Journal officiel de l'Union européenne

L 235

Édition de langue française

Législation

58e année

9 septembre 2015

Sommaire

[1] Texte présentant de l'intérêt pour l'EEE

FR

Les actes dont les titres sont imprimés en caractères maigres sont des actes de gestion courante pris dans le cadre de la politique agricole et ayant généralement une durée de validité limitée.

Les actes dont les titres sont imprimés en caractères gras et précédés d'un astérisque sont tous les autres actes.

[1] Texte présentant de l'intérêt pour l'EEE

II

(Actes non législatifs)

RÈGLEMENTS

RÈGLEMENT D'EXÉCUTION (UE) 2015/1501 DE LA COMMISSION

du 8 septembre 2015

sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) nº 910/2014 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)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ([1]), et notamment son article 12, paragraphe 8,

considérant ce qui suit:

(1) L'article 12, paragraphe 2, du règlement (UE) nº 910/2014 prévoit qu'un cadre d'interopérabilité doit être établi à des fins d'interopérabilité des schémas d'identification électronique nationaux notifiés en application de l'article 9, paragraphe 1, dudit règlement.

(2) Les nœuds jouent un rôle central dans l'interconnexion des schémas d'identification électronique des États membres. Leur contribution est expliquée dans la documentation relative au mécanisme pour l'interconnexion en Europe établi par le règlement (UE) nº 1316/2013 du Parlement européen et du Conseil ([2]), y compris les fonctions et les composants du «nœud eIDAS».

(3) Lorsqu'un État membre ou la Commission fournit un logiciel visant à permettre l'authentification à un nœud exploité dans un autre État membre, la partie qui fournit et met à jour le logiciel utilisé pour le mécanisme d'authentification peut convenir avec la partie qui héberge le logiciel de la façon dont sera gérée l'exploitation du mécanisme d'authentification. Un tel accord ne doit pas imposer de frais ou d'exigences techniques disproportionnés (y compris assistance, responsabilités, hébergement et autres frais) à la partie hôte.

(4) Dans la mesure où la mise en œuvre du cadre d'interopérabilité le justifie, d'autres spécifications techniques fournissant des détails sur les exigences techniques énoncées dans le présent règlement pourraient être élaborées par la Commission, en coopération avec les États membres, en particulier au vu des avis du réseau de coopération visés à l'article 14, point d), de la décision d'exécution (UE) 2015/296 de la Commission ([3]). Ces spécifications devraient être élaborées au titre des infrastructures de services numériques visées par le règlement (UE) nº 1316/2013, qui fournit les moyens de la mise en œuvre pratique du sous-ensemble «identification électronique».

([1]) JO L 257 du 28.8.2014, p. 73.

([2]) Règlement (UE) nº 1316/2013 du Parlement européen et du Conseil du 11 décembre 2013 établissant le mécanisme pour l'interconnexion en Europe, modifiant le règlement (UE) nº 913/2010 et abrogeant les règlements (CE) nº 680/2007 et (CE) nº 67/2010 (JO L 348 du 20.12.2013, p. 129).

([3]) Décision d'exécution (UE) 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (JO L 53 du 25.2.2015, p. 14).

(5) Les exigences techniques énoncées dans le présent règlement devraient s'appliquer sans préjudice des éventuelles modifications apportées aux spécifications techniques susceptibles d'être élaborées en vertu de l'article 12 du présent règlement.

(6) Lors de l'établissement des modalités relatives au cadre d'interopérabilité prévu par le présent règlement, il a été dûment tenu compte du projet pilote à grande échelle STORK, et notamment des spécifications élaborées au titre de ce projet, ainsi que des principes et concepts du cadre européen d'interopérabilité pour les services publics européens.

(7) Les résultats de la coopération entre les États membres ont été pris en compte, dans toute la mesure du possible.

(8) Les mesures prévues par le présent règlement sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement établit les exigences techniques et opérationnelles relatives au cadre d'interopérabilité afin d'assurer l'interopérabilité des schémas d'identification électronique notifiés par les États membres à la Commission.

Ces exigences incluent notamment:

a) les exigences techniques minimales relatives aux niveaux de garantie et la table de correspondance des niveaux de garantie nationaux des moyens d'identification électronique notifiés délivrés en vertu de schémas d'identification électronique notifiés au titre de l'article 8 du règlement (UE) n° 910/2014, telles que décrites aux articles 3 et 4;

b) les exigences techniques minimales en matière d'interopérabilité, telles que décrites aux articles 5 et 8;

c) l'ensemble minimal de données d'identification personnelle représentant de façon univoque une personne physique ou morale, tel que décrit à l'article 11 et à l'annexe;

d) les normes de sécurité opérationnelle communes, telles que décrites aux articles 6, 7, 9 et 10;

e) les modalités de règlement des litiges, telles que décrites à l'article 13.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «nœud», un point de connexion qui fait partie de l'architecture de l'interopérabilité d'identification électronique et participe au processus d'authentification transfrontalière des personnes et qui a la capacité de reconnaître et de traiter ou d'envoyer des transmissions à d'autres nœuds en permettant à l'infrastructure d'identification électronique nationale d'un État membre de fonctionner en interface avec les infrastructures d'identification électronique nationales d'autres États membres

2) «opérateur de nœud», l'entité chargée de faire en sorte que les fonctions du nœud en tant que point de connexion soient assurées de manière correcte et fiable.

Article 3

Exigences techniques minimales relatives aux niveaux de garantie

Les exigences techniques minimales relatives aux niveaux de garantie sont fixées dans le règlement d'exécution (UE) 2015/1502 de la Commission ([1]).

Article 4

Table de correspondance des niveaux de garantie nationaux

L'établissement de la table de correspondance des niveaux de garantie nationaux des schémas d'identification électronique notifiés respecte les exigences du règlement d'exécution (UE) 2015/1502. Les résultats sont notifiés à la Commission au moyen du modèle de notification établi dans la décision d'exécution (UE) 2015/1505 de la Commission ([2]).

Article 5

Nœuds

1. Un nœud situé dans un État membre doit être en mesure de communiquer avec les nœuds d'autres États membres.

2. Les nœuds doivent être en mesure de faire la distinction entre les organismes du secteur public et les autres parties utilisatrices par le biais de moyens techniques.

3. La mise en œuvre par un État membre des exigences techniques énoncées dans le présent règlement ne doit pas avoir pour effet d'imposer aux autres États membres qui souhaitent interopérer avec cette mise en œuvre des exigences techniques et des coûts disproportionnés.

Article 6

Respect de la vie privée et confidentialité des données

1. Le respect de la vie privée, la confidentialité des données échangées et le maintien de l'intégrité des données entre les nœuds sont assurés au moyen des meilleures solutions techniques et pratiques de protection disponibles.

2. Les nœuds ne peuvent stocker aucune donnée personnelle, excepté aux fins de l'article 9, paragraphe 3.

Article 7

Intégrité et authenticité des données dans le cadre de la communication

La communication entre les nœuds assure l'intégrité et l'authenticité des données de manière à garantir que toutes les demandes et réponses sont authentiques et n'ont pas fait l'objet de manipulations non autorisées. À cette fin, les nœuds ont recours à des solutions qui ont été utilisées avec succès dans le cadre d'une utilisation opérationnelle transfrontalière.

([1]) Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (voir page 7 du présent Journal officiel).

([2]) Décision d'exécution (UE) 2015/1505 de la Commission du 8 septembre 2015 établissant les spécifications techniques et les formats relatifs aux listes de confiance visées à l'article 22, paragraphe 5, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (voir page 26 du présent Journal officiel).

Article 8

Format des messages dans le cadre de la communication

La syntaxe utilisée par les nœuds est celle de formats de message communs fondés sur des normes dont on recense plusieurs exemples de déploiement entre les États membres et dont la capacité de fonctionnement dans un environnement opérationnel est prouvée. La syntaxe permet:

a) de traiter convenablement l'ensemble minimal de données d'identification personnelle représentant de façon univoque une personne physique ou morale;

b) de traiter convenablement le niveau de garantie du moyen d'identification électronique;

c) d'établir la distinction entre les organismes du secteur public et les autres parties utilisatrices;

d) de disposer de la flexibilité nécessaire pour répondre aux besoins d'attributs supplémentaires relatifs à l'identification.

Article 9

Gestion des informations de sécurité et des métadonnées

1. L'opérateur de nœud communique les métadonnées relatives à la gestion de nœud sous un format normalisé traitable par machine et d'une façon sûre et digne de confiance.

2. Les paramètres relatifs à la sécurité, au moins, doivent pouvoir être récupérés automatiquement.

3. L'opérateur de nœud stocke des données qui, en cas d'incident, permettent de reconstruire la séquence de l'échange de messages pour déterminer le lieu et la nature de l'incident. Les données sont stockées pendant une durée conforme aux exigences nationales et comportent, au minimum, les éléments suivants:

a) identification du nœud;

b) identification du message;

c) date et heure du message.

Article 10

Normes d'assurance et de sécurité de l'information

1. Les opérateurs de nœuds assurant une authentification apportent la preuve que, eu égard aux nœuds participant au cadre d'interopérabilité, le nœud respecte les exigences de la norme ISO/CEI 27001 par certification, par des méthodes d'évaluation équivalentes ou par conformité à la législation nationale.

2. Les opérateurs de nœud déploient les mises à jour de sécurité critiques sans retard injustifié.

Article 11

Données d'identification personnelle

1. Lorsqu'un ensemble minimal de données d'identification personnelle représentant de façon univoque une personne physique ou morale est utilisé dans un contexte transfrontalier, il respecte les exigences visées à l'annexe.

2. Lorsqu'un ensemble minimal de données pour une personne physique représentant une personne morale est utilisé dans un contexte transfrontalier, il contient la combinaison des attributs énumérés à l'annexe pour les personnes physiques et les personnes morales.

3. Les données sont transmises sur la base des caractères d'origine et, le cas échéant, également transcrites en caractères latins.

Article 12

Spécifications techniques

1. Lorsque cela est justifié par le processus de mise en œuvre du cadre d'interopérabilité, le réseau de coopération établi par la décision d'exécution (UE) 2015/296 peut adopter des avis en vertu de son article 14, point d), sur la nécessité d'élaborer des spécifications techniques. Ces spécifications techniques doivent apporter des précisions sur les exigences techniques visées dans le présent règlement.

2. Conformément à l'avis visé au paragraphe 1, la Commission doit élaborer, en coopération avec les États membres, les spécifications techniques au titre des infrastructures de service numérique du règlement (UE) n° 1316/2013.

3. Le réseau de coopération doit adopter un avis en vertu de l'article 14, point d), de la décision d'exécution (UE) 2015/296, dans lequel il évalue si et dans quelle mesure les spécifications techniques élaborées en vertu du paragraphe 2 correspondent au besoin identifié dans l'avis visé au paragraphe 1 ou aux exigences fixées dans le présent règlement. Il peut recommander que les États membres tiennent compte des spécifications techniques lors de la mise en œuvre du cadre d'interopérabilité.

