DÉCISION D'EXÉCUTION DE LA COMMISSION

du 14 octobre 2013

modifiant les dispositions de la décision 2009/767/CE relatives à l'établissement, à la mise à jour et à la publication de listes de confiance de prestataires de services de certification contrôlés ou accrédités par les États membres

[notifiée sous le numéro C(2013) 6543]

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

(2013/662/UE)

LA COMMISSION EUROPÉENNE,

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

vu la directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur [1], et notamment son article 8, paragraphe 3,

considérant ce qui suit:

(1) La décision 2009/767/CE de la Commission du 16 octobre 2009 établissant des mesures destinées à faciliter l'exécution de procédures par voie électronique par l'intermédiaire des guichets uniques conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur [2] oblige les États membres à rendre disponibles les informations nécessaires pour valider des signatures électroniques avancées basées sur des certificats qualifiés. Ces informations doivent être présentées de manière uniforme en utilisant des «listes de confiance» contenant des données sur les prestataires de services de certification qui délivrent au public des certificats qualifiés 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 [3] et qui sont supervisés ou accrédités par les États membres.

(2) Au regard de l'expérience pratique de mise en œuvre de la décision 2009/767/CE par les États membres, certaines améliorations s'avèrent nécessaires pour optimiser les avantages des listes de confiance. En outre, l'Institut européen des normes de télécommunications (ETSI) a publié de nouvelles spécifications techniques pour les listes de confiance (TS 119 612), qui sont fondées sur les spécifications figurant actuellement dans l'annexe de la décision mais qui, en même temps, apportent un certain nombre d'améliorations aux spécifications existantes.

(3) La décision 2009/767/CE doit donc être modifiée de manière à faire référence aux spécifications techniques 119 612 de l'ETSI et à incorporer les changements jugés nécessaires pour améliorer et faciliter la mise en œuvre et l'utilisation des listes de confiance.

(4) Afin de permettre aux États membres d'apporter les modifications techniques requises à leurs listes de confiance actuelles, il convient que la présente décision s'applique à compter du 1er février 2014.

(5) Les mesures prévues par la présente décision sont conformes à l'avis du comité de la directive sur les services,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Modifications à la décision 2009/767/CE

La décision 2009/767/CE est modifiée comme suit:

1) L'article 2 est modifié comme suit:

a) Les paragraphes 1, 2 et 2 *bis* sont remplacés par le texte suivant:

«1. Chaque État membre chargé du contrôle ou de l'accréditation des prestataires de services de certification délivrant au public des certificats qualifiés établit, tient à jour et publie, conformément aux spécifications techniques figurant à l'annexe, une «liste de confiance» qui contient, au minimum, les informations concernant ces prestataires.

2. Les États membres établissent et publient une version destinée à un traitement électronique de la liste de confiance conformément aux spécifications figurant à l'annexe. Si un État membre choisit de publier une version directement lisible de sa liste de confiance, celle-ci est conforme aux spécifications techniques figurant à l'annexe.

2 *bis*. Les États membres signent électroniquement la version destinée à un traitement électronique de leur liste de confiance afin de garantir son authenticité et son intégrité. Si un État membre publie une version directement lisible de sa liste de confiance, il veille à ce que celle-ci contienne les mêmes données que la version destinée à un traitement électronique et il la signe électroniquement avec le même certificat que celui utilisé pour cette dernière.»

[1] JO L 376 du 27.12.2006, p. 36.
[2] JO L 274 du 20.10.2009, p. 36.
[3] JO L 13 du 19.1.2000, p. 12.

b) Le paragraphe 2 *ter* suivant est inséré:

«2 *ter*. Les États membres veillent à ce que la version destinée à un traitement électronique de leur liste de confiance soit accessible à l'emplacement où elle est publiée à tout moment et sans interruption, hormis à des fins de maintenance.»

c) Le paragraphe 3 est remplacé par le texte suivant:

«3. Les États membres communiquent à la Commission les informations suivantes:

a) le nom de l'organe ou des organes responsables de l'établissement, de la mise à jour et de la publication de la version destinée à un traitement électronique de la liste de confiance;

b) l'emplacement où la version destinée à un traitement électronique de la liste de confiance est publiée;

c) deux ou plusieurs certificats de clé publique de l'exploitant du système, avec périodes de validité espacées de trois mois au minimum, correspondant aux clés privées pouvant être utilisées pour signer électroniquement la version destinée à un traitement électronique de la liste de confiance;

d) toute modification apportée aux informations visées aux points a) à c).»

d) Le paragraphe 3 *bis* suivant est inséré:

«3 *bis*. Si un État membre publie une version directement lisible de la liste de confiance, les informations visées au paragraphe 3 sont également notifiées pour cette version.»

2) L'annexe est remplacée par l'annexe de la présente décision.

Article 2

Application

La présente décision s'applique à compter du 1er février 2014.

Article 3

Destinataires

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 14 octobre 2013.

Par la Commission

Michel BARNIER

Membre de la Commission

ANNEXE

SPÉCIFICATIONS TECHNIQUES APPLICABLES À UN MODÈLE COMMUN DE «LISTE DE CONFIANCE DE PRESTATAIRES DE SERVICES DE CERTIFICATION CONTRÔLÉS OU ACCRÉDITÉS»

PRESCRIPTIONS GÉNÉRALES

1. **Introduction**

Le modèle commun de «liste de confiance de prestataires de services de certification contrôlés ou accrédités» à l'usage des États membres vise à établir une procédure commune pour la fourniture par les États membres d'informations concernant le statut de contrôle ou d'accréditation des services de certification fournis par les prestataires de services de certification ([1]) (CSP) qu'ils contrôlent ou qu'ils accréditent aux fins du respect des dispositions pertinentes de la directive 1999/93/CE. Il s'agit notamment de la fourniture d'informations relatives à l'historique du statut de contrôle ou d'accréditation des services de certification contrôlés ou accrédités.

Ces informations sont essentiellement destinées à étayer la validation de signatures électroniques qualifiées (QES) et de signatures électroniques avancées (AdES) ([2]) reposant sur un certificat qualifié ([3]) ([4]).

Les informations devant figurer obligatoirement sur la liste de confiance (TL) doivent comprendre, au minimum, des informations relatives aux CSP contrôlés ou accrédités qui délivrent des certificats qualifiés (QC) ([5]) conformément aux dispositions de la directive 1999/93/CE [article 3, paragraphes 2 et 3, et article 7, paragraphe 1, point a)], et notamment, quand elles ne font pas partie des QC, des informations concernant les QC sur lesquels repose une signature électronique et indiquant si la signature a été créée ou non au moyen d'un dispositif sécurisé de création de signature (SSCD) ([6]).

Des informations supplémentaires concernant d'autres CSP qui ne délivrent pas de QC mais fournissent des services liés aux signatures électroniques (par exemple, les CSP qui fournissent des services horodateurs et délivrent des jetons d'horodatage, les CSP qui délivrent des certificats non qualifiés, etc.) peuvent figurer sur la liste de confiance au niveau national, sur une base volontaire, pour autant qu'ils soient contrôlés ou accrédités de la même façon que les CSP qui délivrent des QC ou agréés au moyen d'un autre régime d'approbation national. Dans certains États membres, les régimes d'approbation nationaux peuvent différer des systèmes de contrôle ou d'accréditation volontaire applicables aux CSP qui délivrent des QC en termes d'exigences applicables et/ou d'organisation responsable. Les termes «accrédités» et/ou «contrôlés» dans les présentes spécifications couvrent aussi les régimes d'approbation nationaux, mais des informations complémentaires sur la nature de systèmes nationaux éventuels seront communiquées par les États membres dans leur liste de confiance, en fournissant notamment des éclaircissements sur les différences possibles avec les systèmes d'accréditation ou de contrôle appliqués aux CSP qui délivrent des QC.

Le modèle commun repose sur la spécification ETSI TS 119612 v1.1.1 ([7]) (ci-après dénommée «ETSI TS 119612») qui traite des questions d'établissement, de publication, d'emplacement, d'accès, d'authentification et de confiance relatives à ce type de listes.

