 27 mai 2011.

19 Résolution du Parlement européen du 21.9.2010 sur l'achèvement du marché intérieur pour ce qui concerne le commerce en ligne [P7_TA(2010)0320] et résolution du Parlement européen du 15.6.2010 sur la gouvernance de l'internet: les prochaines étapes [P7_TA(2010)0208].

20 JO L 376 du 27.12.2006, p. 36.

l'acceptation mutuelles des moyens d'identification électronique faciliteront la fourniture transnationale de nombreux services dans le marché intérieur et permettront aux entreprises d'étendre leurs activités à l'étranger sans rencontrer beaucoup d'obstacles dans leurs relations avec les pouvoirs publics.

(10) La 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[21] instaure un réseau d'autorités nationales responsables de la santé en ligne. Pour assurer la sécurité et la continuité des soins de santé transnationaux, ce réseau est tenu d'établir des orientations concernant l'accès transnational 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 et l'acceptation mutuelles de l'identification et de l'authentification électroniques sont essentielles pour que les soins de santé transnationaux deviennent une réalité pour les Européens. Lorsque ces derniers doivent se déplacer pour subir un traitement, il faut que leur dossier médical soit accessible dans le pays où les soins sont dispensés, ce qui exige un cadre solide, sûr et fiable en matière d'identification électronique.

(11) L'un des objectifs du présent règlement est de lever les obstacles existants à l'utilisation transnationale des moyens d'identification électronique employés dans les États membres pour accéder, au moins, aux services publics. Le présent règlement ne vise pas à influer sur les systèmes de gestion de l'identité électronique et les infrastructures associées établis dans les États membres. Il a pour but de faire en sorte que, concernant l'accès aux services en ligne transnationaux proposés par les États membres, il soit possible de sécuriser l'identification et l'authentification électroniques.

(12) 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 pas le secteur privé dans la fourniture de ces moyens. Les États membres ne devraient pas être tenus de notifier leurs systèmes d'identification électronique. Il appartient aux États membres de choisir de notifier la totalité, une partie ou aucun des systèmes d'identification électronique utilisés au niveau national pour accéder au moins aux services publics en ligne ou à des services précis.

(13) Il faut fixer certaines conditions, dans le règlement, en ce qui concerne les moyens d'identification électronique qui doivent être acceptés et la façon dont les systèmes devraient être notifiés. Ces conditions devraient permettre aux États membres de susciter la confiance nécessaire dans leurs systèmes d'identification électronique respectifs et faciliter la reconnaissance et l'acceptation mutuelles des moyens d'identification électronique relevant de leurs systèmes notifiés. Le principe de la reconnaissance et de l'acceptation mutuelles devrait s'appliquer si l'État membre notifiant remplit les conditions de notification et si la notification a été publiée au Journal officiel de l'Union européenne. Toutefois, 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.

[21] JO L 88 du 4.4.2011, p. 45.

(14) Les États membres devraient être à même de décider d'impliquer le secteur privé dans la délivrance de moyens d'identification électronique et d'autoriser le secteur privé à utiliser, aux fins de l'identification exigée par des services en ligne ou des transactions électroniques, les moyens d'identification électronique relevant d'un système 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 aux services en ligne transnationaux. Afin de faciliter l'utilisation transnationale de tels moyens d'identification électronique par le secteur privé, la possibilité d'authentification prévue par les États membres devrait être offerte aux parties utilisatrices sans distinction entre secteur public et secteur privé.

(15) L'utilisation transnationale de moyens d'identification électronique relevant d'un système notifié exige des États membres qu'ils coopèrent en assurant l'interopérabilité technique. Cela exclut toute règle technique nationale spécifique imposant par exemple aux parties d'autres pays de se procurer un matériel ou logiciel particulier pour vérifier et valider l'identification électronique notifiée. En revanche, les exigences techniques applicables aux utilisateurs et découlant des spécifications inhérentes au type de jeton employé (par exemple carte à puce) sont inévitables.

(16) La coopération des États membres devrait contribuer à l'interopérabilité technique des systèmes d'identification électronique notifiés en vue de garantir un niveau élevé de confiance et de sécurité, adapté au degré de risque, et l'échange d'informations et des meilleures pratiques entre les États membres en vue de la reconnaissance mutuelle de ces systèmes devrait faciliter une telle coopération.

(17) Le présent règlement devrait aussi instaurer un cadre juridique général concernant l'utilisation des services de confiance électroniques. Toutefois, il ne devrait pas imposer d'obligation générale d'y recourir. En particulier, il ne devrait pas couvrir la fourniture de services sur la base d'accords volontaires régis par le droit privé. Il 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.

(18) Afin de contribuer à l'utilisation transnationale généralisée des services de confiance électroniques, il devrait être possible de les utiliser comme preuve en justice dans tous les États membres.

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

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

(21) Le présent règlement devrait être neutre du point de vue technologique. 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.

(22) Pour accroître la confiance du public 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 service de confiance qualifié devraient être introduites en vue de définir les exigences et obligations à respecter pour assurer un niveau élevé de sécurité de tous les services et produits de confiance qualifiés qui sont utilisés ou fournis.

(23) Conformément aux obligations découlant de la convention des Nations unies relative aux droits des personnes handicapées, qui est entrée en vigueur dans l'Union européenne, 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.

(24) Un prestataire de service de confiance est responsable du traitement de données personnelles et doit donc satisfaire aux obligations énoncées dans la 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[22]. En particulier, la collecte des données doit être limitée autant que possible et compte tenu de la finalité du service fourni.

(25) Les organes de contrôle devraient coopérer et échanger des informations avec les autorités responsables de la protection des données afin d'assurer l'application correcte, par les prestataires de services, de la législation en la matière. L'échange d'informations devrait porter, en particulier, sur les incidents liés à la sécurité et les violations de données à caractère personnel.

(26) 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.

(27) Les dispositions relatives à l'utilisation de pseudonymes dans des certificats ne devraient pas empêcher les États membres d'exiger l'identification des personnes conformément au droit national ou de l'Union.

(28) 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 permettre 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.

(29) La notification des atteintes à la sécurité et de l'analyse des risques pour la sécurité est essentielle pour fournir les informations adéquates aux parties concernées en cas d'atteinte à la sécurité ou de perte d'intégrité.

(30) 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 est demandé aux organes de contrôle de fournir des informations succinctes à la

[22] JO L 281 du 23.11.1995, p. 31.

Commission et à l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

(31) Pour permettre à la Commission et aux États membres d'évaluer l'impact du présent règlement, il devrait être demandé aux organes de contrôle de fournir des statistiques sur les services de confiance qualifiés et l'utilisation qui en est faite.

(32) 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 que les exigences de contrôle essentielles sont satisfaites de façon cohérente et efficace dans tous les États membres.

(33) Pour assurer la pérennité des services de confiance qualifiés et pour accroître la confiance des utilisateurs dans la continuité de ces services, les organes de contrôle devraient veiller à ce que les données des prestataires de services de confiance qualifiés soient conservées et restent accessibles, pendant une période de temps appropriée, même lorsqu'un de ces prestataires cesse d'exister.

(34) 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 et n'y 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 devrait être instauré un système d'assistance mutuelle entre les organes de contrôle dans les États membres.

(35) Il incombe aux prestataires de services de confiance de satisfaire aux exigences définies dans le présent règlement en ce qui concerne la fourniture de services de confiance, en particulier de services de confiance qualifiés. Les organes de contrôle ont la responsabilité de contrôler comment les prestataires de services de confiance satisfont à ces exigences.

(36) Afin de permettre un processus de mise en place, 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 potentiels de services de confiance qualifiés et l'organe de contrôle compétent en vue de faciliter la vérification préalable à la fourniture de services de confiance qualifiés.

(37) Les listes de confiance sont essentielles pour susciter la confiance des opérateurs économiques car elles indiquent le statut qualifié du prestataire de service au moment du contrôle, mais elles ne constituent pas une condition préalable à l'obtention du statut qualifié ni à la fourniture de services de confiance qualifiés, lesquelles sont subordonnées au respect des exigences du présent règlement.

(38) Dès lors qu'il a fait l'objet d'une notification, un service de confiance qualifié ne peut être refusé pour l'accomplissement d'une procédure ou d'une formalité administrative par l'organisme du secteur public concerné, au motif qu'il ne figure pas sur les listes de confiance établies par les États membres. À cette fin, on entend par organisme du secteur public tout pouvoir public ou toute entité chargés de fournir des services

d'administration en ligne comme les déclarations d'impôts en ligne, les demandes de certificat de naissance en ligne, les procédures de marchés publics électroniques, etc.

(39) 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 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[23], des signatures électroniques offrant une moindre garantie de sécurité devraient également être acceptées.

(40) Les dispositifs de création de signature électronique qualifiés devraient pouvoir être confiés par le signataire aux soins d'un tiers pour autant que les mécanismes et procédures appropriés soient appliqués 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 satisfasse aux exigences en matière de signature qualifiée.