4. La Commission fournit une mise en œuvre de référence comme exemple d'interprétation des spécifications techniques. Les États membres peuvent appliquer cette mise en œuvre de référence ou l'utiliser comme exemple lors de l'essai d'autres mises en œuvre des spécifications techniques.

Article 13

Règlement des litiges

1. Tout litige concernant le cadre de l'interopérabilité est, dans la mesure du possible, résolu par les États membres concernés par la négociation.

2. Si aucune solution n'est trouvée conformément au paragraphe 1, le réseau de coopération établi en vertu de l'article 12 de la décision d'exécution (UE) 2015/296 est compétent conformément à son règlement intérieur.

Article 14

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 8 septembre 2015.

Par la Commission
Le président
Jean-Claude JUNCKER

ANNEXE

Exigences relatives à l'ensemble minimal de données d'identification personnelle représentant de manière univoque une personne physique ou morale, visé à l'article 11

1. **Ensemble minimal de données pour une personne physique**

L'ensemble minimal de données pour une personne physique doit contenir tous les attributs obligatoires suivants:

a) nom(s) de famille actuel(s);

b) prénom(s) actuel(s);

c) date de naissance;

d) un identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontalière et qui soit aussi persistant que possible dans le temps.

L'ensemble minimal de données pour une personne physique peut contenir un ou plusieurs des attributs supplémentaires suivants:

a) prénom(s) et nom(s) de famille à la naissance;

b) lieu de naissance;

c) adresse actuelle;

d) sexe.

2. **Ensemble minimal de données pour une personne morale**

L'ensemble minimal de données pour une personne morale doit contenir tous les attributs obligatoires suivants:

a) dénomination légale actuelle;

b) un identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontalière et qui soit aussi persistant que possible dans le temps.

L'ensemble minimal de données pour une personne morale peut contenir un ou plusieurs des attributs supplémentaires suivants:

a) adresse actuelle;

b) numéro d'immatriculation TVA;

c) numéro de référence fiscal;

d) l'identifiant visé à l'article 3, paragraphe 1, de la directive 2009/101/CE du Parlement européen et du Conseil ([1]);

e) l'identifiant d'entité juridique (IEJ) mentionné dans le règlement d'exécution (UE) n° 1247/2012 de la Commission ([2]);

f) le numéro d'enregistrement et d'identification des opérateurs économiques (n° EORI) mentionné dans le règlement d'exécution (UE) n° 1352/2013 de la Commission ([3]);

g) le numéro d'accise visé à l'article 2, point 12) du règlement n° 389/2012 du Conseil ([4]).

([1]) Directive 2009/101/CE du Parlement européen et du Conseil du 16 septembre 2009 tendant à coordonner, pour les rendre équivalentes, les garanties qui sont exigées, dans les États membres, des sociétés au sens de l'article 48, deuxième alinéa, du traité, pour protéger les intérêts tant des associés que des tiers (JO L 258 du 1.10.2009, p. 11).

([2]) Règlement d'exécution (UE) n° 1247/2012 de la Commission du 19 décembre 2012 définissant les normes techniques d'exécution en ce qui concerne le format et la fréquence des déclarations de transactions aux référentiels centraux conformément au règlement (UE) n° 648/2012 du Parlement européen et du Conseil sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (JO L 352 du 21.12.2012, p. 20).

([3]) Règlement d'exécution (UE) n° 1352/2013 de la Commission du 4 décembre 2013 établissant les formulaires prévus par le règlement (UE) n° 608/2013 du Parlement européen et du Conseil concernant le contrôle, par les autorités douanières, du respect des droits de propriété intellectuelle (JO L 341 du 18.12.2013, p. 10).

([4]) Règlement (UE) n° 389/2012 du Conseil du 2 mai 2012 concernant la coopération administrative dans le domaine des droits d'accise et abrogeant le règlement (CE) n° 2073/2004 (JO L 121 du 8.5.2012, p. 1).

RÈGLEMENT D'EXÉCUTION (UE) 2015/1502 DE LA COMMISSION

du 8 septembre 2015

fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) nº 910/2014 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)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE [1], et notamment son article 8, paragraphe 3,

considérant ce qui suit:

(1) L'article 8 du règlement (UE) nº 910/2014 prévoit qu'un schéma d'identification électronique notifié en vertu de l'article 9, paragraphe 1, doit préciser les niveaux de garantie (faible, substantiel et élevé) des moyens d'identification électronique délivrés dans le cadre dudit schéma.

(2) Il est indispensable de déterminer les spécifications techniques, normes et procédures minimales afin d'assurer une compréhension commune des détails des niveaux de garantie et d'assurer l'interopérabilité lors de l'établissement des correspondances entre les différents niveaux de garantie nationaux des schémas d'identification électronique notifiés par rapport aux niveaux de garantie visés à l'article 8, ainsi que le prévoit l'article 12, paragraphe 4, point b), du règlement (UE) nº 910/2014.

(3) Les spécifications et les procédures établies dans le présent acte d'exécution se fondent notamment sur la norme internationale ISO/CEI 29115, qui est la principale norme internationale disponible dans le domaine des niveaux de garantie pour les moyens d'identification électronique. Toutefois, la teneur du règlement (UE) nº 910/2014 diffère de celle de cette norme internationale, en particulier eu égard aux exigences de preuve et de vérification d'identité, ainsi qu'à la façon dont les différences entre les règles des États membres en matière d'identité et les outils existants dans l'Union européenne aux mêmes fins sont prises en compte. Par conséquent, bien que l'annexe se fonde sur cette norme internationale, elle ne devrait pas faire référence à un quelconque contenu spécifique de la norme ISO/CEI 29115.

(4) L'élaboration du présent règlement résulte d'une approche axée sur les résultats, considérée comme étant la plus appropriée, ce qui transparaît également dans les définitions utilisées pour spécifier les termes et concepts. L'objectif du règlement (UE) nº 910/2014 eu égard aux niveaux de garantie des moyens d'identification électronique est pris en considération. Par conséquent, il convient de tenir le plus grand compte du projet pilote à grande échelle STORK, et notamment des spécifications élaborées dans le cadre de ce projet, ainsi que des définitions et des concepts figurant dans la norme ISO/CEI 29115, pour établir les spécifications et les procédures énumérées dans le présent acte d'exécution.

(5) Selon le contexte dans lequel un aspect donné d'un élément d'identification doit être vérifié, les sources faisant autorité peuvent prendre différentes formes, telles que des registres, documents et organismes. Les sources faisant autorité peuvent être différentes selon les États membres, même dans un contexte similaire.

(6) Les exigences de preuve et de vérification d'identité devraient tenir compte des différents schémas et pratiques, tout en assurant un niveau de garantie suffisamment élevé pour établir la confiance nécessaire. Par conséquent, toute acceptation de procédures utilisées précédemment dans un but autre que la délivrance de moyens d'identification électronique devrait être subordonnée à la confirmation que ces procédures remplissent les conditions prévues pour le niveau de garantie correspondant.

[1] JO L 257 du 28.8.2014, p. 73.

(7) Certains facteurs d'authentification, tels que les secrets partagés, les dispositifs physiques et les caractéristiques physiques, sont généralement employés. Toutefois, il y a lieu d'encourager l'utilisation d'un plus grand nombre de facteurs d'authentification, notamment relevant de catégories différentes, pour renforcer la sécurité du processus d'authentification.

(8) Le présent règlement ne devrait pas affecter les droits de représentation des personnes morales. Toutefois, l'annexe devrait prévoir des exigences concernant l'établissement d'un lien entre les moyens d'identification électronique des personnes physiques et morales.

(9) Il convient de reconnaître l'importance des schémas de gestion de la sécurité de l'information et des services, ainsi que celle de l'utilisation de méthodes reconnues et de l'application des principes inscrits dans des normes comme ISO/CEI 27000 et la série ISO/CEI 20000.

(10) Il convient également de tenir compte des bonnes pratiques relatives aux niveaux de garantie dans les États membres.

(11) La certification de la sécurité informatique basée sur des normes internationales est un outil important pour vérifier que les produits respectent les exigences du présent acte d'exécution.

(12) Le comité visé à l'article 48 du règlement (UE) n° 910/2014 n'a pas rendu d'avis dans le délai fixé par son président,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

1. Les niveaux de garantie faible, substantiel et élevé des moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié sont déterminés par référence aux spécifications et procédures figurant à l'annexe.

2. Les spécifications et procédures figurant à l'annexe doivent être utilisées pour spécifier le niveau de garantie des moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié en déterminant la fiabilité et la qualité des éléments suivants:

a) inscription, conformément aux dispositions du point 2.1 de l'annexe du présent règlement établies en vertu de l'article 8, paragraphe 3, point a), du règlement (UE) n° 910/2014;

b) gestion des moyens d'identification électronique, conformément aux dispositions du point 2.2 de l'annexe du présent règlement établies en vertu de l'article 8, paragraphe 3, points b) et f), du règlement (UE) n° 910/2014;

c) authentification, conformément aux dispositions du point 2.3 de l'annexe du présent règlement établies en vertu de l'article 8, paragraphe 3, point c), du règlement (UE) n° 910/2014;

d) gestion et organisation, conformément aux dispositions du point 2.4 de l'annexe du présent règlement établies en vertu de l'article 8, paragraphe 3, points d) et e), du règlement (UE) n° 910/2014.

3. Lorsque les moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié répondent à une exigence énoncée pour un niveau de garantie plus élevé, ils sont réputés respecter l'exigence équivalente d'un niveau de garantie inférieur.

4. Sauf indication contraire dans la partie pertinente de l'annexe, un moyen d'identification électronique délivré dans le cadre d'un schéma d'identification électronique notifié doit, pour correspondre à un niveau de garantie donné, comporter tous les éléments énumérés à l'annexe en ce qui concerne ce niveau de garantie.

Article 2

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 8 septembre 2015.