2. **Structure du modèle commun de liste de confiance**

Le modèle commun de liste de confiance à l'usage des États membres est structuré conformément à la spécification ETSI TS 119612 autour des catégories d'information suivantes:

1. une étiquette de liste de confiance facilitant l'identification de la liste de confiance au cours des recherches électroniques;

2. des informations sur la liste de confiance et son système de délivrance;

3. une séquence de champs contenant des informations d'identification dénuées d'ambiguïté sur chaque CSP contrôlé ou accrédité dans le cadre du système (cette séquence est facultative, c'est-à-dire que lorsqu'elle n'est pas utilisée, la liste sera réputée vide, indiquant l'absence de tout CSP contrôlé ou accrédité dans l'État membre associé aux fins de la liste de confiance);

4. pour chaque CSP figurant sur la liste, les détails de ses services de confiance spécifiques, dont le statut en cours est enregistré sur la liste de confiance, dans une séquence de champs identifiant sans ambiguïté les services de certification contrôlés ou accrédités fournis par le CSP et leur statut en cours (cette séquence doit comporter au minimum une entrée);

([1]) Voir la définition de l'article 2, point 11), de la directive 1999/93/CE.
([2]) Voir la définition de l'article 2, point 2), de la directive 1999/93/CE.
([3]) Pour les AdES reposant sur un QC, l'acronyme «$AdES_{QC}$» sera utilisé dans le présent document.
([4]) Il convient de souligner qu'il existe un certain nombre de services électroniques fondés sur de simples AdES dont l'utilisation transfrontalière serait également facilitée à condition que les services de certification sur lesquels ils reposent (par exemple, la délivrance de certificats non qualifiés) fassent partie des services contrôlés ou accrédités figurant sur la liste de confiance d'un État membre, parmi les informations fournies sur une base volontaire.
([5]) Voir la définition de l'article 2, point 10), de la directive 1999/93/CE.
([6]) Voir la définition de l'article 2, point 6), de la directive 1999/93/CE.
([7]) ETSI TS 119612 v1.1.1 (2013-06) — Electronic Signatures and Infrastructures (ESI); Trusted Lists.

5. pour chaque service de certification contrôlé ou accrédité figurant sur la liste, les informations relatives à l'historique de ce statut, le cas échéant;

6. la signature appliquée sur la liste de confiance.

Dans le cas d'un CSP délivrant des QC, la structure de la liste de confiance et en particulier la composante des informations relatives aux services (conformément au point 4 ci-dessus) permet de compenser, par des informations complémentaires mentionnées dans les extensions d'information sur les services, les cas où le certificat qualifié ne contient pas suffisamment d'informations (destinées à un traitement électronique) sur son statut «qualifié», le fait qu'il repose éventuellement sur un SSCD et notamment des circonstances supplémentaires en vertu desquelles la plupart des CSP (commerciaux) utilisent une seule autorité de certification (CA) pour délivrer plusieurs types de certificats d'entité finale, qualifiés et non qualifiés.

Dans le contexte des services de création de certificat (CA), le nombre d'entrées relatives aux services sur la liste par CSP peut être réduit lorsqu'il existe un ou plusieurs services CA de niveau supérieur dans l'infrastructure à clé publique (PKI) du CSP (par exemple, dans le cas d'une hiérarchie de CA allant d'une CA racine à plusieurs CA délivrant les certificats) en énumérant ces services CA de niveau supérieur et non les services délivrant des certificats d'entité finale (par exemple, en mentionnant uniquement la CA racine du CSP). Cependant, dans ce type de cas, les informations concernant le statut s'appliquent à l'ensemble de la hiérarchie des services CA relevant du service mentionné sur la liste et, il est impératif de maintenir et de garantir le principe consistant à assurer un lien dénué d'ambiguïté entre le service de certification du CSP_{QC} et l'ensemble de certificats à identifier.

2.1. *Description des informations dans chaque catégorie*

1. Étiquette de liste de confiance

2. Informations sur la liste de confiance et son système de délivrance

Cette catégorie comporte notamment les informations suivantes:

— un **identifiant de version de format** de la liste de confiance,

— un **numéro de séquence (ou de publication)** de la liste de confiance,

— des **informations sur le type** de liste de confiance (indiquant, par exemple, que cette liste de confiance fournit des informations sur le statut de contrôle ou d'accréditation de services de certification fournis par des CSP contrôlés ou accrédités par l'État membre considéré aux fins du respect des dispositions de la directive 1999/93/CE),

— des **informations sur (le propriétaire) l'exploitant du système** de la liste de confiance (nom, adresse, coordonnées, etc., de l'organisme chargé, dans l'État membre, de l'établissement, de la mise à jour et de la publication sûre de la liste de confiance),

— des **informations relatives au(x) système(s) de contrôle/accréditation sous-jacent(s)** au(x)quel(s) la liste de confiance est associée, avec notamment, mais pas uniquement:

  — le pays de validité,

  — des informations sur ou une référence à l'endroit où les informations sur le système peuvent être trouvées (modèle du système, règles, critères, communauté concernée, type, etc.),

  — la durée de conservation des informations (sur l'historique),

— les **responsabilités, engagements, avis politiques et/ou juridiques** relatifs à la liste de confiance,

— la **date et l'heure d'émission** de la liste de confiance,

— la **prochaine mise à jour prévue** de la liste de confiance.

3. Informations d'identification dénuées d'ambiguïté sur chaque CSP contrôlé ou accrédité dans le cadre du système

Dans cet ensemble d'informations figurent au moins:

— la dénomination du CSP telle qu'elle figure dans les registres officiels (y compris l'UID de l'organisme CSP, selon les pratiques en usage dans l'État membre),

— l'adresse et les coordonnées de contact du CSP,

— des informations complémentaires sur le CSP, soit mentionnées directement, soit renvoyant à un site à partir duquel ces informations peuvent être téléchargées.

4. Pour chaque CSP de la liste, une séquence de champs contenant des informations d'identification dénuées d'ambiguïté sur un service de certification fourni par le CSP et contrôlé/accrédité conformément à la directive 1999/93/CE

Dans cet ensemble d'informations figureront au moins, pour chaque service de certification fourni par un CSP de la liste, les éléments suivants:

— identifiant du type de service: un identifiant du type de service de certification (par exemple, un identifiant indiquant que le service de certification contrôlé/accrédité du CSP est une autorité de certification délivrant des QC),

— dénomination (commerciale) du service: dénomination (commerciale) de ce service de certification,

— identité numérique du service: un identifiant unique et sans ambiguïté du service de certification,

— statut en cours du service: un identifiant du statut en cours du service,

— date et heure de début du statut en cours,

— informations complémentaires sur le service, le cas échéant: informations complémentaires sur le service (mentionnées directement ou renvoyant à un site à partir duquel ces informations peuvent être téléchargées, par exemple): informations sur la définition du service fournies par l'exploitant du système, informations d'accès concernant le service, informations sur la définition du service fournies par les CSP et autres informations sur le service. Par exemple, pour les services CA/QC, une séquence facultative de n-uplets d'information, chacun de ces n-uplets fournissant:

  — les critères à utiliser pour identifier plus précisément (filtrer), sous le service de confiance identifié, l'ensemble précis des produits fourni par le service [c'est-à-dire l'ensemble de certificats (qualifiés)] pour lequel des informations complémentaires sont requises/fournies en ce qui concerne son statut, la mention d'une prise en charge par un SSCD et/ou la délivrance à une personne morale, et

  — les informations associées («qualifiers») indiquant si l'ensemble des produits fourni par le service identifie les certificats à considérer comme qualifiés et/ou si les certificats qualifiés identifiés provenant de ce service reposent ou non sur un SSCD et/ou des informations concernant la délivrance éventuelle de ces QC à des personnes morales (on considère, par défaut, qu'ils ne sont délivrés qu'à des personnes physiques).