(41) Pour garantir la sécurité juridique concernant la validité de la signature, il est essentiel de préciser les éléments de la signature électronique qualifiée que doit 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 le secteur privé ou public à investir dans de tels services. Les deux éléments devraient faire de la validation de signature électronique qualifiée une procédure aisée et adaptée à toutes les parties au niveau de l'Union.

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

(43) 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.

(44) Le présent règlement devrait prévoir la conservation à long terme des informations, c'est-à-dire la validité juridique des signatures et cachets électroniques sur de longues périodes de temps, et garantir qu'elles pourront être validées indépendamment de l'évolution technologique future.

(45) Afin de développer l'utilisation transnationale des documents électroniques, le présent règlement devrait prévoir une disposition conférant un effet juridique aux documents électroniques, lesquels doivent être considérés comme équivalents aux documents imprimés, sous réserve de l'analyse de risques et pour autant que l'authenticité et l'intégrité des documents soient garanties. Il est également important, pour le développement des transactions électroniques transnationales au sein du marché intérieur, que les documents électroniques originaux ou les copies certifiées délivrés par les autorités compétentes dans un État membre, conformément au droit national, soient aussi acceptés comme tels dans les autres États membres. Le présent règlement ne devrait pas porter atteinte au droit des États membres de déterminer ce qui constitue

[23] JO L 274 du 20.10.2009, p. 36.

un original ou une copie au niveau national, mais garantit que ceux-ci peuvent être utilisés comme tels au niveau transnational.

(46) Comme les autorités compétentes dans les États membres utilisent actuellement différents formats de signature électronique avancée pour signer électroniquement leurs documents, il faut faire en sorte que les États membres, lorsqu'ils reçoivent des documents signés électroniquement, puissent prendre en charge techniquement un nombre minimal 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 un nombre minimal de formats de cachet électronique avancé.

(47) Les cachets électroniques peuvent servir à authentifier, outre un document délivré par une personne morale, tout bien numérique de ladite personne, par exemple un code logiciel ou un serveur.

(48) Faire en sorte qu'il soit possible d'authentifier un site Web et la personne qui en est propriétaire rendrait plus ardue la falsification de sites et limiterait donc la fraude.

(49) Afin de compléter, de façon souple et rapide, certains aspects techniques précis du présent règlement, le pouvoir d'adopter des actes, conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne, devrait être délégué à la Commission en ce qui concerne l'interopérabilité de l'identification électronique; les mesures de sécurité exigées des prestataires de services de confiance; les organismes indépendants reconnus responsables de l'audit des prestataires de services; les listes de confiance; les exigences relatives aux niveaux de sécurité des signatures électroniques; les exigences relatives aux certificats qualifiés de signature électronique, à leur validation et à leur conservation; les organismes responsables de la certification des dispositifs de création de signature électronique qualifiés; les exigences relatives aux niveaux de sécurité des cachets électroniques et aux certificats qualifiés de cachet électronique; et l'interopérabilité des services de fourniture. Il est particulièrement important que la Commission procède aux consultations appropriées tout au long de son travail préparatoire, y compris au niveau des experts.

(50) Lorsqu'elle prépare et élabore des actes délégués, la Commission devrait veiller à ce que tous les documents utiles soient transmis en temps voulu, de façon appropriée et simultanée au Parlement européen et au Conseil.

(51) Afin que des conditions uniformes de mise en œuvre du présent règlement soient réunies, des compétences d'exécution devraient être conférées à la Commission, notamment pour ce qui est de spécifier les numéros de référence des normes dont l'utilisation donnerait une présomption de conformité à certaines exigences énoncées dans le présent règlement ou définies dans des actes délégués. Ces compétences devraient être exercées conformément au 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[24].

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

---

[24] JO L 55 du 28.2.2011, p. 13.

(53) Pour garantir la sécurité juridique aux opérateurs économiques qui utilisent déjà des certificats qualifiés délivrés conformément à la directive 1999/93/CE, il est nécessaire de prévoir un délai suffisant à des fins transitoires. Il est également nécessaire de doter la Commission des moyens d'adopter auparavant les actes d'exécution et les actes délégués.

(54) Comme les objectifs du présent règlement ne peuvent être atteints de manière suffisante par les États membres et peuvent donc, en raison de l'ampleur de l'action, être mieux atteints au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité énoncé 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 cet objectif, notamment en ce qui concerne le rôle, assumé par la Commission, de coordinateur des activités nationales,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

1. Le présent règlement établit des règles applicables à l'identification électronique et aux services de confiance électroniques pour les transactions électroniques en vue d'assurer le bon fonctionnement du marché intérieur.

2. Le présent règlement pose les conditions dans lesquelles un État membre reconnaît et accepte les moyens d'identification électronique des personnes physiques et morales, qui relèvent d'un système d'identification électronique notifié d'un autre État membre.

3. Le présent règlement instaure un cadre juridique pour les signatures électroniques, les cachets électroniques, les horodatages électroniques, les documents électroniques, les services de fourniture électronique et l'authentification de sites Web.

4. Le présent règlement garantit que les services et produits de confiance qui y sont conformes sont autorisés à circuler librement au sein du marché intérieur.

Article 2

Champ d'application

1. Le présent règlement s'applique à l'identification électronique produite par les États membres, en leur nom ou sous leur responsabilité, 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 électroniques sur la base d'accords volontaires régis par le droit privé.

3. Le présent règlement ne s'applique pas aux 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.

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 sans ambiguïté une personne physique ou morale;

2) «moyen d'identification électronique», un élément matériel ou immatériel contenant des données visées au point 1) du présent article et servant à accéder à des services en ligne visés à l'article 5;

3) «système d'identification électronique», un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes visées au point 1 du présent article;

4) «authentification», un processus électronique qui permet de valider l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée électronique;

5) «signataire», une personne physique qui crée une signature électronique;

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

7) «signature électronique avancée», une signature électronique qui satisfait aux exigences suivantes:

(a) être liée uniquement au signataire;

(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 auxquelles elle est associée de telle sorte que toute modification ultérieure des données soit détectable;

8) «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;

9) «données de création de signature électronique», les données uniques qui sont utilisées par le signataire pour créer une signature électronique;

10) «certificat», une attestation électronique qui associe les données de validation d'une signature ou d'un cachet électronique à une personne physique ou une personne morale respectivement et confirme les données de cette personne;

11) «certificat qualifié de signature électronique», une attestation qui sert à étayer les signatures électroniques, qui est délivrée par un prestataire de service de confiance qualifié et qui satisfait aux exigences énoncées à l'annexe I;

12) «service de confiance», un service électronique consistant en la création, la vérification, la validation, le traitement et la conservation de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, de services de fourniture électronique, d'authentification de site Web et de certificats électroniques, y compris de certificats de signature électronique et de cachet électronique;

13) «service de confiance qualifié», un service de confiance qui satisfait aux exigences applicables prévues par le présent règlement;

14) «prestataire de service de confiance», une personne physique ou morale qui fournit un ou plusieurs services de confiance;

15) «prestataire de service de confiance qualifié», un prestataire de service de confiance qui satisfait aux exigences énoncées dans le présent règlement;

16) «produit électronique», un dispositif matériel ou logiciel – ou les composants correspondants de celui-ci – qui est destiné à être utilisé pour la fourniture de services de confiance;

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

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

19) «créateur de cachet», une personne physique qui crée un cachet électronique;

20) «cachet électronique», des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données électroniques pour garantir l'origine et l'intégrité des données associées;

21) «cachet électronique avancé», un cachet électronique qui satisfait aux exigences suivantes:

(a) être lié uniquement au créateur du cachet;

(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;

22) «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;

23) «données de création de cachet électronique», les données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique;

24) «certificat qualifié de cachet électronique», une attestation qui sert à étayer un cachet électronique, qui est délivrée par un prestataire de service de confiance qualifié et qui satisfait aux exigences énoncées à l'annexe III;

25) «horodatage électronique», des données sous forme électronique qui associent d'autres données électroniques à un instant particulier et établissent la preuve que ces données existaient à cet instant;

26) «horodatage électronique qualifié», un horodatage électronique qui satisfait aux exigences énoncées à l'article 33;

27) «document électronique», un document dans un format électronique;

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

29) «service de fourniture électronique qualifié», un service de fourniture électronique qui satisfait aux exigences énoncées à l'article 36;

30) «certificat qualifié d'authentification de site Web», une attestation qui permet d'authentifier un site Web et associe celui-ci à la personne à laquelle le certificat est délivré par un prestataire de service de confiance qualifié et qui satisfait aux exigences énoncées à l'annexe IV;

31) «données de validation», des données qui servent à valider une signature électronique ou 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 service de confiance établi dans d'autres États membres pour des raisons qui relèvent des domaines couverts par le présent règlement.