Par la Commission

Le président

Jean-Claude JUNCKER

ANNEXE

Spécifications techniques et procédures pour les niveaux de garantie faible, substantiel et élevé des moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié

1. Définitions applicables

Aux fins de la présente annexe, on entend par:

1) «source faisant autorité», toute source, quelle que soit sa forme, à laquelle on peut se fier pour obtenir des données, des informations et/ou des éléments d'identification exacts pouvant être utilisés pour prouver l'identité;

2) «facteur d'authentification», un facteur confirmé comme étant lié à une personne, qui relève de l'une des catégories suivantes:

   a) «facteur d'authentification basé sur la possession», un facteur d'authentification dont il revient au sujet de démontrer la possession;

   b) «facteur d'authentification basé sur la connaissance», un facteur d'authentification dont il revient au sujet de démontrer la connaissance;

   c) «facteur d'authentification inhérent», un facteur d'authentification qui est basé sur un attribut physique d'une personne physique, et dont il revient au sujet de démontrer qu'il possède cet attribut physique;

3) «authentification dynamique», un processus électronique utilisant la cryptographie ou d'autres techniques pour fournir un moyen permettant de créer sur demande une preuve électronique attestant que le sujet contrôle ou possède les données d'identification et qui change avec chaque authentification entre le sujet et le système vérifiant l'identité du sujet;

4) «système de gestion de la sécurité de l'information», un ensemble de processus et de procédures visant à gérer les risques associés à la sécurité de l'information pour les maintenir à des niveaux acceptables.

2. Spécifications techniques et procédures

Les éléments des spécifications techniques et des procédures décrits dans la présente annexe servent à déterminer de quelle façon les exigences et les critères de l'article 8 du règlement (UE) n° 910/2014 sont appliqués aux moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique.

2.1. *Inscription*

2.1.1. Demande et enregistrement

Niveau de garantie	Éléments nécessaires
Faible	1. S'assurer que le demandeur est informé des conditions associées à l'utilisation du moyen d'identification électronique. 2. S'assurer que le demandeur est informé des précautions de sécurité recommandées relatives au moyen d'identification électronique. 3. Recueillir les données d'identité pertinentes requises pour la preuve et la vérification d'identité.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.1.2. Preuve et vérification d'identité (personne physique)

Niveau de garantie	Éléments nécessaires
Faible	1. La personne peut être présumée en possession d'un élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique et représentant l'identité alléguée. 2. L'élément d'identification peut être présumé authentique ou on peut présumer qu'il existe selon une source faisant autorité et cet élément semble être valide. 3. L'existence de l'identité alléguée est connue d'une source faisant autorité et on peut présumer que la personne est bien celle qu'elle prétend être.
Substantiel	Niveau faible, plus l'une des options énumérées aux points 1 à 4 ci-après: 1. Il a été vérifié que la personne est en possession d'un élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique et représentant l'identité alléguée et l'élément d'identification fait l'objet d'une vérification visant à déterminer son authenticité ou l'existence de cet élément est connue d'une source faisant autorité et il se rapporte à une personne réelle et des mesures ont été prises pour minimiser le risque que l'identité de la personne ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de l'élément d'identification; ou 2. une pièce d'identité est présentée au cours d'un processus d'enregistrement dans l'État membre où la pièce d'identité a été délivrée et la pièce d'identité semble se rapporter à la personne qui la présente et des mesures ont été prises pour minimiser le risque que l'identité de la personne ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de la pièce d'identité; ou 3. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle énoncée au point 2.1.2 pour le niveau de garantie substantiel, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que ladite garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008 du Parlement européen et du Conseil [1] ou par un organisme équivalent; ou 4. lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé ou substantiel et tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé ou substantiel doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008 ou par un organisme équivalent.

Niveau de garantie	Éléments nécessaires
Élevé	Les exigences du point 1 ou 2 ci-dessous doivent être respectées: 1. Niveau substantiel, plus l'une des options énumérées aux points a) à c) ci-dessous: a) Lorsqu'il a été vérifié que la personne est en possession d'un élément d'identification biométrique ou photographique reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique et que cet élément correspond à l'identité alléguée, l'élément fait l'objet d'une vérification visant à déterminer sa validité selon une source faisant autorité et le demandeur est identifié comme ayant l'identité alléguée par comparaison d'une ou de plusieurs caractéristiques physiques de la personne auprès d'une source faisant autorité; ou b) lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle visée au point 2.1.2 pour le niveau de garantie élevé, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que cette garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et des mesures sont prises pour prouver que les résultats des procédures antérieures demeurent valides; ou c) lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé, et en tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et des mesures sont prises pour prouver que les résultats de cette précédente procédure de délivrance d'un moyen d'identification électronique notifié demeurent valides; OU 2. lorsque le demandeur ne présente pas d'élément d'identification biométrique ou photographique reconnu, les mêmes procédures que celles utilisées au niveau national dans l'État membre de l'entité responsable de l'inscription afin d'obtenir ledit élément d'identification biométrique ou photographique reconnu sont appliquées.

([1]) Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

2.1.3. Preuve et vérification d'identité (personne morale)

Niveau de garantie	Éléments nécessaires
Faible	1. L'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique.

Niveau de garantie	Éléments nécessaires
	2. L'élément d'identification semble être valide et on peut présumer qu'il est authentique ou qu'il existe selon une source faisant autorité, l'inscription d'une personne morale auprès de la source faisant autorité étant une démarche volontaire et régie par un accord entre la personne morale et la source faisant autorité. 3. La personne morale n'est pas connue par une source faisant autorité comme étant dans une situation qui l'empêcherait d'agir en qualité de personne morale.
Substantiel	Niveau faible, plus l'une des options énumérées aux points 1 à 3 ci-après: 1. L'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique, y compris le nom de la personne morale, sa forme juridique et (le cas échéant) son numéro d'immatriculation et l'élément d'identification est soumis à une vérification visant à déterminer s'il est authentique, ou si son existence est connue d'une source faisant autorité, l'inscription de la personne morale auprès de la source faisant autorité étant requise pour que la personne morale puisse exercer ses activités dans son secteur et des mesures ont été prises pour minimiser le risque que l'identité de la personne morale ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration des documents; ou 2. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle visée au point 2.1.3 pour le niveau de garantie substantiel, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures sous réserve que cette garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008 ou par un organisme équivalent; ou 3. lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé ou substantiel, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé ou substantiel doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008 ou par un organisme équivalent.
Élevé	Niveau substantiel, plus l'une des options énumérées aux points 1 à 3 ci-après: 1. L'identité alléguée de la personne morale est établie sur la base de l'élément d'identification reconnu par l'État membre dans lequel est déposée la demande relative au moyen d'identité électronique, y compris le nom de la personne morale, sa forme juridique et au moins un identifiant unique représentant la personne morale utilisé dans un contexte national et l'élément d'identification est soumis à une vérification visant à déterminer s'il est valide selon une source faisant autorité; ou

Niveau de garantie	Éléments nécessaires
	2. lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre dans un but autre que la délivrance du moyen d'identification électronique assurent une garantie équivalente à celle énoncée au point 2.1.3 pour le niveau de garantie élevé, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous réserve que cette garantie équivalente soit confirmée par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et des mesures sont prises pour prouver que les résultats de cette procédure antérieure demeurent valides; ou 3. lorsque les moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité. Lorsque le moyen d'identification électronique servant de base n'a pas été notifié, le niveau de garantie élevé doit être confirmé par un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) nº 765/2008 ou par un organisme équivalent et des mesures sont prises pour prouver que les résultats de cette précédente procédure de délivrance d'un moyen d'identification électronique notifié demeurent valides.

2.1.4. Lien établi entre les moyens d'identification électronique de personnes physiques et morales

Le cas échéant, pour établir un lien entre le moyen d'identification électronique d'une personne physique et le moyen d'identification électronique d'une personne morale («lien établi»), les conditions suivantes s'appliquent:

1) Il doit être possible de suspendre et/ou de révoquer le lien établi. Le cycle de vie d'un lien établi (par exemple activation, suspension, renouvellement, révocation) doit être géré selon des procédures reconnues à l'échelle nationale.

2) La personne physique dont le moyen d'identification électronique est lié au moyen d'identification électronique de la personne morale peut déléguer l'établissement du lien à une autre personne physique sur la base de procédures reconnues à l'échelle nationale. Toutefois, la personne physique délégante reste responsable.

3) L'établissement du lien s'effectue comme suit:

Niveau de garantie	Éléments nécessaires
Faible	1. Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau faible ou supérieur. 2. Le lien a été établi sur la base de procédures reconnues à l'échelle nationale. 3. La personne morale n'est pas connue par une source faisant autorité comme étant dans une situation qui l'empêcherait d'agir au nom de la personne morale.
Substantiel	Point 3 du niveau faible, plus: 1. Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau substantiel ou élevé.

Niveau de garantie	Éléments nécessaires
	2. Le lien a été établi sur la base de procédures reconnues à l'échelle nationale, qui ont abouti à l'enregistrement du lien établi auprès d'une source faisant autorité. 3. Le lien établi a été vérifié sur la base d'informations provenant d'une source faisant autorité.
Élevé	Point 3 du niveau faible et point 2 du niveau substantiel, plus: 1. Il est vérifié que le processus suivi pour prouver l'identité de la personne physique agissant au nom de la personne morale correspond au niveau élevé. 2. Le lien a été vérifié sur la base d'un identifiant unique représentant la personne morale et utilisé dans le contexte national; et sur la base d'informations représentant de façon unique la personne physique et provenant d'une source faisant autorité.

2.2. *Gestion des moyens d'identification électronique*

2.2.1. Caractéristiques et conception des moyens d'identification électronique

Niveau de garantie	Éléments nécessaires
Faible	1. Le moyen d'identification électronique utilise au moins un facteur d'authentification. 2. Le moyen d'identification électronique est conçu pour que l'émetteur prenne des mesures raisonnables afin de vérifier qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.
Substantiel	1. Le moyen d'identification électronique utilise au moins deux facteurs d'authentification de différentes catégories. 2. Le moyen d'identification électronique est conçu de sorte qu'on puisse présumer qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.
Élevé	Niveau substantiel, plus: 1. Le moyen d'identification électronique protège contre les doubles emplois et les manipulations ainsi que contre les attaquants à potentiel d'attaque élevé. 2. Le moyen d'identification électronique est conçu de sorte que la personne à laquelle il appartient puisse le protéger de façon fiable contre toute utilisation non autorisée.

2.2.2. Délivrance, mise à disposition et activation

Niveau de garantie	Éléments nécessaires
Faible	Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il ne sera reçu que par le destinataire prévu.
Substantiel	Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il sera exclusivement remis en la possession de la personne à laquelle il appartient.
Élevé	Le processus d'activation vérifie que le moyen d'identification électronique a été remis exclusivement en la possession de la personne à laquelle il appartient.

2.2.3. Suspension, révocation et réactivation

Niveau de garantie	Éléments nécessaires
Faible	1. Il est possible de suspendre et/ou de révoquer un moyen d'identification électronique de manière rapide et efficace. 2. Des mesures ont été prises pour prévenir toute suspension, révocation et/ou réactivation non autorisées. 3. La réactivation ne pourra avoir lieu que si les exigences de garantie établies avant la suspension ou la révocation sont toujours respectées.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.2.4. Renouvellement et remplacement

Niveau de garantie	Éléments nécessaires
Faible	En tenant compte des risques d'une modification des données d'identification personnelles, le renouvellement ou le remplacement doit satisfaire aux mêmes exigences de garantie que la preuve et la vérification d'identité initiales ou reposer sur un moyen d'identification électronique valide ayant un niveau de garantie identique ou supérieur.
Substantiel	Identique au niveau faible.
Élevé	Niveau faible, plus: Lorsque le renouvellement ou le remplacement est basé sur un moyen d'identification électronique valide, les données d'identité sont vérifiées auprès d'une source faisant autorité.