5. Pour chaque service de certification de la liste, l'historique de son statut

6. Une signature électronique créée à des fins d'authentification pour tous les champs de la TL hormis la valeur de la signature elle-même

3. **Lignes directrices relatives aux entrées de la liste de confiance**

3.1. *Information sur le statut des services de certification contrôlés ou accrédités et de leurs prestataires dans une liste unique*

La liste de confiance d'un État membre désigne la «liste faisant apparaître le statut de contrôle ou d'accréditation des services de certification des prestataires de services de certification contrôlés ou accrédités par l'État membre considéré aux fins du respect des dispositions pertinentes de la directive 1999/93/CE».

Cette liste de confiance est l'instrument unique à utiliser par l'État membre concerné pour communiquer des informations sur le statut de contrôle ou d'accréditation des services de certification et de leurs prestataires:

— **tous les prestataires de services de certification**, tels qu'ils sont définis à l'article 2, point 11), de la directive 1999/93/CE, à savoir «toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques»,

— **qui sont contrôlés ou accrédités** aux fins du respect des dispositions pertinentes de la directive 1999/93/CE.

Sur la base des définitions et des dispositions de la directive 1999/93/CE, notamment en ce qui concerne les CSP pertinents et leurs systèmes de contrôle ou d'accréditation volontaire, on peut établir une distinction entre deux catégories de CSP, à savoir les CSP délivrant des QC au public (CSP_{QC}) et les CSP ne délivrant pas de QC au public mais fournissant «d'autres services (connexes) liés aux signatures électroniques»:

— **CSP délivrant des QC**:

  — Ils doivent être contrôlés par l'État membre dans lequel ils sont établis (s'ils sont établis dans un État membre) et peuvent aussi être accrédités aux fins du respect des dispositions de la directive 1999/93/CE, et notamment des exigences de son annexe I (Exigences concernant les certificats qualifiés) et de son annexe II (Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés). Les CSP délivrant des QC qui sont accrédités dans un État membre sont toujours soumis au système de contrôle approprié de cet État membre, sauf s'ils ne sont pas établis dans l'État membre en question.

— Le système de «contrôle» applicable, ainsi que le système d'«accréditation volontaire» sont définis dans la directive 1999/93/CE et doivent être conformes aux exigences pertinentes et notamment à celles mentionnées à l'article 3, paragraphe 3, à l'article 8, paragraphe 1, à l'article 11 et au considérant 13 [ainsi qu'à l'article 2, point 13), à l'article 3, paragraphe 2, à l'article 7, paragraphe 1, point a), à l'article 8, paragraphe 1, à l'article 11 et aux considérants 4, et 11 à 13].

— **CSP ne délivrant pas de QC:**

— Ils peuvent être couverts par un «régime d'accréditation volontaire» (conforme à la définition et aux dispositions de la directive 1999/93/CE) et/ou par un régime d'autorisation reconnu mis en œuvre au niveau national pour le contrôle du respect des dispositions figurant dans la directive et éventuellement des dispositions nationales qui concernent la fourniture de services de certification [au sens de l'article 2, point 11), de la directive 1999/93/CE].

— Certains des objets physiques ou binaires (logiciels) créés ou produits dans le cadre de la fourniture d'un service de certification peuvent relever d'une «qualification» particulière sur la base de leur conformité aux dispositions et aux exigences établies au niveau national mais cette «qualification» est susceptible de n'être significative qu'au niveau national.

Chaque État membre est responsable de l'établissement et de la mise à jour d'une liste de confiance unique qui fait apparaître le statut de contrôle ou d'accréditation des services de certification fournis par les CSP contrôlés ou accrédités par cet État membre. La liste de confiance doit inclure au moins les CSP délivrant des QC. La liste de confiance peut aussi indiquer le statut d'autres services de certification contrôlés ou accrédités au moyen d'un régime d'approbation défini au niveau national.

3.2. *Un ensemble unique de valeurs de statut de contrôle ou d'accréditation*

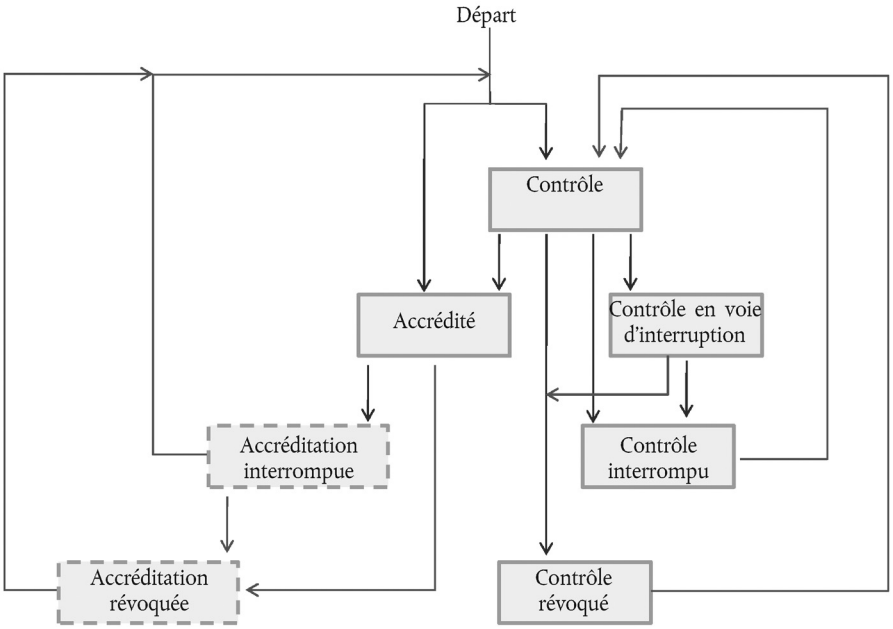
Dans la liste de confiance, la valeur du statut en cours d'un service indique s'il est actuellement «contrôlé» ou «accrédité». En outre, le statut de contrôle ou d'accréditation peut être positif («contrôlé», «accrédité», «contrôle en voie d'interruption»), interrompu («contrôle interrompu», «accréditation interrompue») ou même révoqué («contrôle révoqué», «accréditation révoquée»), en fonction de quoi la valeur correspondante lui est attribuée. Un même service de certification peut, au cours de sa durée de vie, passer du statut de contrôle au statut d'accréditation et inversement ([1]).

La figure 1 ci-dessous décrit, pour un service de certification donné, les possibilités de transition d'un statut à l'autre:

([1]) Par exemple, un prestataire de services de certification établi dans un État membre et fournissant un service de certification contrôlé, à l'origine, par l'État membre (instance de contrôle) peut, après un certain temps, décider d'opter pour une accréditation volontaire pour le service de certification contrôlé. Inversement, un prestataire de services de certification établi dans un autre État membre peut décider de ne pas mettre fin à un service de certification accrédité mais de transformer son statut d'accréditation en statut de contrôle, pour des raisons commerciales ou économiques, par exemple.

Figure 1

Flux attendu du statut de contrôle/d'accréditation pour un service CSP donné



Légende:

Statut provisoire lorsqu'il existe un modèle de contrôle associé (par exemple, pour un CSP délivrant des QC accrédité et contrôlé dans l'État membre où il est établi).
Statut en cours possible lorsqu'il n'existe pas de modèle de contrôle associé (par exemple, pour un CSP accrédité dans un État membre où il n'est pas établi).

Statut en cours possible

Quand il est établi dans un État membre, un service de certification délivrant des QC doit être contrôlé (par l'État membre où il est établi) et peut faire l'objet d'une accréditation volontaire. Lorsque ce service figure dans une liste de confiance, son statut doit correspondre à l'une des valeurs mentionnées plus haut comme «valeur du statut en cours» selon son statut effectif et doit être modifié, le cas échéant, en fonction de la transition d'un statut à l'autre décrite ci-dessus. Toutefois, les valeurs «accréditation interrompue» et «accréditation révoquée» ne peuvent être qu'un «statut provisoire» si le service de CSP_{QC} correspondant figure sur la liste de confiance de l'État membre où il est établi, puisque ce type de service doit, par défaut, être contrôlé (même lorsqu'il n'est pas ou plus accrédité); quand le service correspondant figure sur la liste (est accrédité) dans un autre État membre que celui où il est établi, ces valeurs peuvent être définitives.