2. Les produits qui sont conformes au présent règlement sont autorisés à circuler librement au sein du marché intérieur.

CHAPITRE II

Identification électronique

Article 5

Reconnaissance et acceptation mutuelles

Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée en vertu de la législation nationale ou de pratiques administratives pour accéder à un service en ligne, tout moyen d'identification électronique délivré dans un autre État membre, qui relève d'un système figurant sur la liste publiée par la

Commission conformément à la procédure visée à l'article 7, est reconnu et accepté aux fins de l'accès à ce service.

Article 6

Conditions de notification des systèmes d'identification électronique

1. Les systèmes d'identification électronique sont susceptibles de notification conformément à l'article 7 si toutes les conditions suivantes sont remplies:

(a) les moyens d'identification électronique sont délivrés par l'État membre notifiant ou en son nom ou sous sa responsabilité;

(b) les moyens d'identification électronique peuvent être utilisés pour accéder au moins aux services publics exigeant l'identification électronique dans l'État membre notifiant;

(c) l'État membre notifiant veille à ce que les données d'identification de la personne soient attribuées sans ambiguïté à la personne physique ou morale visée à l'article 3, point 1;

(d) l'État membre notifiant veille à ce qu'une possibilité d'authentification en ligne soit disponible à tout moment et gratuitement afin de permettre aux parties utilisatrices de valider les données d'identification personnelle reçues sous forme électronique. Les États membres n'imposent aucune exigence technique spécifique aux parties utilisatrices établies en dehors de leur territoire, qui envisagent de procéder à cette authentification. Lorsque le système d'identification notifié ou la possibilité d'authentification sont violés ou partiellement compromis, les États membres suspendent ou révoquent immédiatement le système d'identification notifié ou la possibilité d 'authentification ou les éléments compromis en cause et en informent les autres États membres et la Commission conformément à l'article 7;

(e) l'État membre notifiant est responsable:

- i) de l'attribution univoque des données d'identification personnelle visées au point c); et
- ii) de la possibilité d'authentification indiquée au point d).

2. Le point e) du paragraphe 1 est sans préjudice de la responsabilité des parties relativement à une transaction effectuée à l'aide de moyens d'identification électronique relevant du système notifié.

Article 7

Notification

1. Les États membres qui notifient un système d'identification électronique transmettent les informations suivantes à la Commission et lui communiquent toute modification ultérieure dans les meilleurs délais:

(a) description du système d'identification électronique notifié;

(b) autorités responsables du système d'identification électronique notifié;

(c) indication des personnes chargées de gérer l'enregistrement des identifiants personnels univoques;

(d) description de la possibilité d'authentification;

(e) dispositions concernant la suspension ou la révocation du système d'identification notifié, de la possibilité d'authentification ou des parties compromises en cause.

2. Six mois après l'entrée en vigueur du règlement, la Commission publie au *Journal officiel de l'Union européenne* la liste des systèmes d'identification électronique qui ont été notifiés conformément au paragraphe 1, ainsi que les informations essentielles à leur sujet.

3. Si la Commission reçoit une notification après expiration du délai visé au paragraphe 2, elle modifie la liste dans les trois mois qui suivent.

4. La Commission peut définir, au moyen d'actes d'exécution, les circonstances, les formats et procédures de la notification visée aux paragraphes 1 et 3. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

Article 8

Coordination

1. Les États membres coopèrent en vue d'assurer l'interopérabilité des moyens d'identification électronique relevant d'un régime notifié et de renforcer leur sécurité.

2. La Commission arrête, au moyen d'actes d'exécution, les modalités nécessaires pour faciliter la coopération entre les États membres visée au paragraphe 1, en vue d'assurer un niveau élevé de confiance et de sécurité correspondant au degré de risque. Ces actes d'exécution concernent notamment l'échange d'informations, d'expériences et de bonnes pratiques en matière de systèmes d'identification électronique, l'évaluation par les pairs des systèmes d'identification électronique notifiés et l'examen, par les autorités compétentes des États membres, des nouveaux éléments pertinents dans le secteur de l'identification électronique. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

3. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, concernant la fixation d'exigences techniques minimales visant à faciliter l'interopérabilité transnationale des moyens d'identification électronique.

CHAPITRE III

SERVICES DE CONFIANCE

Section 1

Dispositions générales

Article 9

Responsabilité

1. Un prestataire de service de confiance est responsable des dommages directs causés à toute personne physique ou morale en raison d'un manquement aux obligations énoncées à l'article 15, paragraphe 1, sauf s'il peut prouver qu'il n'a pas agi avec négligence.

2. Un prestataire de service de confiance qualifié est responsable des dommages directs causés à toute personne physique ou morale en raison d'un non-respect des exigences énoncées dans le présent règlement, notamment à l'article 19, sauf s'il peut prouver qu'il n'a pas agi avec négligence.

Article 10

Prestataires de services de confiance provenant de pays tiers

1. Les services de confiance qualifiés et les certificats qualifiés fournis par des prestataires de services de confiance qualifiés établis dans un pays tiers sont acceptés comme étant des services de confiance qualifiés et des certificats qualifiés fournis par des prestataires de services de confiance qualifiés établis sur le territoire de l'Union européenne si les services de confiance qualifiés ou les certificats qualifiés provenant du pays tiers sont reconnus en vertu d'un accord conclu entre l'Union et des pays tiers ou des organisations internationales conformément à l'article 218 du TFUE.

2. En ce qui concerne le paragraphe 1, ces accords garantissent que les exigences applicables aux services de confiance qualifiés et aux certificats qualifiés fournis par des prestataires de services de confiance qualifiés établis sur le territoire de l'Union européenne sont respectées par les prestataires de services de confiance dans les pays tiers ou par les organisations internationales, notamment pour ce qui est de la protection des données à caractère personnel, la sécurité et le contrôle.

Article 11

Traitement et analyse des données

1. Lorsqu'ils traitent des données à caractère personnel, les prestataires de services de confiance et les organes de contrôle veillent au traitement loyal et licite des données conformément à la directive 95/46/CE.

2. Les prestataires de services de confiance traitent les données à caractère personnel conformément à la directive 95/46/CE. Ce traitement est strictement limité aux données minimales nécessaires pour délivrer et tenir à jour un certificat ou pour fournir un service de confiance.

3. Les prestataires de services de confiance garantissent la confidentialité et l'intégrité des données relatives au bénéficiaire d'un service de confiance.

4. Sans préjudice des effets juridiques donnés aux pseudonymes en vertu du droit national, les États membres ne peuvent empêcher les prestataires de services de confiance d'indiquer, dans les certificats de signature électronique, un pseudonyme à la place du nom du signataire.

Article 12

Accessibilité pour les personnes handicapées

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

Section 2

Contrôle

Article 13

Organe de contrôle

1. Les États membres désignent un organe approprié établi sur leur territoire ou, moyennant accord mutuel, dans un autre État membre sous la responsabilité de l'État membre qui a procédé à la désignation. Les organes de contrôle sont investis de tous les pouvoirs de contrôle et d'enquête nécessaires à l'exercice de leurs tâches.

2. L'organe de contrôle est responsable de l'exécution des tâches suivantes:

(a) surveiller les prestataires de services de confiance établis sur le territoire de l'État membre qui a procédé à la désignation afin d'assurer qu'ils satisfont aux exigences énoncées à l'article 15;

(b) assurer le contrôle des prestataires de services de confiance qualifiés établis sur le territoire de l'État membre qui a procédé à la désignation ainsi que le contrôle des services de confiance qualifiés qu'ils fournissent afin d'assurer que ces prestataires et les services de confiance qualifiés qu'ils fournissent satisfont aux exigences applicables énoncées dans le présent règlement;

(c) veiller à ce que les informations et les données pertinentes visées à l'article 19, paragraphe 2, point g), et enregistrées par des prestataires de services de confiance qualifiés soient préservées et restent accessibles après que les activités d'un prestataire de service de confiance qualifié ont cessé, afin de garantir la continuité du service.

3. Chaque organe de contrôle soumet chaque année à la Commission et aux États membres, avant la fin du premier trimestre de l'année suivante, un rapport sur les activités de contrôle de la dernière année civile. Ce rapport comprend au moins:

(a) des informations sur ses activités de contrôle;

(b) un résumé des notifications d'atteinte à la sécurité reçues de prestataires de services de confiance, conformément à l'article 15, paragraphe 2;

(c) des statistiques sur le marché et l'utilisation des services de confiance qualifiés, y compris des informations sur les prestataires de services de confiance qualifiés eux-mêmes, sur les services de confiance qualifiés qu'ils fournissent et sur les produits qu'ils utilisent, ainsi que la description générale de leurs clients.

4. Les États membres notifient à la Commission et aux autres États membres le nom et l'adresse de l'organisme de contrôle qu'ils ont désigné.

5. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition de procédures applicables aux tâches visées au paragraphe 2.