2.3. *Authentification*

La présente section met l'accent sur les menaces liées à l'utilisation du mécanisme d'authentification et répertorie les exigences applicables à chaque niveau de garantie. Dans la présente section, les contrôles sont censés être proportionnés aux risques au niveau donné.

2.3.1. Mécanisme d'authentification

Le tableau suivant définit les exigences par niveau de garantie eu égard au mécanisme d'authentification employé par la personne physique ou morale pour utiliser le moyen d'identification électronique destiné à confirmer son identité à une partie utilisatrice.

Niveau de garantie	Éléments nécessaires
Faible	1. La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité. 2. Lorsque des données d'identification personnelle sont mémorisées dans le cadre du mécanisme d'authentification, ces informations sont sécurisées afin d'assurer leur protection contre toute perte ou compromission, y compris une analyse hors ligne. 3. Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque de base renforcé puissent nuire aux mécanismes d'authentification.

Niveau de garantie	Éléments nécessaires
Substantiel	Niveau faible, plus: 1. La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité par une authentification dynamique. 2. Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire aux mécanismes d'authentification.
Élevé	Niveau substantiel, plus: Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque élevé puissent nuire aux mécanismes d'authentification.

2.4. *Gestion et organisation*

Tous les participants fournissant un service lié à l'identification électronique dans un contexte transfrontalier («fournisseurs») doivent disposer de pratiques de gestion de la sécurité de l'information documentées, de politiques, d'approches de la gestion des risques et d'autres contrôles reconnus afin de garantir aux organes de gouvernance appropriés responsables des schémas d'identification électronique dans les différents États membres que des pratiques efficaces sont en place. Tous les éléments/exigences figurant au point 2.4 sont censés être proportionnés aux risques au niveau donné.

2.4.1. Dispositions générales

Niveau de garantie	Éléments nécessaires
Faible	1. Les fournisseurs fournissant un service opérationnel visé par le présent règlement sont une autorité publique ou une personne morale reconnue comme telle par le droit national d'un État membre, avec une organisation établie et pleinement opérationnelle à tous les égards pertinents pour la fourniture des services. 2. Les fournisseurs respectent toute exigence légale qui leur incombe dans le cadre du fonctionnement et de l'exécution du service, y compris les types d'informations pouvant être recherchés, la façon dont la preuve d'identité est établie, le type d'informations pouvant être conservées et leur durée de conservation. 3. Les fournisseurs sont en mesure de démontrer leur capacité à assumer la responsabilité d'éventuels dommages, ainsi que le fait qu'ils disposent de ressources financières suffisantes pour la poursuite de leurs activités et la fourniture des services. 4. Les fournisseurs sont responsables de l'exécution de toute tâche sous-traitée à une autre entité, ainsi que du respect de la politique du schéma, comme s'ils s'étaient acquittés eux-mêmes de leur mission. 5. Les schémas d'identification électronique non constitués par le droit national doivent mettre en place un plan de cessation d'activités efficace. Ce plan comporte des mesures concernant l'organisation en cas d'arrêt de fourniture du service ou de la reprise de la fourniture par un autre fournisseur, la façon dont les autorités compétentes et les utilisateurs finaux sont informés, ainsi que des détails sur les modalités de protection, conservation et destruction des informations conformément à la politique du schéma.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.4.2. Avis publiés et information des utilisateurs

Niveau de garantie	Éléments nécessaires
Faible	1. Il doit exister une définition de service publiée qui inclut toutes les modalités, conditions et frais, y compris les éventuelles limitations de son utilisation. La définition de service doit inclure une politique de confidentialité. 2. Il convient de mettre en place des procédures et politiques appropriées permettant de garantir que les utilisateurs du service sont informés de façon fiable et rapide de tout changement apporté à la définition de service et à toute modalité, condition et politique de confidentialité relative au service spécifié. 3. Il y a lieu de mettre en place des procédures et politiques appropriées permettant d'apporter des réponses complètes et exactes aux demandes de renseignements.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.4.3. Gestion de la sécurité de l'information

Niveau de garantie	Éléments nécessaires
Faible	Il existe un système de gestion de la sécurité de l'information efficace pour la gestion et le contrôle des risques de sécurité de l'information.
Substantiel	Niveau faible, plus: Le système de gestion de la sécurité de l'information adhère à des normes ou principes éprouvés pour la gestion et le contrôle des risques de sécurité de l'information.
Élevé	Identique au niveau substantiel.

2.4.4. Conservation d'informations

Niveau de garantie	Éléments nécessaires
Faible	1. Enregistrer et conserver les informations pertinentes à l'aide d'un système efficace de gestion des informations, en tenant compte de la législation applicable et des bonnes pratiques en matière de protection et de conservation des données. 2. Conserver, autant qu'il est permis par la législation nationale ou par tout autre arrangement administratif national, et protéger les informations pendant aussi longtemps qu'elles sont nécessaires pour auditer et enquêter sur les atteintes à la sécurité, et à des fins de conservation, après quoi les informations doivent être détruites en toute sécurité.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.4.5. Installations et personnel

Le tableau suivant présente les exigences relatives aux installations, au personnel et aux sous-traitants, le cas échéant, qui se chargent des tâches visées par le présent règlement. Le respect de chacune des exigences doit être proportionné au niveau de risque associé au niveau de garantie fourni.

Niveau de garantie	Éléments nécessaires
Faible	1. Il existe des procédures garantissant que le personnel et les sous-traitants sont suffisamment formés, qualifiés et expérimentés eu égard aux compétences nécessaires pour exécuter les tâches qui leur sont confiées. 2. Le personnel et les sous-traitants doivent être en nombre suffisant pour faire fonctionner et gérer de manière adéquate le service conformément à ses politiques et procédures. 3. Les installations utilisées pour fournir le service sont surveillées en permanence et protégées contre les dommages causés par des événements environnementaux, l'accès non autorisé et d'autres facteurs susceptibles d'avoir une incidence sur la sécurité du service. 4. Les installations utilisées pour fournir le service garantissent que l'accès aux zones de conservation ou de traitement d'informations personnelles, cryptographiques ou autres informations sensibles est limité au personnel ou aux sous-traitants autorisés.
Substantiel	Identique au niveau faible.
Élevé	Identique au niveau faible.

2.4.6. Contrôles techniques

Niveau de garantie	Éléments nécessaires
Faible	1. Il existe des contrôles techniques proportionnés pour gérer les risques menaçant la sécurité des services, en protégeant la confidentialité, l'intégrité et la disponibilité de l'information traitée. 2. Les canaux de communication électronique utilisés pour échanger des informations personnelles ou sensibles sont protégés contre les écoutes clandestines, la manipulation et le rejeu. 3. L'accès à du matériel cryptographique sensible, si ce dernier est utilisé pour la délivrance de moyens d'identification électronique et l'authentification, est limité aux rôles et aux applications pour lesquels il est strictement nécessaire. Il convient de s'assurer que ce matériel n'est jamais conservé de manière permanente en texte clair. 4. Il existe des procédures permettant de garantir que la sécurité est maintenue sur la durée et qu'il est possible de réagir aux changements des niveaux de risque, incidents et atteintes à la sécurité. 5. Tous les supports contenant des informations personnelles, cryptographiques ou autres informations sensibles sont stockés, transportés et mis au rebut de façon sécurisée.
Substantiel	Identique au niveau faible, plus: Le matériel cryptographique sensible, s'il est utilisé pour la délivrance de moyens d'identification électronique et l'authentification, est protégé contre toute manipulation non autorisée.
Élevé	Identique au niveau substantiel.

2.4.7. Conformité et audit

Niveau de garantie	Éléments nécessaires
Faible	Il existe des audits internes périodiques dont le champ couvre tous les aspects relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes.

Niveau de garantie	Éléments nécessaires
Substantiel	Il existe des audits internes ou externes indépendants périodiques dont le champ couvre tous les sujets relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes.
Élevé	1. Il existe des audits externes indépendants périodiques dont le champ couvre tous les sujets relatifs à la fourniture des services fournis pour assurer la conformité avec les politiques pertinentes. 2. Lorsqu'un schéma est directement géré par un organisme gouvernemental, il est audité conformément au droit national.

RÈGLEMENT D'EXÉCUTION (UE) 2015/1503 DE LA COMMISSION

du 8 septembre 2015

établissant les valeurs forfaitaires à l'importation pour la détermination du prix d'entrée de certains fruits et légumes

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 1308/2013 du Parlement européen et du Conseil du 17 décembre 2013 portant organisation commune des marchés des produits agricoles et abrogeant les règlements (CEE) nº 922/72, (CEE) nº 234/79, (CE) nº 1037/2001 et (CE) nº 1234/2007 du Conseil [1],

vu le règlement d'exécution (UE) nº 543/2011 de la Commission du 7 juin 2011 portant modalités d'application du règlement (CE) nº 1234/2007 du Conseil en ce qui concerne les secteurs des fruits et légumes et des fruits et légumes transformés [2], et notamment son article 136, paragraphe 1,

considérant ce qui suit:

(1) Le règlement d'exécution (UE) nº 543/2011 prévoit, en application des résultats des négociations commerciales multilatérales du cycle d'Uruguay, les critères pour la fixation par la Commission des valeurs forfaitaires à l'importation des pays tiers, pour les produits et les périodes figurant à l'annexe XVI, partie A, dudit règlement.

(2) La valeur forfaitaire à l'importation est calculée chaque jour ouvrable, conformément à l'article 136, paragraphe 1, du règlement d'exécution (UE) nº 543/2011, en tenant compte des données journalières variables. Il importe, par conséquent, que le présent règlement entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Les valeurs forfaitaires à l'importation visées à l'article 136 du règlement d'exécution (UE) nº 543/2011 sont fixées à l'annexe du présent règlement.

Article 2

Le présent règlement entre en vigueur le jour 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 8 septembre 2015.

Par la Commission,
au nom du président,
Jerzy PLEWA
Directeur général de l'agriculture et du développement rural

[1] JO L 347 du 20.12.2013, p. 671.
[2] JO L 157 du 15.6.2011, p. 1.