Les États membres qui établissent ou ont établi un ou des régime(s) d'approbation reconnu(s) mis en œuvre sur une base nationale pour contrôler la conformité des services fournis par des CSP qui **ne** délivrent **pas** de QC avec les dispositions de la directive 1999/93/CE et éventuellement avec des dispositions nationales applicables à la fourniture de services de certification [au sens de l'article 2, point 11), de la directive 1999/93/CE] doivent répartir ces régimes d'approbation dans les deux catégories suivantes:

— «accréditation volontaire», conformément à la définition et aux dispositions de la directive 1999/93/CE [article 2, point 13), article 3, paragraphe 2, article 7, paragraphe 1, point a), article 8, paragraphe 1, article 11, considérants 4 et 11 à 13],

— «contrôle», conformément aux prescriptions de la directive 1999/93/CE, mis en œuvre par des dispositions et exigences nationales respectant la législation nationale.

En conséquence, un service de certification ne délivrant pas de QC peut être contrôlé ou faire l'objet d'une accréditation volontaire. Lorsque ce service figure dans une liste de confiance, son statut doit correspondre à l'une des valeurs mentionnées plus haut comme «valeur du statut en cours» (voir figure 1) selon son statut effectif et doit évoluer, le cas échéant, en fonction de la transition d'un statut à l'autre décrite ci-dessus.

Dans la liste de confiance doivent figurer des informations relatives au(x) régime(s) de contrôle/accréditation sous-jacents, et notamment:

— des informations relatives au système de contrôle applicable à tout CSP_{QC},

— le cas échéant, des informations relatives au régime national «d'accréditation volontaire» applicable à tout CSP_{QC},

— le cas échéant, des informations sur le système de contrôle applicable aux CSP qui ne délivrent pas de QC,

— le cas échéant, des informations relatives au régime national «d'accréditation volontaire» applicable à tout CSP ne délivrant pas de QC.

Les deux derniers ensembles d'information revêtent une importance cruciale pour les parties qui s'appuient sur le certificat car elles leur permettent d'évaluer le niveau de sécurité et de qualité de ces systèmes de contrôle ou d'accréditation applicables au niveau national aux CSP ne délivrant pas de QC. Quand la liste de confiance contient des informations sur le statut de contrôle ou d'accréditation concernant des services fournis par des CSP qui ne délivrent pas de QC, les ensembles d'informations précités sont fournis au niveau de la liste de confiance par l'intermédiaire des champs «Scheme information URI» (clause 5.3.7 — information fournie par les États membres), «Scheme type/community/rules» (clause 5.3.9 — utilisation d'un texte commun à tous les États membres et d'informations spécifiques facultatives fournies par un État membre) et «TSL policy/legal notice» (clause 5.3.11 — un texte commun à tous les États membres qui renvoie à la directive 1999/93/CE, avec la possibilité, pour chaque État membre, d'ajouter des références ou des textes spécifiques).

Les informations de qualification supplémentaires définies au niveau des systèmes nationaux de contrôle ou d'accréditation relatifs aux CSP qui ne délivrent pas de QC peuvent être fournies au niveau du service, le cas échéant et lorsque c'est nécessaire (pour faire la distinction entre différents niveaux de qualité/sécurité, par exemple), par l'intermédiaire du champ «Additional service information extension» (clause 5.5.9.4.) qui fait partie des «Service information extensions» (clause 5.5.9). Les spécifications détaillées figurant dans le chapitre I fournissent davantage d'informations sur les spécifications techniques correspondantes.

Même si différents organismes d'un même État membre peuvent être chargés du contrôle et de l'accréditation des services de certification dans cet État membre, il est prévu de n'utiliser impérativement qu'une seule entrée par service de certification et de mettre à jour son statut de contrôle/accréditation en conséquence.

3.3. *Entrées de la liste de confiance destinées à faciliter la validation des QES et des* $AdES_{QC}$

Lors de la création de la liste de confiance, la partie la plus critique consiste à établir la partie obligatoire de la liste de confiance, à savoir la «liste de services» par CSP délivrant des QC de sorte qu'elle soit le reflet exact de la situation de chacun de ces services de certification délivrant des QC et que les informations fournies sous chaque entrée soient suffisantes pour faciliter la validation des QES et des $AdES_{QC}$ (lorsqu'elles sont combinées avec le contenu du QC de l'entité finale délivré par le CSP dans le cadre du service de certification mentionné dans cette entrée).

Les informations requises peuvent comporter d'autres informations que la «Service digital identity» d'une seule CA (racine), notamment des informations identifiant le statut de QC des certificats délivrés par ce service CA et indiquant si les signatures sont créées ou non par un SSCD. Au niveau de l'État membre, l'organisme chargé d'établir, de modifier et de tenir à jour la liste de confiance doit donc tenir compte du profil et du contenu de certificat en cours dans chaque QC délivré, pour chaque CSP_{QC} couvert par la liste de confiance.

Idéalement, chaque QC délivré devrait comprendre la déclaration de conformité de QC [1] définie par l'ETSI lorsqu'il est déclaré comme un QC et la déclaration QcSSCD définie par l'ETSI lorsqu'il est déclaré qu'il repose sur un SSCD pour la création de signatures électroniques et/ou que chaque QC délivré comprend l'un des identifiants d'objet (OID) de règles de certificat QCP/QCP + définis par la spécification ETSI EN 319 411-2 [2]. Étant donné que les CSP délivrant des QC utilisent des normes différentes comme références, que les interprétations de ces normes varient considérablement et que l'existence et la préexistence de normes et spécifications techniques normatives ne sont pas toujours connues, le contenu effectif des QC délivrés actuellement n'est pas toujours identique (les déclarations Qc définies par l'ETSI ne sont pas toujours utilisées) et, par conséquent, les parties utilisatrices ne peuvent pas simplement compter sur le certificat du signataire (et sur la chaîne ou le chemin associé) pour évaluer, du moins par traitement informatique, si le certificat sur lequel repose une signature est ou non déclaré comme un QC et s'il est ou non associé à un SSCD par l'intermédiaire duquel la signature électronique a été créée.

[1] Pour la définition de cette déclaration, voir ETSI EN 319 412-5 — Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.

[2] ETSI EN 319 411-2 — Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

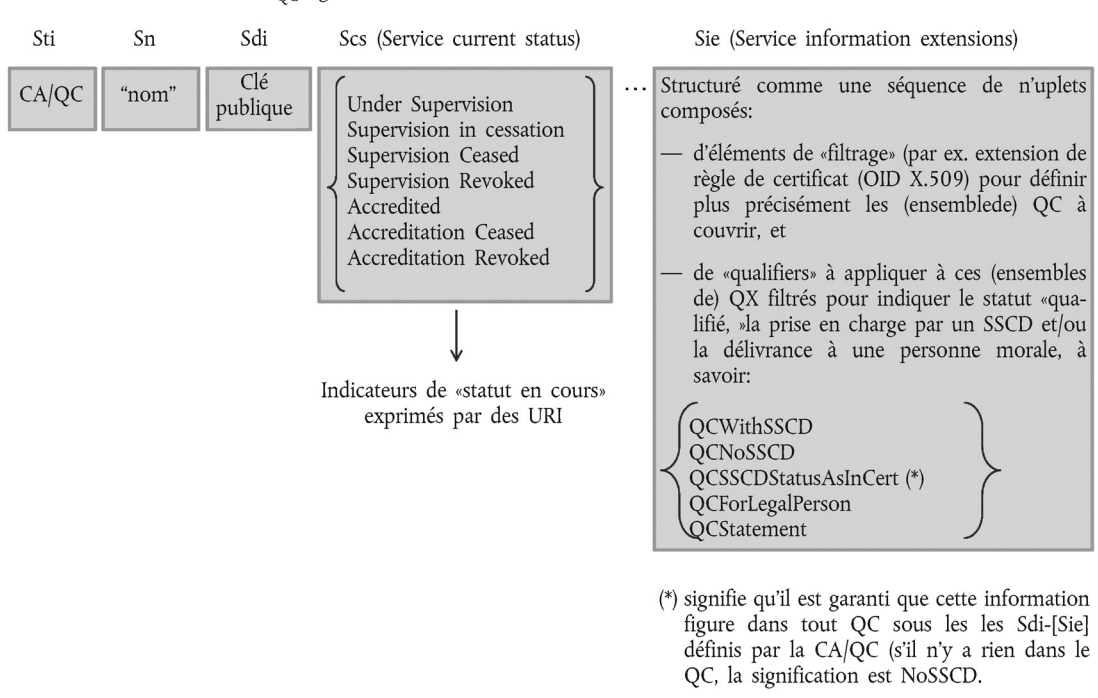
En complétant les champs «Service type identifier» («Sti»), «Service name» («Sn») et «Service digital identity» («Sdi») de l'entrée relative au service au moyen des informations fournies par le champ «Service information extensions» («Sie»), il est possible de déterminer complètement un type spécifique de certificat qualifié émis par un service de certification d'un CSP délivrant des QC qui figure sur la liste et d'indiquer s'il repose ou non sur un SSCD (lorsque ces informations ne figurent pas dans le QC délivré). À cette entrée est associée une information de «Service current status» («Scs»). La situation est illustrée par la figure 2 ci-dessous.