6. La Commission peut définir, au moyen d'actes d'exécution, les circonstances, les formats et procédures aux fins du rapport visé au paragraphe 3. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

Article 14

Assistance mutuelle

1. Les organes de contrôle coopèrent en vue d'échanger des bonnes pratiques et, dans les meilleurs délais, de se communiquer toute information utile et de se prêter une assistance mutuelle afin que les activités puissent être exécutées de façon cohérente. L'assistance mutuelle couvre notamment les demandes d'informations et les mesures de contrôle, telles que les demandes de procéder à des inspections liées aux audits de sécurité visés aux articles 15, 16 et 17.

2. Un organe de contrôle saisi d'une demande d'assistance ne peut refuser d'y donner suite, à moins:

(a) qu'il ne soit pas compétent pour traiter la demande; ou

(b) qu'il soit incompatible avec le présent règlement de donner suite à la demande.

3. Le cas échéant, les organes de contrôle peuvent mener des enquêtes conjointes faisant intervenir des membres des organes de contrôle d'autres États membres.

L'organe de contrôle de l'État membre dans lequel doit avoir lieu l'enquête peut, dans le respect de sa législation nationale, déléguer des missions d'enquête au personnel de l'organe de contrôle qui reçoit l'assistance. Ces compétences ne peuvent être exercées qu'en présence du personnel de l'organe de contrôle d'accueil et sous son autorité. Le personnel de l'organe de contrôle qui reçoit l'assistance est soumis au droit national de l'organe de contrôle d'accueil. L'organe de contrôle d'accueil assume la responsabilité des actes de l'organe de contrôle qui reçoit l'assistance.

4. La Commission peut, au moyen d'actes d'exécution, préciser les formats et les procédures aux fins de l'assistance mutuelle prévue par le présent article. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

Article 15

Exigences de sécurité applicables aux prestataires de services de confiance

1. Les prestataires de services de confiance qui sont établis sur le territoire de l'Union prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu de l'état de la technique, ces mesures garantissent que le niveau de sécurité est adapté au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences des incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tout incident.

Sans préjudice de l'article 16, paragraphe 1, tout prestataire de service de confiance peut soumettre à l'organe de contrôle le rapport d'un audit de sécurité effectué par un organisme indépendant reconnu afin de confirmer que les mesures de sécurité appropriées ont été prises.

2. Les prestataires de services de confiance notifient, sans retard indu et si possible dans un délai de vingt-quatre heures après s'en être aperçus, à l'organe de contrôle compétent, à l'organisme national compétent en matière de sécurité de l'information ainsi qu'à d'autres tiers concernés, tels que les autorités chargées 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 et sur les données à caractère personnel qui y sont liées.

Le cas échéant, notamment lorsqu'une atteinte à la sécurité ou une perte d'intégrité concerne plusieurs États membres, l'organe de contrôle concerné informe les organes de contrôle des autres États membres ainsi que l'Agence chargée de la sécurité des réseaux et de l'information (ENISA).

L'organe de contrôle concerné peut également informer le public ou exiger du prestataire de service de confiance qu'il le fasse, dès lors qu'il constate qu'il est d'utilité publique de divulguer les faits.

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

4. Afin de mettre en œuvre les paragraphes 1 et 2, l'organe de contrôle compétent a le pouvoir de donner des instructions contraignantes aux prestataires de services de confiance.

5. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition plus précise des mesures visées au paragraphe 1.

6. La Commission peut définir, au moyen d'actes d'exécution, les circonstances, les formats et procédures, y compris les délais, aux fins des paragraphes 1 à 3. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

Article 16

Contrôle des prestataires de services de confiance qualifiés

1. Les prestataires de services de confiance qualifiés font l'objet chaque année d'un audit effectué par un organisme indépendant reconnu aux fins de confirmer que les prestataires et les services de confiance qualifiés qu'ils fournissent remplissent les obligations énoncées dans le présent règlement, et transmettent le rapport de l'audit de sécurité à l'organe de contrôle.

2. Sans préjudice des dispositions du paragraphe 1, l'organe de contrôle peut à tout moment, de sa propre initiative ou à la demande de la Commission, soumettre les prestataires de

services de confiance qualifiés à un audit aux fins de confirmer que les prestataires et les services de confiance qualifiés qu'ils fournissent remplissent toujours les obligations énoncées dans le présent règlement. L'organe de contrôle informe les autorités chargées de la protection des données des résultats de ses contrôles lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées.

3. L'organe de contrôle a le pouvoir de donner des instructions contraignantes aux prestataires de services de confiance qualifiés en vue de corriger tout manquement aux obligations constaté dans le rapport de l'audit de sécurité.

4. En ce qui concerne le paragraphe 3, si le prestataire de service de confiance qualifié ne corrige pas ce manquement dans un délai fixé par l'organe de contrôle, il perd son statut qualifié et il est informé par l'organe de contrôle que son statut sera modifié en conséquence dans les listes de confiance visées à l'article 18.

5. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition des conditions de reconnaissance de l'organisme indépendant chargé d'effectuer l'audit de sécurité visé au paragraphe 1 du présent article, à l'article 15, paragraphe 1, et à l'article 17, paragraphe 1.

6. La Commission peut définir, au moyen d'actes d'exécution, les circonstances, les procédures, et les formats applicables aux fins des paragraphes 1, 2 et 4. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

Article 17

Ouverture d'un service de confiance qualifié

1. Les prestataires de services de confiance qualifiés notifient à l'organe de contrôle leur intention de commencer à offrir un service de confiance qualifié et lui présentent un rapport de l'audit de sécurité effectué par un organisme indépendant reconnu, conformément à l'article 16, paragraphe 1. Les prestataires de services de confiance qualifiés peuvent commencer à fournir le service de confiance qualifié après avoir soumis la notification et le rapport de l'audit de sécurité à l'organe de contrôle.

2. Une fois que les documents utiles ont été présentés à l'organe de contrôle conformément au paragraphe 1, les prestataires de services de confiance qualifiés sont inscrits sur les listes de confiance visées à l'article 18, mentionnant que la notification a été introduite.

3. L'organe de contrôle vérifie que le prestataire de service de confiance qualifié et les services de confiance qualifiés qu'il fournit respectent les exigences du règlement.

Si la vérification est concluante, l'organe de contrôle indique le statut qualifié des prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent sur les listes de confiance, dans un délai d'un mois à compter de la notification effectuée conformément au paragraphe 1.

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

4. Un service de confiance qualifié ayant fait l'objet de la notification visée au paragraphe 1 ne peut être refusé pour l'accomplissement d'une procédure ou d'une formalité administrative par l'organisme public concerné au motif qu'il ne figure pas sur les listes visées au paragraphe 3.

5. La Commission peut définir, au moyen d'actes d'exécution, les circonstances, les formats et les procédures applicables aux fins des paragraphes 1, 2 et 3. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

Article 18

Listes de confiance

1. Chaque État membre établit, tient à jour et publie des listes de confiance contenant des informations relatives aux prestataires de services de confiance qualifiés pour lesquels il est compétent, 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 automatique, les listes de confiance visées au paragraphe 1 portant une signature électronique ou un cachet électronique.

3. Les États membres communiquent à la Commission, sans retard indu, les 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 le certificat utilisé pour apposer la signature électronique ou le cachet électronique 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 adaptée au traitement automatique et portant une signature électronique ou un cachet électronique.

5. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition des informations visées au paragraphe 1.

6. La Commission peut définir, au moyen d'actes d'exécution, les spécifications techniques et les formats applicables aux listes de confiance aux fins des paragraphes 1 à 4. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

Article 19

Exigences applicables aux prestataires de services de confiance qualifiés

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

Ces informations sont vérifiées par le prestataire de service de confiance qualifié ou par un tiers agréé agissant sous sa responsabilité:

(a) lorsque la personne physique ou un mandataire de la personne morale se présente en personne, ou

(b) à distance, à l'aide de moyens d'identification électronique relevant d'un système notifié délivrés en conformité avec le point a).