ANNEXE

Valeurs forfaitaires à l'importation pour la détermination du prix d'entrée de certains fruits et légumes

(EUR/100 kg)

Code NC	Code des pays tiers (1)	Valeur forfaitaire à l'importation
0702 00 00	MA	173,3
	MK	48,7
	XS	41,5
	ZZ	87,8
0707 00 05	MK	76,3
	TR	116,3
	XS	42,0
	ZZ	78,2
0709 93 10	TR	133,1
	ZZ	133,1
0805 50 10	AR	135,9
	BO	135,7
	CL	125,5
	UY	142,2
	ZA	136,9
	ZZ	135,2
0806 10 10	EG	239,8
	MK	63,9
	TR	129,5
	ZZ	144,4
0808 10 80	AR	188,7
	BR	93,9
	CL	134,4
	NZ	143,4
	US	112,5
	UY	110,5
	ZA	117,6
	ZZ	128,7
0808 30 90	AR	131,9
	CL	100,0
	TR	122,9
	ZA	113,5
	ZZ	117,1
0809 30 10, 0809 30 90	MK	80,1
	TR	141,7
	ZZ	110,9

(EUR/100 kg)

Code NC	Code des pays tiers (1)	Valeur forfaitaire à l'importation
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Nomenclature des pays fixée par le règlement nº 1106/2012 de la Commission du 27 novembre 2012 portant application du règlement (CE) nº 471/2009 du Parlement européen et du Conseil concernant les statistiques communautaires relatives au commerce extérieur avec les pays tiers, en ce qui concerne la mise à jour de la nomenclature des pays et territoires (JO L 328 du 28.11.2012, p. 7). Le code «ZZ» représente «autres origines».

DÉCISIONS

DÉCISION D'EXÉCUTION (UE) 2015/1504 DE LA COMMISSION

du 7 septembre 2015

accordant à certains États membres des dérogations en ce qui concerne la communication de statistiques conformément au règlement (CE) nº 1099/2008 du Parlement européen et du Conseil concernant les statistiques de l'énergie

[notifiée sous le numéro C(2015) 6105]

(Les textes en langues estonienne, française, grecque, néerlandaise et slovaque sont les seuls faisant foi.)

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

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (CE) nº 1099/2008 du Parlement européen et du Conseil du 22 octobre 2008 concernant les statistiques de l'énergie ([1]), et notamment son article 5, paragraphe 4, et son article 10, paragraphe 2,

considérant ce qui suit:

(1) Conformément à l'article 5, paragraphe 4, du règlement (CE) nº 1099/2008, sur demande dûment justifiée d'un État membre, des dérogations peuvent être accordées en ce qui concerne les composantes des statistiques nationales dont la collecte entraînerait une charge excessive pour les répondants.

(2) Des demandes de dérogation ont été présentées par la Belgique, l'Estonie, Chypre et la Slovaquie en ce qui concerne la communication de statistiques relatives à la consommation d'énergie détaillée des ménages par type d'utilisation finale pour certaines années de référence.

(3) Les informations fournies par ces États membres justifient que des dérogations soient accordées.

(4) Les mesures prévues dans la présente décision sont conformes à l'avis du comité du système statistique européen,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Les dérogations suivantes aux dispositions du règlement (CE) nº 1099/2008 sont accordées:

1. Une dérogation est accordée à la Belgique en ce qui concerne la communication de résultats relatifs à l'année de référence 2015 pour le point 1.2.3, rubriques 4.2.1 à 4.2.5, le point 2.2.3, rubriques 4.2.1 à 4.2.5, le point 3.2.3, rubriques 3.1 à 3.6, le point 4.2.3, rubriques 7.2.1 à 7.2.5, et le point 5.2.4, rubriques 4.2.1 à 4.2.5, de l'annexe B sur les statistiques relatives à la consommation d'énergie détaillée des ménages par type d'utilisation finale (telle que définie au point 2.3, 26e rubrique «Autres secteurs — secteur résidentiel», de l'annexe A).

([1]) JO L 304 du 14.11.2008, p. 1.

2. Une dérogation est accordée à l'Estonie en ce qui concerne la communication de résultats relatifs aux années de référence 2015, 2016 et 2017 pour le point 1.2.3, rubriques 4.2.1 à 4.2.5, le point 2.2.3, rubriques 4.2.1 à 4.2.5, le point 3.2.3, rubriques 3.1 à 3.6, le point 4.2.3, rubriques 7.2.1 à 7.2.5, et le point 5.2.4, rubriques 4.2.1 à 4.2.5, de l'annexe B sur les statistiques relatives à la consommation d'énergie détaillée des ménages par type d'utilisation finale (telle que définie au point 2.3, 26e rubrique «Autres secteurs — secteur résidentiel», de l'annexe A).

3. Une dérogation est accordée à Chypre en ce qui concerne la communication de résultats relatifs aux années de référence 2015, 2016 et 2017 pour le point 1.2.3, rubriques 4.2.1 à 4.2.5, le point 2.2.3, rubriques 4.2.1 à 4.2.5, le point 3.2.3, rubriques 3.1 à 3.6, et le point 5.2.4, rubriques 4.2.1 à 4.2.5, de l'annexe B sur les statistiques relatives à la consommation d'énergie détaillée des ménages par type d'utilisation finale (telle que définie au point 2.3, 26e rubrique «Autres secteurs — secteur résidentiel», de l'annexe A).

4. Une dérogation est accordée à la Slovaquie en ce qui concerne la communication de résultats relatifs aux années de référence 2015 et 2016 pour le point 1.2.3, rubriques 4.2.1 à 4.2.5, le point 2.2.3, rubriques 4.2.1 à 4.2.5, le point 3.2.3, rubriques 3.1 à 3.6, le point 4.2.3, rubriques 7.2.1 à 7.2.5, et le point 5.2.4, rubriques 4.2.1 à 4.2.5, de l'annexe B sur les statistiques relatives à la consommation d'énergie détaillée des ménages par type d'utilisation finale (telle que définie au point 2.3, 26e rubrique «Autres secteurs — secteur résidentiel», de l'annexe A).

Article 2

Le Royaume de Belgique, la République d'Estonie, la République de Chypre et la République slovaque sont destinataires de la présente décision.

Fait à Bruxelles, le 7 septembre 2015.

Par la Commission
Marianne THYSSEN
Membre de la Commission

DÉCISION D'EXÉCUTION (UE) 2015/1505 DE LA COMMISSION

du 8 septembre 2015

établissant les spécifications techniques et les formats relatifs aux listes de confiance visées à l'article 22, paragraphe 5, du règlement (UE) nº 910/2014 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)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ([1]), et notamment son article 22, paragraphe 5,

considérant ce qui suit:

(1) Les listes de confiance sont essentielles pour établir la confiance des opérateurs économiques, car elles indiquent le statut du prestataire de service au moment du contrôle.

(2) L'utilisation transfrontalière des signatures électroniques est facilitée par la décision 2009/767/CE de la Commission ([2]) qui impose aux États membres l'obligation d'établir, de tenir à jour et de publier des listes de confiance contenant des informations relatives aux prestataires de services de certification délivrant au public des certificats qualifiés conformément à la directive 1999/93/CE du Parlement européen et du Conseil ([3]) et qui sont contrôlés et accrédités par les États membres.

(3) L'article 22 du règlement (UE) nº 910/2014 impose aux États membres l'obligation d'établir, de tenir à jour et de publier, de façon sécurisée et sous une forme adaptée au traitement automatisé, des listes de confiance portant une signature électronique ou un cachet électronique et de notifier à la Commission les organismes chargés d'établir les listes de confiance nationales.

(4) Un prestataire de services de confiance et les services de confiance qu'il fournit sont considérés comme qualifiés lorsque le statut qualifié est associé au fournisseur sur la liste de confiance. Afin de s'assurer que les autres obligations découlant du règlement (UE) nº 910/2014, en particulier celles fixées aux articles 27 et 37, puissent être facilement remplies par les prestataires de services à distance et par voie électronique et afin de répondre aux attentes légitimes d'autres prestataires de services de certification qui ne délivrent pas de certificats qualifiés, mais fournissent des services associés aux signatures électroniques en vertu de la directive 1999/93/CE et sont répertoriés au 30 juin 2016, les États membres devraient pouvoir ajouter, dans les listes de confiance, des services de confiance autres que qualifiés, sur une base volontaire, au niveau national, sous réserve qu'il soit clairement indiqué que ces services ne sont pas qualifiés selon le règlement (UE) nº 910/2014.

(5) Conformément au considérant 25 du règlement (UE) nº 910/2014, les États membres peuvent ajouter des types de services de confiance définis au niveau national autres que deux définis à l'article 3, point 16), du règlement (UE) nº 910/2014, sous réserve qu'il soit clairement indiqué qu'ils ne sont pas qualifiés en vertu du règlement (UE) nº 910/2014.

(6) Les mesures prévues à la présente décision sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Les États membres établissent, publient et tiennent à jour des listes de confiance comprenant des informations sur les prestataires de services de confiance qualifiés dont ils sont responsables, ainsi que des informations relatives aux services de confiance qualifiés qu'ils fournissent. Ces listes satisfont aux spécifications techniques énoncées à l'annexe I.

([1]) JO L 257 du 28.8.2014, p. 73.
([2]) Décision 2009/767/CE de la Commission du 16 octobre 2009 établissant des mesures destinées à faciliter l'exécution de procédures par voie électronique par l'intermédiaire des guichets uniques conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur (JO L 274 du 20.10.2009, p. 36).
([3]) Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (JO L 13 du 19.1.2000, p. 12).

Article 2

Les États membres peuvent inclure dans les listes de confiance des informations sur des prestataires de services de confiance non qualifiés, ainsi que des informations relatives aux services de confiance non qualifiés qu'ils fournissent. La liste indique clairement que les prestataires de services de confiance et les services de confiance qu'ils fournissent ne sont pas qualifiés.

Article 3

1. Conformément à l'article 22, paragraphe 2, du règlement (UE) n° 910/2014, les États membres apposent une signature électronique ou un cachet électronique, sous une forme adaptée au traitement automatisé, sur leur liste de confiance selon les spécifications techniques figurant à l'annexe I.

2. Si un État membre publie par voie électronique une version directement lisible de sa liste de confiance, il veille à ce que cette version contienne les mêmes données que celle destinée à un traitement automatisé et il y appose sa signature électronique ou son cachet électronique conformément aux spécifications techniques établies à l'annexe I.

Article 4

1. Les États membres notifient à la Commission les informations visées à l'article 22, paragraphe 3, du règlement (UE) n° 910/2014 à l'aide du modèle figurant à l'annexe II.

2. Les informations visées au paragraphe 1 comprennent au moins deux certificats de clé publique d'exploitant du système, avec des dates de fin de validité espacées d'au minimum trois mois, qui correspondent aux clés privées pouvant être utilisées pour apposer une signature électronique ou un cachet électronique sur la version adaptée au traitement automatisé de la liste de confiance et sur la version directement lisible une fois publiée.