L'ajout d'un service sur la liste en fournissant seulement le «Sdi» d'une CA (racine) signifierait qu'il est garanti (par le CSP délivrant des QC mais aussi par l'organisme de contrôle/accréditation chargé du contrôle/accréditation du CSP en question) que tout certificat d'entité finale délivré par cette (hiérarchie de) CA (racine) contient suffisamment d'informations définies par l'ETSI qui se prêtent à un traitement électronique pour qu'il soit possible d'évaluer s'il s'agit ou non d'un QC et s'il repose ou non sur un SSCD. Si, par exemple, cette dernière affirmation ne se vérifie pas (c'est-à-dire que le QC ne contient pas assez d'informations normalisées définies par l'ETSI qui se prêtent à un traitement électronique permettant de savoir s'il repose ou non sur un SSCD), en ne faisant figurer sur la liste que le «Sdi» de cette CA (racine), on ne peut que supposer que les QC délivrés par cette hiérarchie de CA (racine) ne reposent sur aucun SSCD. Pour indiquer que ces QC doivent être considérés comme reposant sur un SSCD, il convient d'utiliser le champ «Sie» (cela indique aussi que cette information est garantie par le CSP délivrant des QC et contrôlé/accrédité par l'organisme de contrôle ou d'accréditation).

Figure 2

Entrée relative au service pour un CSP délivrant des QC mentionné sur la liste de confiance

Principes généraux – règles d'édition – entrées CSP_{QC} (services figurant dans la liste)



(*) signifie qu'il est garanti que cette information figure dans tout QC sous les les Sdi-[Sie] définis par la CA/QC (s'il n'y a rien dans le QC, la signification est NoSSCD.

Les spécifications techniques du présent modèle commun de liste de confiance permettent d'utiliser une combinaison de cinq grands types d'information pour l'entrée relative au service:

— le «Service type identifier» («Sti»), c'est-à-dire l'identification de la CA délivrant des QC («CA/QC»),

— le «Service name» («Sn»),

— les informations de «Service digital identity» («Sdi») qui identifient un service figurant sur la liste, par exemple (au minimum) la clé publique d'une CA qui délivre des QC,

— pour les services CA/QC, des informations facultatives de «Service information extensions» («Sie») qui permettent d'inclure plusieurs éléments d'information spécifiques relatifs au service concernant le statut de révocation des certificats expirés, des caractéristiques complémentaires des QC, la reprise d'un CSP par un autre CSP et d'autres informations complémentaires sur le service. Par exemple, les caractéristiques complémentaires des QC sont représentées par une séquence d'un ou plusieurs n-uplets, chaque n-uplet fournissant:

  — les critères à utiliser pour identifier plus précisément (filtrer), sous le service de certification identifié par le «Sdi», l'ensemble exact de certificats qualifiés pour lequel des informations complémentaires sont requises/fournies concernant l'indication du statut «qualifié», la prise en charge par un SSCD et/ou la délivrance à une personne morale, et

  — les informations associées («qualifiers») indiquant si cet ensemble de certificats qualifiés doit être considéré comme «qualifié», s'il repose ou non sur un SSCD ou si ces informations associées font partie du QC sous une forme normalisée qui se prête à un traitement informatique, et/ou des informations concernant la délivrance de ces QC à des personnes morales (on considère, par défaut, qu'ils ne sont délivrés qu'à des personnes physiques).

— les informations sur le «statut en cours» de l'entrée relative à ce service, qui indiquent:

  — s'il s'agit d'un service contrôlé ou accrédité, et

  — le statut de contrôle/d'accréditation lui-même.

3.4. *Lignes directrices pour la création, la modification et l'utilisation des entrées relatives aux services des* CSP_{QC}

Les **lignes directrices générales** sont les suivantes:

1. S'il existe une garantie [fournie par le CSP_{QC} et contrôlée/accréditée par l'organisme de contrôle (SB) ou d'accréditation (SA)] que, pour un service figurant sur la liste et identifié par un «Sdi», tout QC reposant sur un SSCD contient bien la déclaration de conformité Qc définie par l'ETSI, et contient la déclaration QcSSCD et/ou l'identifiant QCP + Object Identifier (OID), l'utilisation d'un «Sdi» approprié est suffisante et le champ «Sie» peut être utilisé de manière optionnelle et ne devra pas nécessairement contenir d'informations concernant la prise en charge par un SSCD.

2. S'il existe une garantie (fournie par le CSP_{QC} et contrôlée/accréditée par le SB/SA) que, pour un service figurant sur la liste et identifié par un «Sdi», tout QC ne reposant pas sur un SSCD contient bien la déclaration de conformité Qc et/ou le QCP OID, et ne contient pas la déclaration QcSSCD ou l'identifiant QCP + OID, l'utilisation d'un «Sdi» approprié est suffisante et le champ «Sie» peut être utilisé de manière optionnelle et ne doit pas nécessairement contenir d'informations concernant la prise en charge par un SSCD (ce qui signifie qu'il ne repose pas sur un SSCD).

3. S'il existe une garantie (fournie par le CSP_{QC} et contrôlée/accréditée par le SB/SA) que, pour un service figurant sur la liste et identifié par un «Sdi», tout QC contient bien la déclaration de conformité QC, et que certains de ces QC sont censés reposer sur des SSCD et d'autres pas (par exemple, la distinction peut être établie grâce à des OID de règles de certificats spécifiques au CSP différentes ou à d'autres informations spécifiques au CSP se trouvant dans le QC, directement ou indirectement, destinées à un traitement informatique ou non), mais reposent sur un certificat qui ne contient NI la déclaration QcSSCD NI le QCP(+) OID de l'ETSI, l'utilisation d'un «Sdi» approprié n'est peut-être pas suffisante ET le champ «Sie» doit être utilisé pour mentionner explicitement des informations concernant la prise en charge par un SSCD, ainsi qu'un complément d'informations éventuel destiné à identifier l'ensemble de certificats couvert. Il est possible que différentes «SSCD support information values» doivent être entrées pour un même «Sdi» lorsque le champ «Sie» est utilisé.

4. S'il existe une garantie (fournie par le CSP_{QC} et contrôlée/accréditée par le SB/SA) que, pour un service figurant sur la liste et identifié par un «Sdi», tout QC ne contient ni la déclaration de conformité Qc, ni l'identifiant QCP OID, ni la déclaration QcSSCD, ni l'identifiant QCP + OID, mais qu'il est assuré que certains des certificats d'entité finale délivrés sous ce «Sdi» sont censés être des QC et/ou reposer sur des SSCD et d'autres pas (par exemple, la distinction peut être établie grâce à des OID de règles de certificats spécifiques au CSP_{QC} différentes ou à d'autres informations spécifiques au CSP_{QC} se trouvant dans le QC, directement ou indirectement, destinées à un traitement informatique ou non), l'utilisation d'un «Sdi» approprié ne sera pas suffisante ET le champ «Sie» doit être utilisé pour mentionner explicitement des informations de qualification. Il est possible que différentes «SSCD support information values» doivent être entrées pour un même «Sdi» lorsque le champ «Sie» est utilisé.