2. Les prestataires de services de confiance qualifiés qui fournissent des services de confiance qualifiés:

(a) emploient du personnel qui possède l'expertise, l'expérience et les qualifications nécessaires, applique des procédures administratives et de gestion correspondant à des normes européennes ou internationales et a reçu une formation appropriée concernant les règles en matière de sécurité et de protection des données à caractère personnel;

(b) endossent la responsabilité des dommages en maintenant des ressources financières suffisantes ou en ayant un système d'assurance responsabilité approprié;

(c) avant d'établir une relation contractuelle, informent toute personne désireuse d'utiliser un service de confiance qualifié des conditions précises relatives à l'utilisation de ce service;

(d) utilisent des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et la fiabilité du processus qu'ils prennent en charge;

(e) utilisent des systèmes fiables pour stocker les données qui leur sont fournies, sous une forme vérifiable garantissant que:

– les données ne sont publiquement disponibles pour des recherches qu'avec le consentement de la personne pour laquelle elles ont été publiées,

– seules des personnes autorisées peuvent introduire et modifier les données,

– l'authenticité des informations peut être vérifiée;

(f) prennent des mesures contre la falsification et le vol de données;

(g) enregistrent pour une durée appropriée toutes les informations pertinentes concernant les données publiées et reçues par le prestataire de service de confiance qualifié, aux fins notamment de pouvoir fournir des preuves en justice. Ces enregistrements peuvent être effectués par voie électronique;

(h) ont un plan actualisé en cas de résiliation afin d'assurer la continuité du service conformément aux dispositions formulées par l'organe de contrôle en vertu de l'article 13, paragraphe 2, point c);

(i) assurent le traitement licite des données à caractère personnel conformément à l'article 11.

3. Les prestataires de services de confiance qualifiés qui délivrent des certificats qualifiés enregistrent la révocation d'un certificat dans leur base de données relative aux certificats dans les dix minutes qui suivent la prise d'effet de cette révocation.

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 la révocation des certificats qualifiés qu'ils ont délivrés. Ces informations sont disponibles à tout moment pour chaque certificat au moins, de manière automatique, 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. Les systèmes et les produits fiables sont présumés satisfaire aux exigences énoncées à l'article 19 lorsqu'ils respectent ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Section 3

Signature électronique

Article 20

Effets juridiques et acceptation des signatures électroniques

1. L'efficacité juridique et la recevabilité comme preuve en justice ne peuvent être refusées à une signature électronique au seul motif qu'elle se présente sous une forme électronique.

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

3. Les signatures électroniques qualifiées sont reconnues et acceptées dans tous les États membres.

4. Si une signature électronique offrant un niveau de garantie de sécurité inférieur à celui de la signature électronique qualifiée est requise, dans le cas notamment où un État membre l'exige pour l'accès à un service en ligne offert par un organisme du secteur public sur la base d'une évaluation appropriée des risques liés à un tel service, toutes les signatures électroniques correspondant au moins au même niveau de garantie de sécurité sont reconnues et acceptées.

5. Les États membres n'exigent pas, pour l'accès transnational à un service en ligne offert par un organisme du secteur public, de signature électronique présentant un niveau de garantie de sécurité supérieur à celui d'une signature électronique qualifiée.

6. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition des différents niveaux de sécurité des signatures électroniques visés au paragraphe 4.

7. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux niveaux de sécurité des signatures électroniques. Une signature électronique est présumée garantir le niveau de sécurité défini dans un acte délégué adopté en vertu du paragraphe 6 lorsqu'elle respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Article 21

Certificats qualifiés de signature électronique

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

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

3. Si un certificat qualifié de signature électronique a été révoqué après la première activation, il perd sa validité et un renouvellement de sa validité ne peut en aucun cas le faire recouvrer son statut antérieur.

4. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition plus précise des exigences énoncées à l'annexe I.

5. 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 énoncées à l'annexe I lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Article 22

Exigences applicables aux dispositifs de création de signature électronique qualifiés

1. Les dispositifs de création de signature électronique qualifiés respectent les exigences énoncées 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 énoncées à l'annexe II lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Article 23

Certification des dispositifs de création de signature électronique qualifiés

1. Les dispositifs de création de signature électronique qualifiés peuvent être certifiés par les organismes publics ou privés compétents désignés par les États membres, à condition d'avoir fait l'objet d'un processus d'évaluation de la sécurité conformément à l'une des normes relatives à l'évaluation de la sécurité des produits informatiques figurant sur une liste qui sera établie par la Commission au moyen d'actes d'exécution. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

2. Les États membres notifient à la Commission et aux autres États membres le nom et l'adresse de l'organisme public ou privé, visé au paragraphe 1, qu'ils ont désigné.

3. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition de critères spécifiques que doivent respecter les organismes désignés visés au paragraphe 1.

Article 24

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

1. Les États membres notifient à la Commission, sans retard indu, les dispositifs de création de signature électronique qualifiés qui ont été certifiés par les organismes visés à l'article 23. Ils notifient également à la Commission, sans retard indu, les dispositifs de création de signature électronique qui ne seraient 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 qui sont certifiés.

3. La Commission peut définir, au moyen d'actes d'exécution, les circonstances, les formats et les procédures applicables aux fins du paragraphe 1. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

Article 25

Exigences applicables à la validation des signatures électroniques qualifiées

1. Une signature électronique qualifiée est considérée comme valable s'il peut être établi avec une grande certitude qu'au moment de la signature:

(a) le certificat sur lequel repose la signature est un certificat qualifié de signature électronique conforme aux dispositions prévues à l'annexe I;

(b) le certificat qualifié requis est authentique et valable;

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

(d) l'ensemble de données représentant le signataire sans ambiguïté est correctement fourni à la partie utilisatrice;

(e) l'utilisation d'un pseudonyme est clairement indiquée à la partie utilisatrice, si tel est le cas;

(f) la signature électronique a été créée par un dispositif de création de signature électronique qualifié;

(g) l'intégrité des données signées n'a pas été compromise;

(h) les exigences prévues à l'article 3, point 7, sont satisfaites;

(i) le système utilisé pour valider la signature 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.

2. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition plus précise des exigences énoncées au paragraphe 1.

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 énoncées au paragraphe 1 lorsqu'elle respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Article 26

Service de validation qualifié des signatures électroniques qualifiées

1. Un prestataire de service de confiance qualifié fournit un service de validation qualifié des signatures électroniques qualifiées lorsqu'il:

(a) fournit une validation en conformité avec les dispositions de l'article 25, 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 des signatures électroniques qualifiées est présumé satisfaire aux exigences énoncées au paragraphe 1, point b), lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Article 27

Conservation des signatures électroniques qualifiées

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

2. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition plus précise des exigences énoncées au paragraphe 1.

3. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables à la conservation des signatures électroniques qualifiées. La

conservation des signatures électroniques qualifiées est présumée satisfaire aux exigences énoncées au paragraphe 1 lorsqu'elle respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Section 4

Cachets électroniques

Article 28

Effets juridiques des cachets électroniques

1. L'efficacité juridique et la recevabilité comme preuve en justice ne peuvent être refusées à un cachet électronique au seul motif qu'il se présente sous une forme électronique.

2. Un cachet électronique qualifié bénéficie d'une présomption légale quant à la garantie de l'origine et de l'intégrité des données auxquelles il est lié.

3. Un cachet électronique qualifié est reconnu et accepté dans tous les États membres.

4. Si un cachet électronique offrant un niveau de garantie de sécurité inférieur à celui du cachet électronique qualifié est requis, dans le cas notamment où un État membre l'exige pour l'accès à un service en ligne offert par un organisme du secteur public sur la base d'une évaluation appropriée des risques liés à un tel service, tous les cachets électroniques correspondant au moins au même niveau de garantie de sécurité sont reconnus et acceptés.

5. Les États membres n'exigent pas, pour l'accès à un service en ligne offert par un organisme du secteur public, de cachet électronique présentant un niveau de garantie de sécurité supérieur à celui des cachets électroniques qualifiés.

6. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition des différents niveaux de garantie de sécurité des cachets électroniques visés au paragraphe 4.

7. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux niveaux de garantie de sécurité des cachets électroniques. Un cachet électronique est présumé garantir le niveau de sécurité défini dans un acte délégué adopté en vertu du paragraphe 6 lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Article 29

Exigences applicables aux certificats qualifiés de cachet électronique

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

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

3. Si un certificat qualifié de cachet électronique a été révoqué après la première activation, il perd sa validité et un renouvellement de sa validité ne peut en aucun cas le faire recouvrer son statut antérieur.

4. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition plus précise des exigences énoncées à l'annexe III.

5. 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 énoncées à l'annexe III lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Article 30

Dispositifs de création de cachet électronique qualifiés

1. L'article 22 s'applique *mutatis mutandis* aux exigences applicables aux dispositifs de création de cachet électronique qualifiés.

2. L'article 23 s'applique *mutatis mutandis* à la certification des dispositifs de création de cachet électronique qualifiés.

3. L'article 24 s'applique *mutatis mutandis* à la publication d'une liste de dispositifs de création de cachet électronique qualifiés.

Article 31

Validation et conservation des cachets électroniques qualifiés

Les articles 25, 26 et 27 s'appliquent *mutatis mutandis* à la validation et à la conservation des cachets électroniques qualifiés.

Section 5

Horodatage électronique

Article 32

Effet juridique des horodatages électroniques

1. L'efficacité juridique et la recevabilité comme preuve en justice ne peuvent être refusées à un horodatage électronique au seul motif qu'il se présente sous une forme électronique.

2. Un horodatage électronique qualifié bénéficie d'une présomption légale quant à la garantie de l'instant indiqué et de l'intégrité des données auxquelles se rapporte cet instant.

