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».