Le principe général par défaut veut que, pour chaque CSP figurant sur la liste de confiance, il y ait une seule entrée relative au service par clé publique pour un service de vérification de type CA/QC, c'est-à-dire par autorité de certification délivrant (directement) des QC. Dans certaines circonstances exceptionnelles et sous certaines conditions strictement surveillées, l'organisme de contrôle/accréditation d'un État membre peut décider d'utiliser, comme «Sdi» d'une entrée unique de la liste des services fournis par un CSP de la liste, la clé publique d'une CA racine ou de niveau supérieur

dans la PKI du CSP (par exemple dans le cas d'une hiérarchie de CA allant d'une CA racine à plusieurs CA délivrant les certificats), au lieu d'énumérer tous les services CA subordonnés délivrant des certificats (c'est-à-dire mentionner une autorité de certification qui ne délivre pas directement des QC d'entité finale mais qui certifie une hiérarchie de CA jusqu'aux CA qui délivrent les QC aux entités finales). Les conséquences (avantages et inconvénients) de l'utilisation d'une telle clé publique d'une CA racine ou de niveau supérieur en tant que valeur «Sdi» dans une entrée relative au service de la liste de confiance doivent être soigneusement examinées par les États membres qui y ont recours. En outre, lorsqu'un État membre fait usage de cette possibilité de dérogation au principe appliqué par défaut, il doit fournir les documents nécessaires pour faciliter la création et la vérification du chemin de certification. Par exemple, dans le cas d'un CSP_{QC} utilisant une CA racine qui englobe plusieurs CA délivrant des QC et des non-QC, mais pour lequel les QC contiennent uniquement la déclaration de conformité QC et aucune indication de prise en charge par un SSCD, le fait de mentionner uniquement le «Sdi» de la CA racine sur la liste signifierait, suivant les règles exposées ci-dessus, qu'aucun des QC délivrés sous cette CA Racine ne repose sur un SSCD. S'il existe des QC qui reposent effectivement sur un SSCD, sans qu'une déclaration destinée à un traitement électronique figure dans les certificats pour indiquer cette prise en charge, il est vivement recommandé d'utiliser la déclaration QcSSCD dans les QC délivrés à l'avenir. Dans l'intervalle (jusqu'à l'expiration du dernier QC ne contenant pas cette information), la liste de confiance doit utiliser le champ «Sie» et le champ «Qualifications Extension» associé, en fournissant par exemple des informations de filtrage permettant d'identifier un ou des ensemble(s) de certificats au moyen d'OID spécifiques à des CSP_{QC} qui peuvent être utilisés par les CSP_{QC} pour établir une distinction entre différents types de QC (certains reposant sur des SSCD et d'autres pas) et en recourant à des «Qualifiers» pour associer des informations explicites sur la prise en charge par un SSCD aux ensembles de certificats (filtrés).

Les **lignes directrices d'usage général** pour les applications, services ou produits liés aux signatures électroniques reposant sur une liste de confiance conforme aux présentes spécifications techniques sont les suivantes:

Une entrée «Sti» «CA/QC» (et, de la même manière, une entrée CA/QC qualifiée de «CA/QC racine» par l'utilisation du champ «Sie» «Service information Extension»)

— indique que tous les certificats d'entité finale délivrés par la CA identifiée par le «Sdi» (et, de la même manière, dans la hiérarchie de CA découlant de la CA racine identifiée par le «Sdi») sont des QC **à condition** d'être déclarés comme tels dans le certificat au moyen d'une déclaration Qc appropriée (à savoir une déclaration de conformité Qc) qui se prête au traitement électronique et/ou aux de QCP(+) OID définies par l'ETSI (ce qui est garanti par l'organisme de contrôle/accréditation, voir ci-dessus les lignes directrices générales pour la création et la modification des entrées).

Note: Si le champ «Sie» ne contient pas d'informations de «Qualifications Extension» ou si un certificat d'entité finale qui est déclaré être un QC n'est pas identifié plus précisément par une entrée «Qualifications Extension» liée dans le champ «Sie», les informations destinées à un traitement électronique se trouvant dans le QC sont contrôlées/accréditées comme des informations exactes. Cela signifie qu'il est garanti que l'utilisation (ou non) des déclarations Qc appropriées (à savoir des déclarations de conformité QcC, QcSSCD) et/ou de QCP(+) OID définis par l'ETSI est conforme à ce qui est annoncé par le CSP_{QC},

— **et SI** le champ «Sie» contient des informations de «Qualifications Extension», en sus de la règle d'interprétation par défaut mentionnée ci-dessus, les certificats qui sont identifiés par l'utilisation de cette entrée «Sie» de «Qualifications Extension», construite sur le principe d'une séquence de filtres qui identifient plus précisément un ensemble de certificats, doivent être examinés en fonction des «Qualifiers» associés fournissant des informations supplémentaires sur le statut qualifié, la prise en charge par un SSCD et/ou la personne morale (par ex. les certificats qui contiennent un OID spécifique dans l'extension de règle des certificats et/ou qui ont un modèle spécifique de «Key usage» et/ou qui sont filtrés par l'utilisation d'une valeur spécifique qui apparaît dans un champ spécifique du certificat ou dans une extension, etc.). Ces informations de qualification font partie de l'ensemble suivant de «Qualifiers» utilisés pour compenser le manque d'informations contenues dans le QC correspondant, et qui servent respectivement:

  — à indiquer le statut qualifié: «QCStatement» signifiant que le(s) certificat(s) est(sont) qualifié(s),

  ET/OU

  — à indiquer la nature de la prise en charge par un SSCD

    — la valeur «QCWithSSCD» signifiant «QC reposant sur un SSCD», ou

    — la valeur «QCNoSSCD» signifiant «QC ne reposant pas sur un SSCD», ou

    — la valeur «QCSSCDStatusAsInCert» signifiant qu'il est garanti que tout QC contient, sous les informations «Sdi» – «Sie» de cette entrée CA/QC, des informations concernant la prise en charge par un SSCD,

  ET/OU

— à indiquer la délivrance à une personne morale:

— la valeur «QCForLegalPerson» signifiant que le certificat a été délivré à une personne morale.

3.5. *Services sur lesquels reposent les services «CA/QC» qui ne font pas partie du «Sdi» «CA/QC»*

Les services liés aux QC qui indiquent le statut de validité d'un certificat et dont les informations (par exemple, les CRL et les réponses OCSP) sont signées par une entité disposant d'une clé privée non certifiée selon un chemin de certification qui aboutit à une CA délivrant des QC («CA/QC») mentionnée sur la liste seront eux-mêmes inclus sur la liste de confiance en énumérant les services de statut de validité du certificat en tant que tels dans la TL (par exemple avec un type de service de «OCSP/QC» ou «CRL/QC» respectivement) puisque ces services peuvent être considérés comme faisant partie des services «qualifiés» contrôlés/accrédités liés à la fourniture de services de certification QC. Bien sûr, les répondeurs OCSP ou les émetteurs de CRL dont les certificats sont signés par des CA relevant de la hiérarchie d'un service CA/QC qui figure sur la liste doivent être considérés comme valables conformément à la valeur de statut du service CA/QC de la liste.

Une disposition similaire peut être appliquée aux services de certification qui délivrent des certificats non qualifiés (services de type «CA/PKC»).

La liste de confiance comprendra des services de statut de validité du certificat quand les informations relatives à l'emplacement de ces services ne figurent pas dans les certificats d'entités finales auxquels ils s'appliquent.