3. Un horodatage électronique qualifié est reconnu et accepté dans tous les États membres.

Article 33

Exigences applicables aux horodatages électroniques qualifiés

1. Un horodatage électronique qualifié satisfait aux exigences suivantes:

(a) il est lié avec exactitude au temps universel coordonné (TUC) de manière à exclure toute possibilité de modification indétectable des données;

(b) il est basé sur une horloge exacte;

(c) il est délivré par un prestataire de service de confiance qualifié;

(d) il est signé au moyen d'une signature électronique avancée ou d'un cachet électronique avancé du prestataire de service 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'exactitude du lien entre instant et données et l'exactitude de l'horloge. L'exactitude du lien entre instant et données et l'exactitude de l'horloge sont présumées satisfaire aux exigences énoncées au paragraphe 1 lorsqu'elles respectent ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Section 6

Documents électroniques

Article 34

Effets juridiques et acceptation des documents électroniques

1. Un document électronique est considéré comme équivalent à un document imprimé et recevable comme preuve en justice, compte tenu du niveau de garantie de son authenticité et de son intégrité.

2. Un document portant une signature électronique qualifiée ou un cachet électronique qualifié de la personne compétente pour délivrer le document pertinent bénéficie d'une présomption légale quant à son authenticité et à son intégrité à condition que le document ne contienne pas de caractéristiques dynamiques susceptibles de le modifier automatiquement.

3. Lorsqu'il est exigé un document original ou une copie certifiée pour la fourniture d'un service en ligne offert par un organisme du secteur public, les documents électroniques qui sont délivrés par les personnes compétentes pour délivrer les documents imprimés correspondants et qui sont considérés comme des originaux ou des copies certifiées en vertu du droit national de l'État membre d'origine doivent au moins être acceptés dans les autres États membres sans exigence supplémentaire.

4. La Commission peut définir, au moyen d'actes d'exécution, les formats des signatures électroniques et des cachets électroniques qui sont acceptés lorsqu'un État membre exige, pour la fourniture d'un service en ligne offert par un organisme du secteur public, un document signé ou cacheté visé au paragraphe 2. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2.

Section 7

Service de fourniture électronique qualifié

Article 35

Effet juridique d'un service de fourniture électronique

1. Les données envoyées ou reçues à l'aide d'un service de fourniture électronique sont recevables comme preuves en justice en ce qui concerne l'intégrité des données et l'exactitude de la date et l'heure à laquelle les données ont été envoyées ou reçues par un destinataire déterminé.

2. Les données envoyées ou reçues au moyen d'un service de fourniture électronique qualifié bénéficient d'une présomption légale quant à l'intégrité des données et à l'exactitude de la date et de l'heure indiquées par le service de fourniture électronique qualifié concernant l'envoi ou la réception des données.

3. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition de mécanismes permettant l'envoi ou la réception de données au moyen de services de fourniture électronique, qui sont utilisés en vue de favoriser l'interopérabilité entre les services de fourniture électronique.

Article 36

Exigences applicables aux services de fourniture électronique qualifiés

1. Les services de fourniture électronique qualifiés satisfont aux exigences suivantes:

(a) ils doivent être fournis par un ou plusieurs prestataires de services de confiance qualifiés;

(b) ils doivent permettre l'identification univoque de l'expéditeur et, le cas échéant, du destinataire;

(c) le processus d'envoi ou de réception de données doit être garanti par une signature électronique avancée ou par un cachet électronique avancé du prestataire de service de confiance qualifié de manière à exclure toute possibilité de modification indétectable des données;

(d) toute modification des données nécessaire pour l'envoi ou la réception de celles-ci doit être clairement signalée à l'expéditeur et au destinataire des données;

(e) la date d'envoi, de réception et toute modification des données doivent être indiquées par un horodatage électronique qualifié;

(f) si les données sont transférées entre deux prestataires de services de confiance qualifiés ou plus, les exigences fixées aux points a) à e) 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 énoncées au paragraphe 1 lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

Section 8

Authentification de site Web

Article 37

Exigences applicables aux certificats qualifiés d'authentification de site Web

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

2. Les certificats qualifiés d'authentification de site Web sont reconnus et acceptés dans tous les États membres.

3. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, en ce qui concerne la définition plus précise des exigences énoncées à l'annexe IV.

4. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux certificats qualifiés d'authentification de site Web. Un certificat qualifié d'authentification de site Web est présumé satisfaire aux exigences énoncées à l'annexe IV lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 39, paragraphe 2. La Commission publie ces mesures au *Journal officiel de l'Union européenne*.

CHAPITRE IV

ACTES DÉLÉGUÉS

Article 38

Exercice de la délégation

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

2. Le pouvoir d'adopter des actes délégués visé à l'article 8, paragraphe 3, à l'article 13, paragraphe 5, à l'article 15, paragraphe 5, à l'article 16, paragraphe 5, à l'article 18, paragraphe 5, à l'article 20, paragraphe 6, à l'article 21, paragraphe 4, à l'article 23, paragraphe 3, à l'article 25, paragraphe 2, à l'article 27, paragraphe 2, à l'article 28, paragraphe 6, à l'article 29, paragraphe 4, à l'article 30, paragraphe 2, à l'article 31, à l'article 35, paragraphe 3, et à l'article 37, paragraphe 3, est conféré à la Commission pour une durée indéterminée à compter de l'entrée en vigueur du présent règlement.

3. La délégation de pouvoir visée à l'article 8, paragraphe 3, à l'article 13, paragraphe 5, à l'article 15, paragraphe 5, à l'article 16, paragraphe 5, à l'article 18, paragraphe 5, à l'article 20, paragraphe 6, à l'article 21, paragraphe 4, à l'article 23, paragraphe 3, à l'article 25, paragraphe 2, à l'article 27, paragraphe 2, à l'article 28, paragraphe 6, à l'article 29, paragraphe 4, à l'article 30, paragraphe 2, à l'article 31, à l'article 35, paragraphe 3, et à l'article 37, paragraphe 3, peut être révoquée à tout moment par le Parlement européen ou par le Conseil. La décision de révocation met un terme à la délégation du pouvoir qui y est spécifié. 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 n'affecte pas la validité des actes délégués déjà en vigueur.

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

5. Un acte délégué adopté en vertu de l'article 8, paragraphe 3, de l'article 13, paragraphe 5, de l'article 15, paragraphe 5, de l'article 16, paragraphe 5, de l'article 18, paragraphe 5, de l'article 20, paragraphe 6, de l'article 21, paragraphe 4, de l'article 23, paragraphe 3, de l'article 25, paragraphe 2, de l'article 27, paragraphe 2, de l'article 28, paragraphe 6, de l'article 29, paragraphe 4, de l'article 30, paragraphe 2, de l'article 31, de l'article 35, paragraphe 3, et de l'article 37, paragraphe 3, n'entre en vigueur que s'il n'a donné lieu à aucune objection du Parlement européen ou du Conseil dans un délai de deux mois à compter de sa notification à ces deux institutions 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 formuler d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

CHAPITRE V

ACTES D'EXÉCUTION

Article 39

Procédure de comité

1. La Commission est assistée par un comité. Il s'agit d'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 40

Rapport

La Commission rend compte au Parlement européen et au Conseil de l'application du présent règlement. Le premier rapport est présenté au plus tard quatre ans après l'entrée en vigueur du présent règlement. Les rapports suivants sont ensuite présentés tous les quatre ans.

Article 41

Abrogation

1. La directive 1999/93/CE est abrogée.

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

3. 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.

4. Les certificats qualifiés délivrés en vertu de la directive 1999/93/CE sont considérés comme des certificats qualifiés de signature électronique au titre du présent règlement jusqu'à leur expiration, cette période ne pouvant cependant pas dépasser cinq ans à compter de l'entrée en vigueur du présent règlement.

Article 42

Entrée en vigueur

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

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*

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 automatique, que le certificat est délivré comme certificat qualifié de signature électronique;

(b) un ensemble de données représentant sans ambiguïté le prestataire de service 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 numéro d'immatriculation tels qu'ils figurent dans les registres officiels;
- pour une personne physique: le nom de la personne

(c) un ensemble de données représentant sans ambiguïté le signataire à qui le certificat est délivré, comprenant au moins le nom du signataire ou un pseudonyme qui est identifié comme tel;

(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 service de confiance qualifié;

(g) la signature électronique avancée ou le cachet électronique avancé du prestataire de service 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 de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié;

(j) le cas échéant, une mention indiquant, au moins sous une forme adaptée au traitement automatique, que 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.