3. En vertu de l'article 22, paragraphe 4 du règlement (UE) n° 910/2014, la Commission met à la disposition du public, par l'intermédiaire d'un canal sécurisé vers un serveur web authentifié, les informations visées aux paragraphes 1 et 2, telles que notifiées par les États membres, dans une version adaptée au traitement automatisé et sur laquelle est apposée une signature ou un cachet.

4. La Commission peut mettre à la disposition du public, par l'intermédiaire d'un canal sécurisé vers un serveur web authentifié, les informations visées aux paragraphes 1 et 2, telles que notifiées par les États membres, dans une version directement lisible portant une signature ou un cachet.

Article 5

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

La présente décision est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 8 septembre 2015.

Par la Commission

Le président

Jean-Claude JUNCKER

ANNEXE I

SPÉCIFICATIONS TECHNIQUES RELATIVES À UN MODÈLE COMMUN DE LISTES DE CONFIANCE

CHAPITRE I

EXIGENCES GÉNÉRALES

Les listes de confiance comprennent des informations actualisées et tous les historiques, à compter de l'inscription d'un prestataire de services de confiance dans les listes de confiance, sur l'état des services de confiance répertoriés.

Les termes «approuvés», «accrédités» et/ou «contrôlés» dans les présentes spécifications couvrent aussi les régimes d'approbation nationaux, mais des informations complémentaires sur la nature d'un tel système national seront communiquées par les États membres dans leur liste de confiance, en fournissant notamment des éclaircissements sur les différences possibles avec les systèmes de contrôle appliqués aux prestataires de services de confiance qualifiés et aux services de confiance qualifiés qu'ils fournissent.

Les informations figurant sur la liste de confiance visent principalement à soutenir la validation des jetons de service de confiance qualifié, à savoir des objets physiques ou binaires (logiques) générés ou émis à la suite de l'utilisation d'un service de confiance qualifié, par exemple des signatures/cachets électroniques nommément qualifiés, des signatures/cachets électroniques avancés accompagnés d'un certificat qualifié, des horodatages qualifiés, des preuves de livraison électronique qualifiées, etc.

CHAPITRE II

SPÉCIFICATIONS DÉTAILLÉES POUR LE MODÈLE COMMUN DE LISTES DE CONFIANCE

Les présentes spécifications se fondent sur les spécifications et les prescriptions établies dans ETSI TS 119 612 v2.1.1 (ci-après dénommée ETSI TS 119 612).

Lorsque aucune prescription n'est prévue dans les présentes spécifications, les prescriptions des clauses 5 et 6 d'ETSI TS 119 612 doivent être appliquées dans leur intégralité. Lorsque des prescriptions spécifiques sont établies dans les présentes spécifications, elles prévalent sur les prescriptions correspondantes d'ETSI TS 119 612. En cas de divergence entre les présentes prescriptions et les prescriptions d'ETSI TS 119 612, les présentes prescriptions prévalent.

Scheme name (clause 5.3.6)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.3.6 de la TS 119 612, selon lesquelles la dénomination suivante doit être utilisée pour le système:

«EN_name_value» = «Liste de confiance comprenant des informations relatives aux prestataires de services de confiance qualifiés qui sont contrôlés par l'État membre émetteur, ainsi que les informations relatives aux services de confiance qualifiés qu'ils fournissent, conformément aux dispositions pertinentes établies par le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.»

Scheme information URI (clause 5.3.7)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.3.7 de la TS 119 612, selon lesquelles «les informations appropriées concernant le système» doivent inclure au minimum:

a) Des informations introductives, communes à tous les États membres, concernant la portée et le contexte de la liste de confiance, du système de contrôle sous-jacent et, le cas échéant, du (des) système(s) d'homologation national(aux) (par exemple accréditation). Le texte commun à utiliser est le suivant, la chaîne de caractères «[*nom de l'État membre concerné*]» devant être remplacée par le nom de l'État membre concerné:

> «La présente liste est la liste de confiance comprenant des informations relatives aux prestataires de services de confiance qualifiés qui sont contrôlés par *[nom de l'État membre concerné]*, ainsi que les informations relatives aux services de confiance qualifiés qu'ils fournissent, conformément aux dispositions pertinentes établies par le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

L'utilisation transfrontalière des signatures électroniques est facilitée par la décision 2009/767/CE de la Commission du 16 octobre 2009 qui impose aux États membres l'obligation d'établir, de tenir à jour et de publier des listes de confiance contenant des informations relatives aux prestataires de services de certification délivrant des certificats qualifiés au public conformément à la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques et qui sont surveillés/accrédités par les États membres. La présente liste de confiance est la continuation de la liste de confiance établie par la décision 2009/767/CE.»

Les listes de confiance sont des éléments essentiels pour établir la confiance entre les acteurs du marché électronique en permettant aux utilisateurs de déterminer le statut qualifié et l'historique du statut des prestataires de services de confiance et de leurs services.

Les listes de confiance des États membres incluent, au minimum, des informations visées aux articles 1er et 2 de la décision d'exécution (UE) 2015/1505 de la Commission.

Les États membres peuvent inclure dans les listes de confiance des informations relatives à des prestataires de services de confiance non qualifiés, ainsi que des informations relatives aux services de confiance non qualifiés qu'ils fournissent. Il doit être clairement indiqué qu'ils ne sont pas qualifiés selon le règlement (UE) no 910/2014.

Les États membres peuvent inclure, dans les listes de confiance, des informations relatives à des services de confiance définis au niveau national de types autres que ceux définis en vertu de l'article 3, point 16, du règlement (UE) no 910/2014. Il convient d'indiquer clairement qu'ils ne sont pas qualifiés selon le règlement (UE) no 910/2014.

b) Informations spécifiques sur le système de contrôle sous-jacent et, le cas échéant, sur le(s) système(s) d'homologation national(aux) (par exemple, accréditation), en particulier ([1]):

1) informations sur le système de contrôle national applicable aux prestataires de services de confiance qualifiés et non qualifiés et aux services de confiance qualifiés et non qualifiés qu'ils fournissent, comme le prévoit le règlement (UE) no 910/2014;

2) informations, le cas échéant, sur les systèmes d'accréditation volontaire nationaux applicables aux prestataires de services de certification ayant délivré des certificats qualifiés en vertu de la directive 1999/93/CE.

Ces informations spécifiques doivent comprendre, au minimum, pour chaque système sous-jacent énuméré ci-dessus:

1) une description générale;

2) des informations sur le processus suivi pour le système de contrôle national et, le cas échéant, pour l'homologation en vertu d'un système d'homologation national;

3) des informations sur les critères de contrôle ou, le cas échéant, d'approbation des prestataires de services de confiance;

4) des informations sur les critères et les règles utilisés pour sélectionner les organismes de surveillance ou d'audit et sur la manière dont les prestataires de services de confiance et les services de confiance qu'ils fournissent sont évalués par ces organismes;

5) le cas échéant, d'autres informations de contact et informations générales applicables au fonctionnement du système.

Scheme type/community/rules (clause 5.3.9)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.3.9 de la TS 119 612.

Il inclut seulement les URI anglais.

([1]) Les ensembles d'informations sont d'une importance cruciale pour permettre aux parties qui s'appuient sur les certificats d'évaluer la qualité et le niveau de sécurité de tels systèmes. Ces informations doivent être fournies au niveau de la liste de confiance via les champs «Scheme information URI» (clause 5.3.7 — informations à fournir par l'État membre), «Scheme type/community/rules» (clause 5.3.9 — par l'utilisation d'un texte commun à tous les États membres) et «TSL policy/legal notice» (clause 5.3.11 — un texte commun à tous les États membres, avec la possibilité pour chaque État membre d'ajouter des textes ou des références spécifiques) prévus par le présent document. Des informations supplémentaires sur ces systèmes pour les services de confiance non qualifiés et sur les services de confiance (qualifiés) définis au niveau national peuvent être fournies au niveau du service, le cas échéant et si nécessaire (par exemple pour distinguer plusieurs niveaux de qualité ou de sécurité) par l'utilisation du champ «Scheme service definition URI» (clause 5.5.6).

Il comprend au moins deux URI:

1) un URI commun aux listes de confiance de tous les États membres pointant vers un texte descriptif qui doit s'appliquer à toutes les listes de confiance, comme suit:

URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

Texte descriptif:

«Participation in a scheme

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

Policy/rules for the assessment of the listed services

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) Nº 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

The "qualified" status of a trust service is indicated by the combination of the "Service type identifier" ("Sti") value in a service entry and the status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time". Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A "CA/QC" "Service type identifier" ("Sti") entry (possibly further qualified as being a "RootCA-QC" through the use of the appropriate "Service information extension" ("Sie") additionalServiceInformation Extension)

— indicates that any end-entity certificate issued by or under the CA represented by the "Service digital identifier" ("Sdi") CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

  — the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),

  — the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. "undersupervision", "supervisionincessation", "accredited" or "granted") for that entry.

— **and IF** "Sie" "Qualifications Extension" information is present, then in addition to the above default rule, those certificates that are identified through the use of "Sie" "Qualifications Extension" information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the "SSCD support" and/or "Legal person as subject" (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific "Key usage" pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of "Qualifiers" used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

  — to indicate the qualified certificate nature:

    — "QCStatement" meaning the identified certificate(s) is(are) qualified under directive 1999/93/EC,

    — "QCForESig" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014,

    — "QCForESeal" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014/EU,

    — "QCForWSA" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014/EU.

  — to indicate that the certificate is not to be considered as qualified:

    — "NotQualified" meaning the identified certificate(s) is(are) not to be considered as qualified, and/or

  — to indicate the nature of the SSCD support:

    — "QCWithSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

    — "QCNoSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

    — "QCSSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

  — to indicate the nature of the QSCD support:

    — "QCWithQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

    — "QCNoQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

    — "QCQSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

    — "QCQSCDManagedOnBehalf" indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate, and/or

— to indicate issuance to Legal Person:

— "QCForLegalPerson" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

— if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, and

— if no "Sie" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "QCStatement" qualifier, or

— an "Sie" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "NotQualified" qualifier,

then the certificate is not to be considered as qualified.

"Service digital identifiers" are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other "Sti" type entry is that, for that "Sti" identified service type, the listed service named according to the "Service name" field value and uniquely identified by the "Service digital identity" field value has the current qualified or approval status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time".

Specific interpretation rules for any additional information with regard to a listed service (e.g. "Service information extensions" field) may be found, when applicable, in the Member State specific URI as part of the present "Scheme type/community/rules" field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.»

2) Un URI spécifique à la liste de confiance de chaque État membre pointant vers un texte descriptif qui doit s'appliquer à la liste de confiance dudit État membre:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC où CC = le code pays ISO 3166-1 ([1]) alpha-2 utilisé dans le champ «Scheme territory» (clause 5.3.10)

— qui informe les utilisateurs des règles spécifiques à l'État membre en question selon lesquelles les services inclus sur la liste sont évalués conformément au système de contrôle et, le cas échéant, au système d'homologation dudit État membre,

— qui fournit aux utilisateurs une description spécifique de l'État membre en question quant à la manière d'utiliser et d'interpréter le contenu de la liste de confiance en ce qui concerne les services de confiance non qualifiés et/ou les services de confiance définis au niveau national répertoriés. Ce texte peut être utilisé pour indiquer que le système national d'homologation prévoit éventuellement un traitement distinct en ce qui concerne les CSP ne délivrant pas de QC et la manière dont le champ «Scheme service definition URI» (clause 5.5.6) et le champ «Service information extension» (clause 5.5.9) sont utilisés à cette fin.

Les États membres PEUVENT définir et utiliser des URI supplémentaires développant l'URI spécifique d'État membre (autrement dit, des URI définis à partir de cet URI hiérarchique).

TSL policy/legal notice (clause 5.3.11)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.3.11 de la TS 119 612, selon lesquelles l'avis politique/juridique concernant le statut juridique du système ou les obligations juridiques qu'il respecte dans le ressort où il est établi et/ou les éventuelles contraintes ou conditions qui s'appliquent à la tenue à jour et à la publication

([1]) ISO 3166-1:2006: «Codes pour la représentation des noms de pays et de leurs subdivisions — Partie 1: Codes des pays».

de la liste de confiance doivent consister en une séquence de chaînes de caractères multilingues (voir clause 5.1.4) fournissant, en anglais britannique comme langue obligatoire et éventuellement dans une ou plusieurs langues nationales, le texte même de cet avis politique ou juridique établi comme suit:

1) Une première partie obligatoire, commune à toutes les listes de confiance des États membres indiquant le cadre juridique applicable, et dont la version anglaise est la suivante:

   The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC.

   Texte dans la ou les langues nationales de l'État membre:

   Le cadre juridique applicable de la présente liste de confiance est le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

2) Une partie ensuite, en option, spécifique à chaque liste de confiance, indiquant les références aux cadres juridiques nationaux applicables spécifiques.

Service current status (clause 5.5.4)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.5.4 de la TS 119 612.

La migration de la valeur «Service current status» des services énumérés sur la liste de confiance des États membres de l'Union européenne le jour précédant la date d'entrée en vigueur du règlement (UE) nº 910/2014 (soit le 30 juin 2016) doit être exécutée le jour de l'entrée en vigueur du règlement (soit le 1er juillet 2016) comme le prévoit l'annexe J d'ETSI TS 119 612.

CHAPITRE III

CONTINUITÉ DES LISTES DE CONFIANCE

Les certificats à notifier à la Commission conformément à l'article 4, paragraphe 2, de la présente décision satisfont aux prescriptions de la clause 5.7.1 d'ETSI TS 119 612 et sont délivrés de sorte:

— que leurs dates de fin de validité soient espacées d'au moins trois mois («pas après»),

— qu'ils soient créés sur de nouvelles paires de clés. Les paires de clés précédemment utilisées ne doivent pas être recertifiées.

En cas d'expiration de l'un des certificats de clé publique pouvant être utilisés pour valider la signature ou le cachet de la liste de confiance qui a été notifié à la Commission et publié dans les listes centrales de pointeurs de la Commission, les États membres doivent:

— lorsque la liste de confiance actuellement publiée a été signée ou scellée avec une clé privée dont le certificat de clé publique a expiré, republier, sans délai, une nouvelle liste de confiance signée ou scellée avec une clé privée dont le certificat de clé publique notifié est en cours de validité,

— si nécessaire, créer de nouvelles paires de clés qui pourraient servir à signer ou sceller la liste de confiance et entreprendre la génération de leurs certificats de clé publique correspondants,

— notifier promptement à la Commission la nouvelle liste de certificats de clé publique correspondant aux clés privées qui pourraient servir à signer ou sceller la liste de confiance.

En cas de compromission ou de retrait d'une des clés privées correspondant à l'un des certificats de clé publique qui pourrait servir à valider la signature ou le cachet de la liste de confiance, qui a été notifié à la Commission et qui est publié dans les listes centrales de pointeurs de la Commission, les États membres doivent:

— republier, sans retard, une nouvelle liste de confiance signée ou scellée au moyen d'une clé privée non compromise si la liste de confiance publiée a été signée ou scellée avec une clé privée compromise ou retirée,

— si nécessaire, créer de nouvelles paires de clés qui pourraient servir à signer ou sceller la liste de confiance et entreprendre la génération de leurs certificats de clé publique correspondants,

— notifier promptement à la Commission la nouvelle liste de certificats de clé publique correspondant aux clés privées qui pourraient servir à signer ou sceller la liste de confiance.

En cas de compromission ou de retrait de toutes les clés privées correspondant aux certificats de clé publique qui pourraient servir à valider la signature de la liste de confiance, qui ont été notifiés à la Commission et qui sont publiés sur la liste centrale de pointeurs de la Commission, les États membres doivent:

— créer de nouvelles paires de clés qui pourraient servir à signer ou sceller la liste de confiance et entreprendre la génération de leurs certificats de clé publique correspondants,

— republier, sans retard, une nouvelle liste de confiance signée ou scellée au moyen d'une de ces nouvelles clés privées, dont le certificat de clé publique correspondant doit être notifié,

— notifier promptement à la Commission la nouvelle liste de certificats de clé publique correspondant aux clés privées qui pourraient servir à signer ou sceller la liste de confiance.

CHAPITRE IV

SPÉCIFICATIONS POUR LA VERSION DIRECTEMENT LISIBLE DE LA LISTE DE CONFIANCE

Lorsqu'une version directement lisible de la liste de confiance est établie et publiée, elle doit être fournie sous la forme d'un document PDF (Portable Document Format) conforme à la norme ISO 32000 [1] qui doit être formaté conformément au profil PDF/A [ISO 19005 [2]].

Le contenu de la version directement lisible fondée sur PDF/A de la liste de confiance doit respecter les exigences suivantes:

— la structure de la version directement lisible doit refléter le modèle logique décrit par la TS 119 612,

— chaque champ présent doit être visible et indiquer:

  — l'intitulé du champ (par exemple «Service type identifier»),

  — la valeur du champ (par exemple «http://uri.etsi.org/TrstSvc/Svctype/CA/QC»),

  — la signification (description) de la valeur du champ, le cas échéant (par exemple «Un service de génération de certificat créant et signant des certificats basés sur l'identité et d'autres attributs vérifiés par les services d'enregistrement en question.»),

  — le cas échéant, plusieurs versions en langage naturel telles que prévues sur la liste de confiance,

— les champs et valeurs correspondantes suivants des certificats numériques [3], présents dans le champ «Service digital identity», doivent apparaître au minimum dans la version directement lisible:

  — Version

  — Numéro de série de certificat

  — Algorithme de signature

  — Émetteur — tous les champs de nom distingué pertinents

  — Période de validité

  — Objet — tous les champs de nom distingué pertinents

[1] ISO 32000-1:2008: Gestion de documents — Format de document portable — Partie 1: PDF 1.7.
[2] ISO 19005-2:2011: Gestion de documents — Format de fichier des documents électroniques pour une conservation à long terme — Partie 2: Utilisation de l'ISO 32000-1 (PDF/A-2).
[3] Recommandation ITU-T X.509 | ISO/IEC 9594-8: Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire: Cadre général des certificats de clé publique et d'attribut (voir http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— Clé publique

— Identifiant de la clé de l'autorité

— Identifiant de la clé de l'objet

— Utilisation de la clé

— Utilisation avancée de la clé

— Politiques de certification — tous les identifiants de politique et «qualifiers» de politique

— Tableau de correspondance des politiques

— Autre nom de l'objet

— Attributs d'annuaire de l'objet

— Contraintes de base

— Contraintes de politique

— Points de distribution CRL ([1])

— Accès aux informations sur l'autorité

— Accès aux informations sur l'objet

— Déclarations de certificat qualifié ([2])

— Algorithme de hachage

— Valeur de hachage du certificat

— la version directement lisible doit être facilement imprimable,

— une signature ou un cachet doit être apposé par l'exploitant du système sur la version directement lisible selon la signature avancée PDF spécifiée aux articles 1er et 3 de la décision d'exécution (UE) 2015/1505 de la Commission.

([1]) RFC 5280: Certificat internet X.509 PKI et profil CRL.
([2]) RFC 3739: internet X.509 PKI: Profil de certificats qualifiés.

ANNEXE II

MODÈLE POUR LES NOTIFICATIONS DES ÉTATS MEMBRES

Les informations devant être notifiées par les États membres en vertu de l'article 4, paragraphe 1, de la présente décision contiennent les données suivantes et tout changement s'y rapportant:

1) État membre, en utilisant les codes ISO 3166-1 ([1]) Alpha 2 avec les exceptions suivantes:

   a) Le code de pays pour le Royaume-Uni est «UK».

   b) Le code de pays pour la Grèce est «EL».

2) L'organisme ou les organismes responsables de l'établissement, de l'entretien et de la publication de la version adaptée au traitement automatisé et de la version directement lisible des listes de confiance:

   a) Nom de l'exploitant du système: l'information fournie doit être identique — sensible à la casse — à la valeur «Scheme operator name» figurant sur la liste de confiance dans autant de langues qu'utilisées sur la liste de confiance.

   b) Les informations facultatives destinées à l'usage interne de la Commission uniquement lorsque l'organisme compétent doit être contacté (les informations ne seront pas publiées sur la liste compilée des listes de confiance de la CE):

      — adresse de l'exploitant du système;

      — coordonnées de la ou des personnes responsables (nom, numéro de téléphone, adresse électronique).

3) L'endroit où est publiée la version adaptée au traitement automatisé de la liste de confiance *(endroit où est publiée la liste de confiance actuelle)*.

4) L'endroit, le cas échéant, où est publiée la version directement lisible de la liste de confiance *(endroit où est publiée la liste de confiance actuelle)*. Lorsqu'une liste de confiance directement lisible n'est plus publiée, une mention en faisant état.

5) Les certificats de clé publique qui correspondent aux clés privées pouvant être utilisées pour apposer une signature électronique ou un cachet électronique à la version adaptée au traitement automatisé de la liste de confiance et à la version directement lisible des listes de confiance: ces certificats seront fournis sous la forme de certificats DER codés Privacy Enhanced Mail Base64. Pour une notification de changement, des informations supplémentaires au cas où un nouveau certificat doit remplacer un certificat spécifique sur la liste de la Commission et au cas où le certificat notifié doit être ajouté au(x) certificat(s) existant(s) sans remplacement.

6) Date de soumission des données notifiées aux points 1) à 5).

Les données notifiées selon les points 1), 2) a), 3), 4) et 5) doivent figurer sur la liste compilée CE de listes de confiance en remplacement des informations précédemment notifiées incluses à cette liste compilée.

([1]) ISO 3166-1: «Codes pour la représentation des noms de pays et de leurs subdivisions — Partie 1: Codes des pays».

DÉCISION D'EXÉCUTION (UE) 2015/1506 DE LA COMMISSION

du 8 septembre 2015

établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement (UE) nº 910/2014 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)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ([1]), et notamment son article 27, paragraphe 5, et son article 37, paragraphe 5,

considérant ce qui suit:

(1) Les États membres doivent mettre en place les moyens techniques nécessaires au traitement des documents signés électroniquement qui sont requis pour utiliser un service en ligne proposé par un organisme du secteur public ou en son nom.

(2) En vertu du règlement (UE) nº 910/2014, les États membres exigeant un cachet ou une signature électronique avancé pour utiliser un service en ligne proposé par un organisme du secteur public, ou en son nom, doivent reconnaître les cachets et les signatures électroniques avancés, les cachets et les signatures électroniques avancés reposant sur un certificat qualifié et les cachets et les signatures électroniques qualifiés dans des formats spécifiques, ou d'autres formats validés conformément à des méthodes de référence spécifiques.

(3) Pour définir les formats et les méthodes de référence spécifiques, il convient de tenir compte des pratiques, normes et actes législatifs de l'Union en vigueur.

(4) La décision d'exécution 2014/148/UE de la Commission ([2]) définit plusieurs des formats de signatures électroniques avancées les plus couramment employés devant être pris en charge techniquement par les États membres lorsqu'une procédure administrative en ligne exige une signature électronique avancée. Établir les formats de référence vise à faciliter la validation transfrontalière des signatures électroniques et à améliorer l'interopérabilité transfrontalière des procédures électroniques.

(5) Les normes figurant à l'annexe de la présente décision sont les normes en vigueur pour les formats de signatures électroniques avancées. Les formes d'archivage à long terme des formats référencés étant actuellement en cours de révision par les organismes de normalisation, les normes détaillant l'archivage à long terme sont exclues du champ d'application de la présente décision. Lorsque la nouvelle version des normes référencées sera disponible, les références aux normes et les clauses sur l'archivage à long terme seront révisées.

(6) Les signatures électroniques avancées et les cachets électroniques avancés sont similaires du point de vue technique. Par conséquent, les normes applicables aux formats des signatures électroniques avancées s'appliquent *mutatis mutandis* aux formats des cachets électroniques avancés.

(7) Lorsqu'un format de cachet ou de signature électronique autre que ceux dont la prise en charge technique est la plus courante est utilisé pour apposer une signature ou un cachet, il convient de fournir des moyens de validation permettant la vérification transfrontalière de ces cachets ou signatures électroniques. Pour que les États membres destinataires puissent se fier aux outils de validation d'un autre État membre, il convient de fournir des informations facilement accessibles sur ces outils de validation en les faisant figurer dans les documents électroniques, les signatures électroniques ou les conteneurs de documents électroniques.

([1]) JO L 257 du 28.8.2014, p. 73.

([2]) Décision d'exécution 2014/148/UE de la Commission du 17 mars 2014 modifiant la décision 2011/130/UE établissant des exigences minimales pour le traitement transfrontalier des documents signés électroniquement par les autorités compétentes conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur (JO L 80 du 19.3.2014, p. 7).

(8) Lorsque des possibilités de validation de cachets ou de signatures électroniques adaptées au traitement automatisé sont disponibles dans les services publics d'un État membre, elles sont mises à la disposition de l'État membre destinataire et lui sont transmises. Cependant, la présente décision est sans préjudice de l'application de l'article 27, paragraphes 1 et 2, et de l'article 37, paragraphes 1 et 2, du règlement (UE) nº 910/2014 lorsque le traitement automatisé des possibilités de validation pour d'autres méthodes n'est pas possible.

(9) Afin de fournir des exigences comparables pour la validation et de renforcer la confiance dans les possibilités de validation fournies par les États membres pour des formats de cachets ou de signatures électroniques autres que ceux couramment pris en charge, les exigences relatives aux outils de validation établies par la présente décision découlent des exigences applicables à la validation des cachets et signatures électroniques qualifiés visées aux articles 32 et 40 du règlement (UE) nº 910/2014.

(10) Les mesures prévues par la présente décision sont conformes à l'avis du comité établi par l'article 48 du règlement (UE) nº 910/2014.

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Les États membres qui exigent une signature électronique avancée ou une signature électronique avancée reposant sur un certificat qualifié, en application de l'article 27, paragraphes 1 et 2, du règlement (UE) nº 910/2014, reconnaissent les signatures électroniques avancées XML, CMS ou PDF au niveau de conformité B, T ou LT, ou au moyen d'un conteneur de signature associé, lorsque ces signatures respectent les spécifications techniques énumérées à l'annexe.

Article 2

1. Les États membres qui exigent une signature électronique avancée ou une signature électronique avancée reposant sur un certificat qualifié, en application de l'article 27, paragraphes 1 et 2, du règlement (UE) nº 910/2014, reconnaissent les formats de signatures électroniques autres que ceux visés à l'article 1er de la présente décision, sous réserve que l'État membre dans lequel le prestataire de services de confiance utilisé par le signataire est établi propose d'autres possibilités de validation de signature adaptées, le cas échéant, au traitement automatisé.

2. Les possibilités de validation de signature:

a) permettent aux autres États membres de valider les signatures électroniques reçues en ligne, gratuitement et de manière compréhensible pour les locuteurs non natifs;

b) figurent dans le document signé, dans la signature électronique ou dans le conteneur de documents électroniques; et

c) confirment la validité d'une signature électronique avancée, à condition que:

1) le certificat qui prend en charge la signature électronique avancée ait été valide au moment de la signature et, lorsque la signature électronique avancée est prise en charge par un certificat qualifié, le certificat qualifié qui prend en charge ladite signature ait été, au moment de la signature, un certificat qualifié pour signature électronique conforme à l'annexe I du règlement (UE) nº 910/2014 et qu'il ait été établi par un prestataire de services de confiance qualifié;

2) les données de validation de signature correspondent aux données transmises à la partie utilisatrice;

3) l'ensemble unique de données représentant le signataire soit correctement fourni à la partie utilisatrice;

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

5) lorsque la signature électronique avancée est créée par un dispositif de création de signature électronique qualifié, l'utilisation d'un tel dispositif soit clairement indiquée à la partie utilisatrice;

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

7) les exigences prévues à l'article 26 du règlement (UE) n° 910/2014 aient été satisfaites au moment de la signature;

8) le système utilisé pour valider la signature électronique avancée fournisse à la partie utilisatrice le résultat correct du processus de validation et permette à celle-ci de détecter tout problème pertinent relatif à la sécurité.

Article 3

Les États membres qui exigent un cachet électronique avancé ou un cachet électronique avancé reposant sur un certificat qualifié, conformément à l'article 37, paragraphes 1 et 2, du règlement (UE) n° 910/2014, reconnaissent les cachets électroniques avancés XML, CMS ou PDF au niveau de conformité B, T ou LT ou au moyen d'un conteneur de cachet associé, lorsqu'ils respectent les spécifications techniques énumérées à l'annexe.

Article 4

1. Les États membres qui exigent un cachet électronique avancé ou un cachet électronique avancé reposant sur un certificat qualifié, en application de l'article 37, paragraphes 1 et 2, du règlement (UE) n° 910/2014, reconnaissent les formats de cachets électroniques autres que ceux visés à l'article 3 de la présente décision, sous réserve que l'État membre dans lequel le prestataire de services de confiance utilisé par le créateur du cachet est établi propose d'autres possibilités de validation de cachet adaptées, le cas échéant, au traitement automatisé.

2. Les possibilités de validation de cachet:

a) permettent aux autres États membres de valider les cachets électroniques reçus en ligne, gratuitement et de manière compréhensible pour les locuteurs non natifs;

b) figurent dans le document cacheté, dans le cachet électronique ou dans le conteneur de documents électroniques;

c) confirment la validité d'un cachet électronique avancé, à condition que:

1) le certificat qui prend en charge le cachet électronique avancé ait été valide au moment de l'apposition du cachet et, lorsque le cachet électronique avancé est pris en charge par un certificat qualifié, le certificat qualifié qui prend en charge ledit cachet ait été, au moment de l'apposition du cachet, un certificat qualifié pour cachet électronique conforme à l'annexe III du règlement (UE) n° 910/2014 et qu'il ait été établi par un prestataire de services de confiance qualifié;

2) les données de validation du cachet correspondent aux données communiquées à la partie utilisatrice;

3) l'ensemble unique de données représentant le créateur du cachet soit correctement fourni à la partie utilisatrice;

4) l'utilisation d'un pseudonyme soit clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de l'apposition du cachet;

5) lorsque le cachet électronique avancé est créé par un dispositif de création de cachet électronique qualifié, l'utilisation d'un tel dispositif soit clairement indiquée à la partie utilisatrice;

6) l'intégrité des données cachetées n'ait pas été compromise;

7) les exigences prévues à l'article 36 du règlement (UE) n° 910/2014 aient été satisfaites au moment de l'apposition du cachet;

8) le système utilisé pour valider le cachet électronique avancé fournisse à la partie utilisatrice le résultat correct du processus de validation et permette à celle-ci de détecter tout problème pertinent relatif à la sécurité.

Article 5

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

La présente décision est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 8 septembre 2015.

Par la Commission

Le président

Jean-Claude JUNCKER

ANNEXE

Liste des spécifications techniques relatives aux signatures électroniques avancées XML, CMS ou PDF et au conteneur de signature associé

Les signatures électroniques avancées visées à l'article 1er de la décision doivent respecter les spécifications techniques ETSI suivantes, à l'exception de leur clause 9:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1 ([1])
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1 ([2])
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2 ([3])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Le conteneur de signature associé visé à l'article 1er de la décision doit respecter les spécifications techniques ETSI suivantes:

Associated Signature Container Baseline Profile	ETSI TS 103174 v.2.2.1 ([1])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

Liste des spécifications techniques relatives aux cachets électroniques avancés XML, CMS ou PDF et au conteneur de cachet associé

Les cachets électroniques avancés visés à l'article 3 de la décision doivent respecter les spécifications techniques ETSI suivantes, à l'exception de leur clause 9:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2

Le conteneur de cachet associé visé à l'article 3 de la décision doit respecter les spécifications techniques ETSI suivantes:

Associated Seal Container Baseline Profile	ETSI TS 103174 v.2.2.1

ISSN 1977-0693 (édition électronique)
ISSN 1725-2563 (édition papier)

Office des publications de l'Union européenne
2985 Luxembourg
LUXEMBOURG

FR