4. **Définitions et abréviations**

Les sigles et définitions applicables aux fins du présent document sont les suivants:

Terme	Sigle	Définition
Prestataire de service de certification	CSP	Tel que défini à l'article 2, point 11), de la directive 1999/93/CE.
Autorité de certification	CA	1. un prestataire de service de certification qui crée et attribue des certificats de clé publique; ou 2. un service technique de création de certificat utilisé par un prestataire de service de certification qui crée et attribue des certificats de clé publique. *REMARQUE:* Voir la clause 4 de la norme EN 319 411-2 [1] pour plus d'explications sur la notion d'autorité de certification.
Autorité de certification délivrant des certificats qualifiés	CA/QC	Une CA qui respecte les exigences prévues à l'annexe II de la directive 1999/93/CE et délivre des certificats qualifiés conformes aux exigences prévues à l'annexe I de la directive 1999/93/CE.
Certificat	Certificat	Tel que défini à l'article 2, point 9), de la directive 1999/93/CE.
Certificat qualifié	QC	Tel que défini à l'article 2, point 10), de la directive 1999/93/CE.
Signataire	Signataire	Tel que défini à l'article 2, point 3), de la directive 1999/93/CE.
Contrôle	Contrôle	Renvoie au contrôle prévu à l'article 3, paragraphe 3, de la directive 1999/93/CE. Celle-ci prescrit aux États membres d'instaurer un système adéquat permettant de contrôler les CSP établis sur leur territoire et délivrant des certificats qualifiés au public, assurant ainsi le contrôle du respect des dispositions de la directive.
Accréditation volontaire	Accréditation	Telle que définie à l'article 2, point 13), de la directive 1999/93/CE.
Liste de confiance	TL	Désigne la liste indiquant le statut en matière de contrôle ou d'accréditation des services de certification des fournisseurs de services de certification qui sont contrôlés ou accrédités par l'État membre visé en ce qui concerne le respect des dispositions de la directive 1999/93/CE.

Terme	Sigle	Définition
Liste du statut des services de confiance	TSL	Forme d'une liste signée utilisée en tant que base pour la présentation des informations de statut des services de confiance conformément aux spécifications ETSI TS 119612.
Service de confiance		Service qui renforce la confiance dans les transactions électroniques (recourant en général, mais pas obligatoirement, à des techniques de chiffrement ou à des documents confidentiels) (ETSI TS 119612). *NOTE*: Ce terme est employé dans un sens plus général que celui de service de certification délivrant des certificats ou fournissant d'autres services liés aux signatures électroniques.
Prestataire de service de confiance	TSP	Organisme responsable de la prestation d'un ou plusieurs services de confiance (électroniques). (Ce terme est employé dans un sens plus général que CSP.)
Jeton de service de confiance	TrST	Un objet physique ou binaire (logique) produit ou délivré en conséquence de l'utilisation d'un service de confiance. On peut citer comme exemples de TrST binaires les certificats, les listes de révocation de certificat (CRL), les jetons d'horodatage (TST) et les réponses du protocole de vérification en ligne de certificat (OCSP).
Signature électronique qualifiée	QES	Une AdES identifiée par un QC et créée par un dispositif sécurisé de création de signature tel que défini à l'article 2 de la directive 1999/93/CE.
Signature électronique avancée	AdES	Telle que définie à l'article 2, point 2), de la directive 1999/93/CE.
Signature électronique avancée identifiée par un certificat qualifié	$AdES_{QC}$	Une signature électronique qui respecte les exigences applicables aux AdES et qui est identifiée par un QC tel que défini à l'article 2 de la directive 1999/93/CE.
Dispositif sécurisé de création de signature	SSCD	Tel que défini à l'article 2, point 6), de la directive 1999/93/CE.

([1]) EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

Dans les chapitres suivants, — les mots-clés «DOIT» et «OBLIGATOIRE» et leurs différentes formes grammaticales sont à comprendre dans le sens des termes «MUST», «REQUIRED» et «SHALL» tels que décrits dans le RFC 2119, — le mot-clé «NE DOIT PAS» et ses différentes formes grammaticales sont à comprendre dans le sens des termes «MUST NOT» et «SHALL NOT» tels que décrits dans le RFC 2119, — les mots-clés «DEVRAIT» et «RECOMMANDÉ» et leurs différentes formes grammaticales sont à comprendre dans le sens des termes «SHOULD» et «RECOMMENDED» tels que décrits dans le RFC 2119, — les mots-clés «NE DEVRAIT PAS» et «NON RECOMMANDÉ» et leurs différentes formes grammaticales sont à comprendre dans le sens des termes «SHOULD NOT» et «NOT RECOMMENDED» tels que décrits dans le RFC 2119, — les mots-clés «PEUT» et «OPTIONNEL» et leurs différentes formes grammaticales sont à comprendre dans le sens des termes «MAY» et «OPTIONAL» tels que décrits dans le RFC 2119 ([1]).

CHAPITRE I

SPÉCIFICATIONS DÉTAILLÉES DU MODÈLE COMMUN POUR LA «LISTE DE CONFIANCE DE PRESTATAIRES CONTRÔLÉS OU ACCRÉDITÉS DE SERVICES DE CERTIFICATION»

Les présentes spécifications sont basées sur les spécifications et les prescriptions d'ETSI TS 119612 v1.1.1 (ci -après dénommée ETSI TS 119612).

Lorsque aucune prescription n'est prévue dans les présentes spécifications, les prescriptions des clauses 5 et 6 d'ETSI TS 119612 DOIVENT être appliquées dans leur intégralité. Lorsque des prescriptions spécifiques sont prévues dans les présentes spécifications, elles DOIVENT être appliquées à la place des prescriptions correspondantes d'ETSI TS 119612. En cas de contradiction entre les présentes spécifications et celles d'ETSI TS 119612, les présentes spécifications DOIVENT être appliquées.

Scheme operator name (clause 5.3.4)

Ce champ est OBLIGATOIRE et DOIT être conforme aux spécifications de la clause 5.3.4 de la TS 119612.

([1]) IETF RFC 2119: «Key words for use in RFCs to indicate Requirements Levels».

Un pays PEUT avoir des organismes de contrôle et d'accréditation distincts, et même des organismes différents pour différentes activités en rapport. Il appartient à chaque État membre de désigner l'exploitant du système de la liste de confiance de l'État membre. Il est à supposer que l'organisme de contrôle, l'organisme d'accréditation et l'exploitant du système (lorsqu'il s'agit d'organismes distincts) auront chacun leurs propres responsabilités.

Dans toute situation où plusieurs organismes sont responsables du contrôle, de l'accréditation ou d'aspects liés à l'exploitation du système, cette répartition des responsabilités DOIT être prise en considération et décrite en tant que telle dans les informations sur le système faisant partie de la liste de confiance, y compris dans les informations spécifiques au système fournies par le champ «Scheme information URI» (clause 5.3.7).

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 119612, selon lesquelles la dénomination suivante DOIT être utilisée pour le système:

«EN_name_value» = «Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Scheme Operator's Member State for compliance with the relevant provisions laid down in directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.»

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 119612, selon lesquelles «les informations appropriées concernant le système» DOIVENT inclure au minimum:

— Des informations introductives, communes à tous les États membres, concernant la portée et le contexte de la liste de confiance et du système de contrôle et d'accréditation sous-jacent. Le texte commun à utiliser est le suivant, où la chaîne de caractères «[*name of the relevant Member State*]» DOIT être remplacée par le nom de l'État membre concerné:

«The present list is the 'Trusted List of supervised/accredited Certification Service Providers' providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions of directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in directive 1999/93/EC,

— allowing for a trusted validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)], including, when this is not part of the QCs, information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in directive 1999/93/EC, including compliance with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of directive 1999/93/EC, in particular those laid down in Article 3(3), Article 8.(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List at a national level on a voluntary basis.»

— Des informations spécifiques sur le ou les systèmes sous-jacents de contrôle et d'accréditation, et notamment [1]:

  — des informations relatives au système de contrôle applicable à tout CSP_{QC},

  — le cas échéant, des informations sur le système national d'accréditation volontaire applicable aux CSP_{QC},

  — le cas échéant, des informations sur le système de contrôle applicable aux CSP qui ne délivrent pas de QC,

  — le cas échéant, des informations relatives au régime national d'accréditation volontaire applicable à tout CSP ne délivrant pas de QC.