ANNEXE II

Exigences applicables aux dispositifs de création de signature électronique qualifiés

1. Les dispositifs de création de signature électronique qualifiés doivent au moins garantir, par les moyens techniques et procédures appropriés, que:

(a) la confidentialité des données de création de signature électronique utilisées pour générer la signature électronique est assurée;

(b) les données de création de signature électronique utilisées pour générer la signature électronique ne peuvent être établies plus d'une fois;

(c) l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour générer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification par les moyens techniques actuellement disponibles;

(d) les données de création de signature électronique utilisées pour générer une 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 soumission 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 est confiée à un prestataire de service de confiance qualifié.

4. Un prestataire de service de confiance qualifié gérant des données de création de signature électronique pour le compte d'un signataire peut reproduire les données de création de signature électronique à des fins de sauvegarde sous réserve du respect des conditions suivantes:

(a) le niveau de sécurité des ensembles de données reproduits est 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 automatique, que le certificat est délivré comme certificat qualifié de cachet électronique;

(b) un ensemble de données représentant sans ambiguïté le prestataire de service 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 numéro d'immatriculation tels qu'ils figurent dans les registres officiels;
- pour une personne physique: le nom de la personne;

(c) un ensemble de données représentant sans ambiguïté la personne morale à qui le certificat est délivré, comprenant au moins son nom et 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 service de confiance qualifié;

(g) la signature électronique avancée ou le cachet électronique avancé du prestataire de service 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 de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié;

(j) le cas échéant, une mention indiquant, au moins sous une forme adaptée au traitement automatique, que 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.

ANNEXE IV

Exigences relatives aux certificats qualifiés d'authentification de site Web

Les certificats qualifiés d'authentification de site Web contiennent:

(a) une mention indiquant, au moins sous une forme adaptée au traitement automatique, que le certificat est délivré comme certificat qualifié d'authentification de site Web;

(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 numéro d'immatriculation tels qu'ils figurent dans les registres officiels;
- pour une personne physique: le nom de la personne;

(c) un ensemble de données représentant sans ambiguïté la personne morale à qui le certificat est délivré, comprenant au moins son nom et son numéro d'immatriculation tels qu'ils figurent dans les registres officiels;

(d) des éléments de l'adresse comprenant au moins la ville et l'État membre de la personne morale à qui le certificat est délivré, tels qu'ils figurent dans les registres officiels;

(e) le(s) nom(s) de domaine exploité(s) par la personne morale à qui 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 service de confiance qualifié;

(h) la signature électronique avancée ou le cachet électronique avancé du prestataire de service de confiance qualifié délivrant le certificat;

(i) l'endroit où peut être obtenu gratuitement le certificat sur lequel repose la signature électronique avancée ou le cachet électronique avancé mentionnés 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.

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

La présente fiche financière présente en détail les exigences à satisfaire en termes de dépenses administratives afin de mettre en œuvre la proposition de règlement sur *l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.*

À l'issue de la procédure législative et des débats pour l'adoption du règlement proposé par le Conseil et le Parlement européen, la Commission aura besoin de douze équivalents temps plein pour élaborer les actes délégués et les actes d'exécution correspondants, pour garantir la disponibilité des normes organisationnelles et techniques, pour traiter les informations notifiées par les États membres, et notamment pour tenir à jour les informations liées aux listes de confiance, pour sensibiliser les parties intéressées - et notamment les citoyens et les PME - aux avantages associés à l'utilisation de l'identification, de l'authentification et des signatures électroniques et des services de confiance associés (services eIAS) et pour engager un dialogue avec les pays tiers afin d'assurer l'interopérabilité des eIAS au niveau mondial.

1.1. Dénomination de la proposition/de l'initiative

Proposition de la Commission relative à un règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

1.2. Domaine(s) politique(s) concerné(s) dans la structure ABM/ABB[25]

09 SOCIÉTÉ DE L'INFORMATION

1.3. Nature de la proposition/de l'initiative

☐ La proposition/l'initiative porte sur une **action nouvelle**

☐ La proposition/l'initiative porte sur une **action nouvelle suite à un projet pilote/une action préparatoire**[26]

☐ La proposition/l'initiative est relative à la **prolongation d'une action existante**

☑ La proposition/l'initiative porte sur **une action réorientée vers une nouvelle action**

[25] ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

[26] Tel que visé à l'article 49, paragraphe 6, point a) ou b), du règlement financier.

1.4. Objectifs

1.4.1. Objectif(s) stratégique(s) pluriannuel(s) de la Commission visé(s) par la proposition/l'initiative

Les objectifs généraux de la proposition sont ceux des politiques générales de l'UE dans lesquelles s'inscrit la proposition, telles que la stratégie Europe 2020. Cette dernière vise à faire de l'UE une «économie intelligente, durable et inclusive avec des niveaux d'emploi, de productivité et de cohésion sociale élevés».

1.4.2. Objectif(s) spécifique(s) et activité(s) ABM/ABB concernée(s)

Susciter une confiance accrue dans les transactions électroniques paneuropéennes et garantir la reconnaissance juridique transnationale de l'identification, de l'authentification et des signatures électroniques et des services de confiance associés ainsi qu'un niveau élevé de protection des données et de responsabilisation des utilisateurs dans le marché unique (voir les actions clés 3 et 16 de la stratégie numérique pour l'Europe).

Activité(s) ABM/ABB concernée(s)

09 02 – Cadre réglementaire de la stratégie numérique pour l'Europe

1.4.3. Résultat(s) et incidence(s) attendu(s)

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

Établir, pour les services eIAS, un environnement réglementaire sans ambiguïté qui faciliterait la tâche aux utilisateurs et susciterait une confiance accrue dans le monde numérique.

1.4.4. Indicateurs de résultats et d'incidences

Préciser les indicateurs permettant de suivre la réalisation de la proposition/de l'initiative.

1. existence de fournisseurs eIAS qui exercent des activités dans plusieurs États membres de l'UE;

2. niveau d'interopérabilité atteint par les dispositifs (lecteurs de cartes à puce, par exemple) entre les secteurs et les pays;

3. utilisation des eIAS par toutes les catégories de la population;

4. degré d'utilisation des eIAS par les utilisateurs finaux pour les transactions nationales et internationales (transnationales);

5. degré d'harmonisation entre les États membres en ce qui concerne la législation relative aux eIAS;

6. systèmes d'identification électronique notifiés à la Commission;

7. services accessibles au moyen d'identifications électroniques notifiées dans le secteur public (administration en ligne, santé en ligne, justice en ligne, marchés publics en ligne);

8. services accessibles à l'aide de moyens d'identification électronique notifiés dans le secteur privé (services bancaires en ligne, commerce en ligne, jeux d'argent en ligne, accès à des sites web, services internet plus sûrs).

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme

Les divergences dans la mise en œuvre de la directive sur les signatures électroniques au niveau national dues à des différences d'interprétation par les États membres causent des problèmes d'interopérabilité transnationale qui finissent par conduire à une situation fragmentée dans l'UE et à des distorsions dans le marché intérieur. Elles s'accompagnent d'un manque de confiance dans les systèmes électroniques qui empêche les citoyens européens de bénéficier des mêmes services dans l'environnement numérique que dans le monde réel.

1.5.2. Valeur ajoutée de l'intervention de l'UE

Une action au niveau de l'UE procurerait des avantages évidents par rapport à des mesures au niveau des États membres. L'expérience a montré que non seulement les mesures nationales ne suffisent pas à rendre possibles les transactions électroniques transnationales mais qu'elles ont au contraire créé des obstacles à l'interopérabilité des signatures électroniques au niveau de l'UE et qu'elles produisent actuellement le même effet sur l'identification et l'authentification électroniques et les services de confiance associés.

1.5.3. Leçons tirées d'expériences similaires

La proposition est fondée sur l'expérience acquise avec la directive sur les signatures électroniques, dont les objectifs n'ont pas pu être atteints en raison d'une transposition et d'une mise en œuvre fragmentées.

1.5.4. Compatibilité et synergie éventuelle avec d'autres instruments appropriés

Plusieurs autres grandes initiatives de l'UE visant à éliminer les problèmes d'interopérabilité et de reconnaissance transnationale liés à certains types d'interactions électroniques, telles que la directive sur les services, les directives sur les marchés publics, la directive révisée sur la TVA (factures électroniques) ou le règlement sur l'initiative citoyenne européenne, font référence à la directive sur les signatures électroniques.

Par ailleurs, le règlement proposé établira un cadre juridique propice à l'adoption généralisée des projets pilotes à grande échelle qui ont été mis en place au niveau de l'UE pour soutenir le développement de moyens de communication électronique interopérables et dignes de confiance (notamment l'initiative SPOCS, destinée à appuyer la mise en œuvre de la directive Services; le projet STORK, qui soutient la mise en place et l'utilisation de systèmes d'identification électronique interopérables, l'initiative PEPPOL qui soutient la mise en place et l'utilisation de solutions interopérables en matière de marchés publics en ligne, epSOS, qui soutient la mise en place et l'utilisation de solutions interopérables de santé en ligne et eCodex, qui

soutient la mise en place et l'utilisation de solutions interopérables en matière de justice en ligne).

1.6. Durée et incidence financière

☐ Proposition/initiative à **durée limitée**

– ☐ Proposition/initiative en vigueur à partir de [JJ/MM]AAAA jusqu'en [JJ/MM]AAAA

– ☐ Incidence financière de AAAA jusqu'en AAAA

☑ Proposition/initiative à **durée illimitée**

1.7. Mode(s) de gestion prévu(s[27])

☑ **Gestion centralisée directe** par la Commission

☐ **Gestion centralisée indirecte** par délégation de tâches d'exécution à:

– ☐ des agences exécutives

– ☐ des organismes créés par les Communautés[28]

– ☐ des organismes publics nationaux/organismes avec mission de service public

– ☐ des personnes chargées de l'exécution d'actions spécifiques en vertu du Titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné au sens de l'article 49 du règlement financier

☐ **Gestion partagée** avec les États membres

☐ **Gestion décentralisée** avec des pays tiers

☐ **Gestion conjointe** avec des organisations internationales ***(à préciser***)

Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques»

Remarques

[//]

[27] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_fr.html

[28] Tels que visés à l'article 185 du règlement financier.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

La première évaluation aura lieu quatre ans après l'entrée en vigueur du règlement. Le règlement contient une disposition qui prévoit explicitement que la Commission présentera au Parlement européen et au Conseil un rapport sur son application. Les rapports suivants seront ensuite présentés tous les quatre ans. La Commission appliquera ses méthodes d'évaluation. Ces évaluations seront effectuées à l'aide d'études ciblées relatives à la mise en œuvre des instruments juridiques, de questionnaires adressés aux autorités nationales, de discussions d'experts, d'ateliers, d'enquêtes Eurobaromètre, etc.

2.2. Système de gestion et de contrôle

2.2.1. Risque(s) identifié(s)

Une analyse d'impact a été réalisée et elle accompagne la présente proposition de règlement. Le nouvel instrument juridique assurera la reconnaissance et l'acceptation mutuelles de l'identification électronique dans un contexte transnational, améliorera le cadre actuel relatif aux signatures électroniques, renforcera le contrôle national des prestataires de services de confiance et conférera un effet et une reconnaissance juridiques aux services de confiance associés. Il introduit également le recours à des actes délégués et à des actes d'exécution pour garantir la souplesse vis-à-vis de l'évolution technologique.

2.2.2. Moyen(s) de contrôle prévu(s)

Des méthodes de contrôle existantes appliquées par la Commission couvriront les crédits supplémentaires.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées.

Des mesures de prévention de la fraude existantes appliquées par la Commission couvriront les crédits supplémentaires.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

- Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et ligne budgétaire

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro [Libellé…..….]	CD/CND (29)	de pays AELE[30]	de pays candidats[31]	de pays tiers	au sens de l'article 18, paragraphe 1, point a bis), du règlement financier
5	09. 01 01 01 Dépenses relatives au personnel en activité dans la DG Société de l'information et médias	CND	Non	Non	Non	Non
5	09. 01 02 01 Personnel externe	CND	Non	Non	Non	Non

29 CD = crédits dissociés / CND = crédits non dissociés.
30 AELE: Association européenne de libre-échange.
31 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

3.2. Incidence estimée sur les dépenses

3.2.1. Synthèse de l'incidence estimée sur les dépenses

Rubrique du cadre financier pluriannuel:	Numéro	[Rubrique 1. **Croissance intelligente et inclusive** ……..……]

DG: INFSO			Année **2014**	Année **2015**	Année **2016**	Année **2017**	Année **2018**	**Année 2019**	**Année 2020**	**TOTAL**
• Crédits opérationnels										
Numéro de ligne budgétaire – s.o.	Engagements	(1)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
	Paiements	(2)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
Numéro de ligne budgétaire – s.o.	Engagements	(1a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
	Paiements	(2a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[32]			0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
Numéro de ligne budgétaire		(3)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
TOTAL des crédits Pour la DG INFSO	Engagements	=1+1a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
	Paiements	=2+2a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**

[32] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

Rubrique du cadre financier pluriannuel:	**5**	«Dépenses administratives»

En millions d'euros (à la 3e décimale)

		Année **2014**	Année **2015**	Année **2016**	Année **2017**	Année **2018**	Année **2019**	Année **2020**	**TOTAL**
		DG: INFSO							
• Ressources humaines		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Autres dépenses administratives									
TOTAL DG INFSO	Crédits	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

TOTAL des crédits pour la RUBRIQUE 5 du cadre financier pluriannuel	(Total engagements = Total paiements)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

En millions d'euros (à la 3e décimale)

		Année **2014**	Année **2015**	Année **2016**	Année **2017**	Année **2018**	Année **2019**	Année **2020**	**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 5 du cadre financier pluriannuel	Engagements	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
	Paiements	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

3.2.2. Incidence estimée sur les crédits opérationnels

– ☑ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☐ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

3.2.3. Incidence estimée sur les crédits de nature administrative

3.2.3.1. Synthèse

– ☐ La proposition/initiative n'engendre pas l'utilisation de crédits de nature administrative

– ☑ La proposition/initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En millions d'euros (à la 3e décimale)

	Année **N 2014**	Année **2015**	Année **2016**	Année **2017**	Année **2018**	Année **2019**	Année **2020**	**TOTAL**
RUBRIQUE 5 du cadre financier pluriannuel								
Ressources humaines	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Autres dépenses administratives								
Sous-total RUBRIQUE 5 du cadre financier pluriannuel	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Hors RUBRIQUE 5[33] du cadre financier pluriannuel								
Ressources humaines								
Autres dépenses de nature administrative								
Sous-total hors RUBRIQUE 5 du cadre financier pluriannuel								

TOTAL	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

3.2.3.2. Besoins estimés en ressources humaines

– ☐ La proposition/initiative n'engendre pas l'utilisation de ressources humaines

– ☑ La proposition/initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en valeur entière (ou au plus une décimale)

		Année **2014**	Année **2015**	Année **2016**	Année **2017**	Année **2018**	Année **2019**	Année **2020**
• Emplois du tableau des effectifs (postes de fonctionnaires et d'agents temporaires)								
09 01 01 01 (au siège et dans les bureaux de représentation de la Commission)		9	9	9	9	9	9	9
XX 01 01 02 (en délégation)								
XX 01 05 01 (recherche indirecte)								
10 01 05 01 (recherche directe)								
• Personnel externe (en équivalent temps plein – ETP)[34]								
09 01 02 01 (AC, INT, END de l'enveloppe globale)		3	3	3	3	3	3	3
XX 01 02 02 (AC, INT, JED, AL et END dans les délégations)								
XX 01 04 yy[35]	au siège[36]							
	en délégation							
XX 01 05 02 (AC, INT, END sur recherche indirecte)								
10 01 05 02 (AC, INT, END sur recherche directe)								
Autre ligne budgétaire (à spécifier)								
TOTAL		**12**	**12**	**12**	**12**	**12**	**12**	**12**

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et à la lumière des contraintes budgétaires existantes.

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Gérer les procédures législatives liées à l'adoption du règlement proposé et des actes délégués et actes d'exécution par le Conseil et le Parlement européen. Domaines prioritaires: 1. Établir un nouveau cadre législatif sur les services de confiance électroniques 2. Favoriser l'adoption de services de confiance électroniques en sensibilisant davantage les PME et les particuliers à leur potentiel. 3. Assurer le suivi de la directive 1999/93/CE, notamment en ce qui concerne les aspects internationaux. 4. Exploiter l'effet de levier des projets pilotes à grande échelle pour accélérer la réalisation concrète de l'objectif du nouveau cadre législatif.
Personnel externe	Voir ci-dessus

[34] AC = agent contractuel; INT = intérimaire; JED = jeune expert en délégation. AL= agent local; END = expert national détaché.

[35] Sous-plafond de personnel externe sur crédits opérationnels (anciennes lignes «BA»).

[36] Fonds structurels, Fonds européen agricole pour le développement rural (Feader) et Fonds européen pour la pêche (FEP).

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

– ☑ La proposition/l'initiative est compatible avec la programmation financière existante.

– ☐ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

Expliquez la reprogrammation requise, en précisant les lignes budgétaires concernées et les montants correspondants.

– ☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel[37].

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants.

3.2.5. Participation de tiers au financement

– ☑ La proposition/l'initiative ne prévoit pas de cofinancement par des tierces parties.

– ☐ La proposition/l'initiative prévoit un cofinancement estimé ci-après:

3.3. Incidence estimée sur les recettes

– ☑ La proposition/l'initiative est sans incidence financière sur les recettes.

– ☐ La proposition/l'initiative a une incidence financière décrite ci-après:

- ☐ sur les ressources propres
- ☐ sur les recettes diverses

[37] Voir points 19 et 24 de l'accord interinstitutionnel.