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

  — une description générale,

  — des informations sur le processus adopté par l'organisme de contrôle ou d'accréditation pour contrôler ou accréditer les CSP, et sur le processus adopté par les CSP en vue d'être contrôlés ou accrédités,

  — des informations sur les critères sur lesquels porte le contrôle ou l'accréditation des CSP.

— Le cas échéant, des informations spécifiques sur les «qualifications» que certains des objets physiques ou binaires (logiques) produits ou délivrés en conséquence de la fourniture d'un service de certification sont susceptibles de recevoir sur la base de leur respect des dispositions et des exigences fixées au niveau national, y compris la signification de telles «qualifications» et les dispositions et exigences nationales en rapport.

Des informations supplémentaires sur le système spécifiques aux États membres PEUVENT être fournies sur une base volontaire, notamment:

— des informations sur les critères et les règles utilisés pour sélectionner les organismes de surveillance ou d'audit et sur la manière dont les CSP sont contrôlés (surveillés) ou accrédités (soumis à des audits) par ces organismes,

— 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 119612. Il DOIT comprendre au moins deux URI:

— 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 of supervised/accredited Certification Service Providers' providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

  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

  The Trusted List of a Member State must provide, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)], including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

[1] Les deux derniers 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 ces systèmes de contrôle et d'accréditation applicables aux CSP qui ne délivrent pas de QC. 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 renvoyant à la directive 1999/93/CE, avec la possibilité pour chaque État membre d'ajouter des textes ou des références spécifiques) prévus par le présent document. Des informations supplémentaires sur les systèmes nationaux de contrôle et d'accréditation pour les CSP ne délivrant pas de QC 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).

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in directive 1999/93/EC, including compliance with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of directive 1999/93/EC, in particular those laid down in Article 3(3), Article 8)(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a 'voluntary accreditation' system (as defined in and in compliance with directive 1999/93/EC) and/or under a nationally defined 'recognised approval scheme' implemented on a national basis for the supervision of compliance with the provisions laid down in directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Article 2(11) of directive 1999/93/EC). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific 'qualification' on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a 'qualification' is likely to be limited solely to the national level.

Interpretation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a Trusted List according to the Annex of Commission Decision [reference to the present Decision] are as follows:

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

— indicates that from the 'Service digital identifier' ('Sdi') identified CA (similarly within the CA hierarchy starting from the 'Sdi' identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) **provided** that it is claimed as such in the certificate through the use of appropriate EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

Note: if no 'Sie' 'Qualifications Extension' information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related 'Sie' 'Qualifications Extension' information, then the 'machine-processable' information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— **and IF** 'Sie' 'Qualifications Extension' information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this 'Sie' 'Qualifications Extension' information, which is constructed on the principle of a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing some additional information regarding the qualified status, the 'SSCD support' and/or 'Legal person as subject' (e.g. those 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.). Those qualifiers are part of the following set of 'Qualifiers' used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the qualified status: 'QCStatement' meaning the identified certificate(s) is(are) qualified,

AND/OR

— to indicate the nature of the SSCD support:

— 'QCWithSSCD' qualifier value meaning 'QC supported by an SSCD', or

— 'QCNoSSCD' qualifier value meaning 'QC not supported by an SSCD', or

— 'QCSSCDStatusAsInCert' qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the 'Sdi' – 'Sie' provided information in this CA/QC entry,

AND/OR

— to indicate issuance to Legal Person:

— 'QCForLegalPerson' qualifier value meaning 'Certificate issued to a Legal Person'.

The general interpretation rule for any other 'Sti' type entry is that the listed service named according to the 'Sn' field value and uniquely identified by the 'Sdi' field value has a current supervision/accreditation status according to the 'Scs' 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 Technical specifications for a Common Template for the 'Trusted List of supervised/accredited Certification Service Providers' in the Annex of Commission Decision 2009/767/EC for further details on the fields, description and meaning for the Member States' Trusted Lists.»

— un URI spécifique à la liste de confiance de chaque État membre pointant vers un texte descriptif qui DOIT s'appliquer à la TL 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 DOIVENT être évalués conformément aux systèmes respectifs de contrôle et d'accréditation volontaire 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 certification autres que ceux qui concernent la délivrance de QC. Ce texte peut être utilisé pour indiquer que les systèmes nationaux de contrôle ou de surveillance prévoient 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 à partir de 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 119612, 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 de la liste de confiance DOIVENT consister en une chaîne de caractères multilingue (au format texte seul) composée de deux parties:

1. une première partie obligatoire, commune aux listes de confiance de tous les États membres (avec l'anglais du Royaume-Uni en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales), indiquant que le cadre juridique applicable est la directive 1999/93/CE et sa mise en œuvre correspondante dans les lois de l'État membre spécifié dans le champ «Scheme Territory».

   Version anglaise du texte commun:

   «The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.»

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

Texte dans la ou les langues nationales de l'État membre: [traduction(s) officielle(s) du texte anglais ci-dessus, à savoir, pour le texte en langue française:]. «Le cadre juridique applicable à la présente implémentation TSL de la liste de confiance des prestataires de service de certification contrôlés ou accrédités pour [nom de l'État membre] est la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques et sa mise en œuvre dans le droit de [nom de l'État membre].»

2. une seconde partie facultative, spécifique à chaque liste de confiance (avec l'anglais du Royaume-Uni en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales), fournissant les références de cadres juridiques nationaux spécifiques applicables (par exemple en ce qui concerne les systèmes nationaux de contrôle ou d'accréditation de CSP qui ne délivrent pas de QC).

CHAPITRE II

CONTINUITÉ DES LISTES DE CONFIANCE

Les certificats à notifier à la Commission conformément à l'article 3, point c), de la présente décision DOIVENT être délivrés de telle façon:

— qu'ils comportent des dates de validité espacées de trois mois au minimum,

— qu'ils soient créés à partir de nouvelles paires de clés, afin qu'aucune paire de clés précédemment utilisée n'ait à être recertifiée.

En cas de compromission ou de retrait d'UNE des clés privées correspondant à la clé publique qui pourrait servir à valider la signature de la liste de confiance et qui a été notifiée à la Commission et publiée dans les listes centrales de pointeurs de la Commission, les États membres DOIVENT:

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

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

En cas de compromission ou de retrait de TOUTES les clés privées correspondant à la clé publique qui pourrait servir à valider la signature de la liste de confiance et qui a été notifiée à la Commission et publiée dans les listes centrales de pointeurs de la Commission, les États membres DOIVENT:

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

— republier, sans retard, une nouvelle liste de confiance signée 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 la liste de confiance.

CHAPITRE III

SPÉCIFICATIONS POUR LA FORME DIRECTEMENT LISIBLE DE LA LISTE DE CONFIANCE

Si une forme directement lisible (HR) de la liste de confiance est établie et publiée, elle DEVRAIT 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 forme directement lisible fondée sur PDF/A de la liste de confiance DEVRAIT respecter les exigences suivantes:

— la structure de la forme HR DEVRAIT refléter le modèle logique décrit par la TS 119612,

— chaque champ présent DEVRAIT être visible et indiquer:

  — l'intitulé du champ (p. ex. «Service type identifier»),

  — la valeur du champ (p. ex. «CA/QC»),

  — la signification (description) de la valeur du champ, le cas échéant (p. ex. «Une autorité de certification délivrant des certificats de clé publique»),

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

([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)

— les champs et valeurs correspondantes suivants des certificats numériques présents dans le champ «Service digital identity» DEVRAIENT apparaître au minimum dans la forme HR:

  — Version

  — Numéro de série

  — Algorithme de signature

  — Émetteur

  — Valide à partir de

  — Valide jusqu'à

  — Objet

  — Clé publique

  — Règles de certificat

  — Identifiant de la clé de l'objet

  — Points de distribution CRL

  — Identifiant de la clé de l'autorité

  — Utilisation de la clé

  — Contraintes de base

  — Algorithme d'empreinte

  — Empreinte

— la forme HR DEVRAIT être facilement imprimable,

— La forme HR DOIT être signée par l'exploitant du système, conformément au profil de base des signatures PAdES [1].

[1] ETSI TS 103172 (mars 2012) — Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile