Ce document constitue un outil de documentation et n'engage pas la responsabilité des institutions

►B ►C1 **DÉCISION 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

[notifiée sous le numéro C(2009) 7806]

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

(2009/767/CE) ◄

(JO L 274 du 20.10.2009, p. 36)

Modifiée par:

		Journal officiel		
		n°	page	date
►M1	Décision 2010/425/UE de la Commission du 28 juillet 2010	L 199	30	31.7.2010
►M2	Règlement (UE) nº 519/2013 de la Commission du 21 février 2013	L 158	74	10.6.2013

Rectifiée par:

►C1 Rectificatif, JO L 299 du 14.11.2009, p. 18 (2009/767/CE)
►C2 Rectificatif, JO L 4 du 7.1.2011, p. 6 (2009/767/CE)

▼B
▼C1

DÉCISION 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

[notifiée sous le numéro C(2009) 7806]

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

(2009/767/CE)

LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES,

vu le traité instituant la Communauté 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) Parmi les obligations de simplification administrative imposées aux États membres par le chapitre II de la directive 2006/123/CE, et notamment les articles 5 et 8, figure l'obligation de veiller à ce que les procédures et formalités relatives à l'accès à une activité de service et à son exercice puissent être effectuées facilement, à distance et par voie électronique, par l'intermédiaire des «guichets uniques».

(2) Ces procédures et formalités doivent pouvoir être exécutées par-delà les frontières entre États membres, par l'intermédiaire des «guichets uniques», conformément à l'article 8 de la directive 2006/123/CE.

(3) Pour que l'obligation consistant à simplifier les procédures et les formalités et à faciliter l'utilisation transfrontalière des «guichets uniques» soit respectée, les procédures exécutées par voie électronique devraient faire appel à des solutions simples, notamment en ce qui concerne l'utilisation des signatures électroniques. Dans les cas où un niveau élevé de sécurité ou une équivalence à une signature manuscrite sont jugés nécessaires après que les formalités et procédures concrètes ont fait l'objet d'une évaluation des risques appropriée, les prestataires de services pourraient avoir à fournir, pour certaines procédures et formalités, des signatures électroniques avancées qui sont basées sur des certificats qualifiés avec ou sans dispositif sécurisé de création de signature.

[1] JO L 376 du 27.12.2006, p. 36.

▼C1

(4) Le cadre communautaire relatif aux signatures électroniques a été établi par la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques ([1]). Afin de faciliter l'utilisation transfrontalière effective des signatures électroniques avancées basées sur des certificats qualifiés, il convient de renforcer la confiance inspirée par ces signatures, quel que soit l'État membre dans lequel le signataire ou le prestataire de service de certification qui délivre le certificat qualifié est établi. Pour ce faire, il pourrait être envisagé de rendre les informations nécessaires pour valider les signatures électroniques plus facilement disponibles sous une forme fiable, notamment les informations relatives aux prestataires de services de certification contrôlés ou accrédités dans un État membre et aux services qu'ils offrent.

(5) Afin de faciliter l'utilisation de ces informations et de garantir un niveau de détail approprié permettant au destinataire de valider la signature électronique, il convient que les États membres fassent figurer ces informations dans un modèle commun mis à la disposition du public,

A ARRÊTÉ LA PRÉSENTE DÉCISION:

Article premier

Utilisation et acceptation de signatures électroniques

1. Pour l'exécution de certaines procédures et formalités par voie électronique par l'intermédiaire des guichets uniques visés à l'article 8 de la directive 2006/123/CE, les États membres peuvent imposer, si cela se révèle justifié sur la base d'une évaluation des risques encourus et conformément à l'article 5, paragraphes 1 et 3, de ladite directive, que le prestataire de service utilise des signatures électroniques avancées qui soient basées sur des certificats qualifiés, avec ou sans dispositif sécurisé de création de signature, conformément aux définitions et aux dispositions de la directive 1999/93/CE.

2. Les États membres acceptent, pour l'exécution des procédures et formalités visées au paragraphe 1, toute signature électronique avancée basée sur un certificat qualifié, avec ou sans dispositif sécurisé de création de signature, sans préjudice de la possibilité qu'ils ont de limiter cette acceptation aux signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature, si l'évaluation des risques mentionnée au paragraphe 1 le justifie.

3. Les États membres ne subordonnent pas l'acceptation de signatures électroniques avancées basées sur un certificat qualifié, avec ou sans dispositif sécurisé de création de signature, à des exigences qui créent des obstacles à l'utilisation, par les prestataires de services, de procédures exécutées par voie électronique par l'intermédiaire des guichets uniques.

([1]) JO L 13 du 19.1.2000, p. 12.

▼C1

4. Sans préjudice du paragraphe 2, les États membres peuvent accepter des signatures électroniques autres que des signatures électroniques avancées basées sur un certificat qualifié, avec ou sans dispositif sécurisé de création de signature.

Article 2

Établissement, mise à jour et publication de listes de confiance

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 en annexe, une «liste de confiance» qui contient les informations minimales concernant ces prestataires.

▼M1

2. Les États membres établissent et publient une version directement lisible et une version destinée à un traitement électronique de la liste de confiance conformément aux spécifications figurant en annexe.

2 *bis*. Les États membre signent électroniquement la version destinée à un traitement électronique de leur liste de confiance et publient, au minimum, la version directement lisible de la liste de confiance par l'intermédiaire d'un canal sécurisé afin de garantir son authenticité et son intégrité.

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 des versions directement lisibles et des versions destinées à un traitement électronique de la liste de confiance;

b) l'emplacement où la version directement lisible et celle destinée à un traitement automatique de la liste de confiance sont publiées;

c) le certificat de clé publique utilisé pour mettre en œuvre le canal sécurisé par lequel la version directement lisible de la liste de confiance est publiée ou, si celle-ci est signée électroniquement, le certificat de clé publique utilisé pour la signer;

d) le certificat de clé publique utilisé pour signer électroniquement la version destinée à un traitement électronique de la liste de confiance;

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

4. La Commission met à la disposition de tous les États membres, par l'intermédiaire d'un canal sécurisé vers un serveur informatique authentifié, les informations visées au paragraphe 3, telles qu'elles ont été communiquées par les États membres, sous une forme directement lisible et sous une forme destinée à un traitement électronique.

▼C1

Article 3

Application

La présente décision s'applique à compter du 28 décembre 2009.

Article 4

Destinataires

Les États membres sont destinataires de la présente décision.

▼C1

ANNEXE

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

PRÉFACE

1. **Généralités**

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 que pourraient suivre tous les États membres pour la fourniture d'informations concernant le statut de contrôle ou d'accréditation des services de certifications 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, y compris en ce qui concerne la fourniture d'informations relatives à l'historique du statut de contrôle ou d'accréditation des services de certification contrôlés ou accrédités.

Les informations devant figurer obligatoirement dans la liste de confiance (TL) doivent comprendre un minimum d'informations relatives aux CSP contrôlés ou accrédités qui délivrent des certificats qualifiés (QC) ([2]) conformément aux dispositions de la directive 1999/93/CE [article 3, paragraphes 2 et 3, et article 7, paragraphe 1, point a)], et notamment des informations concernant le QC sur lequel repose une signature électronique et le recours éventuel à un dispositif sécurisé de création de signature (SSCD) ([3]) pour créer la signature.

Des informations supplémentaires concernant d'autres CSP contrôlés ou accrédités ne délivrant pas de QC mais fournissant 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.

Ces informations sont essentiellement destinées à étayer la validation de signatures électroniques qualifiées (QES) et de signatures électroniques avancées (AdES) ([4]) reposant sur un certificat qualifié ([5]) ([6]).

Le modèle commun proposé est compatible avec une mise en œuvre fondée sur la spécification ETSI TS 102 231 ([7]) qui traite des questions d'établissement, de publication, d'accès, d'emplacement, d'authentification et de confiance relatives à ce type de liste.

([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 10), de la directive 1999/93/CE.
([3]) Voir la définition de l'article 2, point 6), de la directive 1999/93/CE.
([4]) Voir la définition de l'article 2, point 2), de la directive 1999/93/CE.
([5]) Pour les SEA reposant sur un CQ, l'acronyme «SEA_{CQ}» sera utilisé dans le présent document.
([6]) Il convient de souligner qu'il existe un certain nombre de services électroniques fondés sur de simples SEA 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.
([7]) ETSI TS 102 231 — Signatures électroniques et infrastructures (ESI): exigences relatives aux renseignements sur le statut des fournisseurs de services de confiance.

▼C1

2. **Lignes directrices relatives aux entrées de la liste de confiance (TL)**

2.1. *Une TL axée sur les services de certification contrôlés ou accrédités*

Services de certification et prestataires de services de certification pertinents dans une liste unique

La liste de confiance d'un État membre se définit comme «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 doit couvrir:

— 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, et 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],

  — 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.

▼C1

La liste de confiance (TL) d'un État membre doit fournir un minimum d'informations relatives aux CSP contrôlés ou accrédités qui délivrent des certificats qualifiés (QC) au public conformément aux dispositions de la directive 1999/93/CE [article 3, paragraphes 2 et 3, et article 7, paragraphe 1, point a)], et notamment des informations concernant le QC sur lequel repose une signature électronique et le recours éventuel à un dispositif sécurisé de création de signature pour créer la signature.

Des informations supplémentaires concernant services contrôlés ou accrédités fournis par des CSP ne délivrant pas de QC au public (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.

La liste de confiance vise à:

— recenser et fournir des informations fiables concernant le statut de contrôle ou d'accréditation des services de certification fournis par les prestataires de services de certification qui sont contrôlés ou accrédités par l'État membre responsable de l'établissement et de la mise à jour de la liste aux fins du respect des dispositions pertinentes de la directive 1999/93/CE,

— faciliter la validation des signatures électroniques reposant sur les services de certification contrôlés ou accrédités fournis par les CSP figurant sur la liste.

Un ensemble unique de valeurs de statut de contrôle ou d'accréditation

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 de supervision des services de certification fournis par les CSP contrôlés ou accrédités par cet État membre.

Le fait qu'un service donné soit contrôlé ou accrédité fait partie de son statut. En outre, le statut de contrôle ou d'accréditation peut être en «cours de validité», «en cours de suspension», «suspendu» ou même «révoqué». Un même service de certification peut, au cours de sa durée de vie, passer du statut contrôlé au statut accrédité 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.

▼C1

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

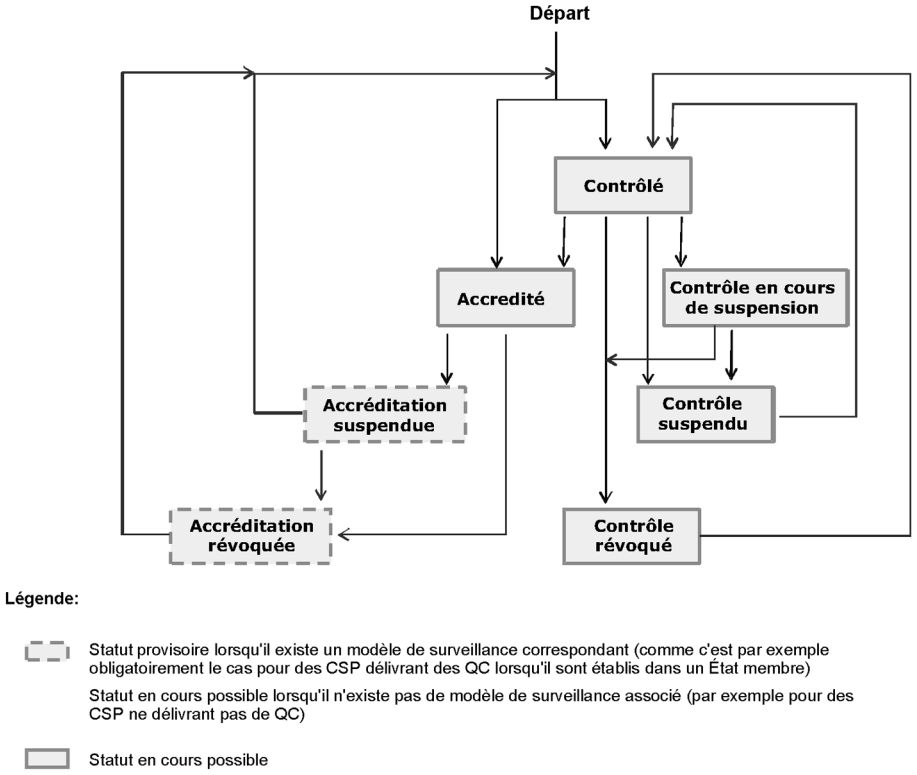


Figure 1

Un service de certification délivrant des QC doit être contrôlé (s'il est établi dans un État membre) et peut faire l'objet d'une accréditation volontaire. Lorsque ce service figure dans une liste de confiance, son statut peut correspondre à l'une quelconque des possibilités mentionnées plus haut. Toutefois, il faut noter que les statuts accréditation suspendue et accréditation révoquée ne peuvent être des statuts provisoires que dans le cas de services de CSP_{QC} établis dans un État membre, puisque ce type de service doit, par défaut, être contrôlé (même lorsqu'il n'est pas ou plus accrédité).

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 aux dispositions de la directive 1999/93/CE, avec, éventuellement, des dispositions nationales relatives à la fourniture de services de certification [au sens de l'article 2, point 11), de la directive] doivent répartir ces régimes 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 à la directive 1999/93/CE et mis en œuvre par des dispositions et exigences nationales respectant la législation nationale.

▼C1

En conséquence, un service de certification ne délivrant pas de certificats qualifiés peut être contrôlé ou faire l'objet d'une accréditation volontaire. Lorsque ce service figure dans une liste de confiance, son statut peut correspondre à l'une quelconque des possibilités mentionnées plus haut (voir figure 1).

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 relatives au système de contrôle applicable à tout CSP ne délivrant 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 du «Scheme information URI» (clause 5.3.7 – information fournie par les États membres), des «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 de la «TSL policy/legal notice» (clause 5.3.11 – un texte commun à tous les États membres qui renvoie à la directive 1999/93/CE, chaque État membre ayant la possibilité d'ajouter des références ou des textes qui lui soient 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 de l'extension «additionalServiceInformation» (clause 5.8.2) qui fait partie de la «Service information extension» (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 qu'une seule entrée par service de certification (identifié par sa «Service digital identity» selon ETSI TS 102 231 [1]) et de mettre à jour son statut de contrôle/accréditation selon les besoins. La signification des statuts précités est expliquée dans la clause 5.5.4 des spécifications détaillées figurant dans le chapitre I.

2.2. *Entrées de TL destinées à faciliter la validation des QES et des $AdES_{QC}$*

Lors de la création de la TL, la partie la plus critique consiste à établir la partie obligatoire de la TL, c'est-à-dire 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 de fin délivré par le CSP dans le cadre du service de certification mentionné dans cette entrée).

[1] ETSI TS 102 231 — *Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information*.

▼C1

Dans la mesure où il n'existe pas de profil de QC réellement interopérable et transfrontalier, les informations requises peuvent comporter d'autres informations que la «Service digital identity» d'une seule CA (racine), en particulier les informations qui identifient le statut de QC du certificat délivré et celles qui concernent le recours éventuel à un dispositif sécurisé de création de signature (SSCD) pour créer les signatures. Au niveau de l'État membre, l'organisme chargé d'établir, de modifier et de tenir à jour la TL (soit l'«exploitant du système» au sens de ETSI TS 102 231) doit donc tenir compte du profil et du contenu de certificat en cours dans chaque QC délivré, pour chaque CSP_{QC} couvert par la TL.

Idéalement, chaque QC délivré devrait comprendre la déclaration de conformité de QC définie par l'ETSI ([1]) 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 pour la stratégie en matière de certificats (OID) QCP/QCP+ définis par ETSI TS 101 456 ([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). Par conséquent, les parties qui s'appuient sur des certificats ne peuvent pas simplement se baser sur le certificat du signataire (et sur la chaîne ou le chemin associé) pour établir, au moins d'une manière lisible en machine, 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.

Grâce aux informations fournies par le champ «Service information extensions» («Sie») et entrées dans les champs «Service type identifier» («Sti»), «Service name» («Sn») et «Service digital identity» («Sdi») ([3]), le modèle commun de TL proposé permet de définir sans ambiguïté un type spécifique de certificat qualifié délivré par un service de certification listé fourni par un CSP délivrant des QC et de savoir s'il repose ou non sur un SSCD (lorsque ces informations ne figurent pas dans le QC délivré). À cette entrée est naturellement associée une information spécifique de «Service current status» («Scs»). La situation est illustrée par la figure 2 ci-dessous.

Le fait de lister un service en fournissant seulement le «Sdi» d'une AC (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 de fin délivré par cette (hiérarchie) de CA (Racine) contient suffisamment d'informations définies par l'ETSI et lisibles en machine 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 et lisibles en machine permettant de savoir s'il repose ou non sur un SSCD), en ne listant 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. Afin de pouvoir considérer que ces QC reposent sur un SSCD, ce fait doit être indiqué par le «Sie» (cela indique aussi que le fait est garanti par le CSP délivrant des QC et contrôlé/accrédité par l'organisme de contrôle ou d'accréditation).

([1]) Voir ETSI TS 101 862 — *Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile*.

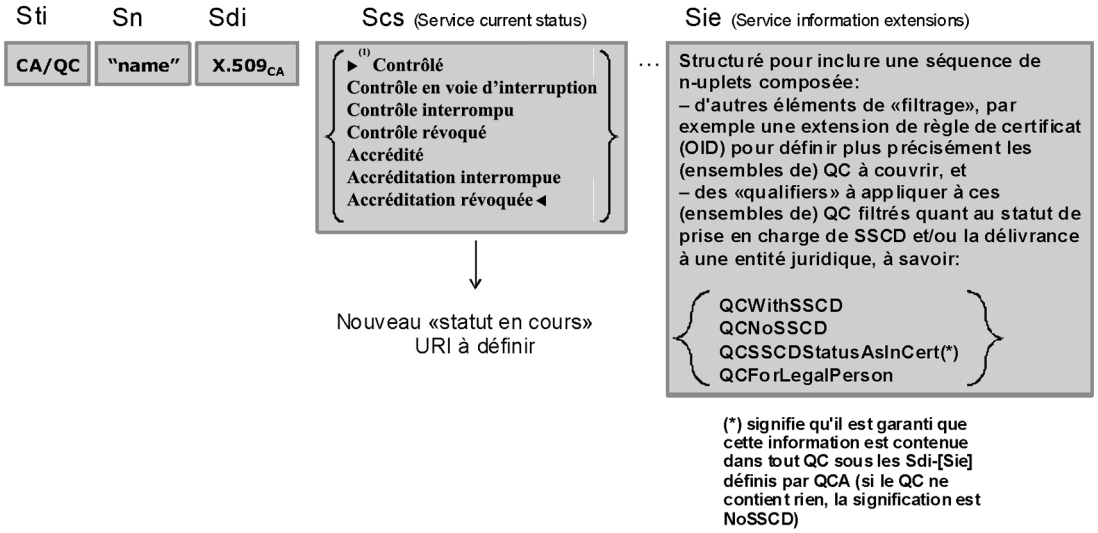
([2]) Voir ETSI TS 101 456 — *Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates*.

([3]) Soit, au minimum, un certificat X.509 v3 de la QCA de délivrance ou d'une CA supérieure dans le chemin de certification.

▼C1

Principes généraux — règles de modification — entrées CSP_{QC} (services listés)

Entrée concernant un service pour un CSP_{QC} listé:



▶(1) C2

Figure 2

Entrée concernant un service pour un CSP listé délivrant des QC dans la TL mise en œuvre au format TSL

Les spécifications techniques relatives au modèle commun de TL actuelles permettent d'utiliser une combinaison de cinq grands types d'information pour l'entrée correspondant au service:

— le «Service type identifier» («Sti»), c'est-à-dire l'identification de l'AC 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) le certificat X.509v3 d'une CA qui délivre des QC,

— pour les services CA/QC, des informations facultatives relatives aux «Service information extensions» («Sie») qui permettront d'inclure 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, le service spécifique (c'est-à-dire l'ensemble de certificats qualifiés) pour lequel des informations supplémentaires sont requises/fournies en ce qui concerne la mention de 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 identifié plus précisément repose ou non sur un SSCD ou si ces informations associées font partie du QC sous une forme normalisée lisible en machine, 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),

▼C1

— 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.

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

Pour la création et la modification des entrées, 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 ou d'accréditation) que, pour un service listé 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 d'objet (OID) QCP+, 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 l'organisme de contrôle ou d'accréditation) que, pour un service listé et identifié par un «Sdi», tout QC ne reposant pas sur un SSCD contient bien soit la déclaration de conformité Qc définie par l'ETSI et/ou l'OID QCP, et qu'il n'est pas censé contenir la déclaration QcSSCD ou l'OID QCP+, 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 (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 l'organisme de contrôle ou d'accréditation) 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 à différents CSP ou à d'autres informations spécifiques au CSP se trouvant dans le QC, directement ou indirectement, lisible en machine ou non) mais qu'il ne contient ni la déclaration QcSSCD NI l'OID QCP(+) de l'ETSI, alors l'utilisation d'un «Sdi» approprié peut ne pas être suffisante et le champ «Sie» doit être utilisé afin que des informations concernant la prise en charge par un SSCD soient explicitement mentionnées, ainsi qu'une éventuelle extension d'information destinée à identifier l'ensemble de certificats couvert. Il est possible que différentes «SSCD support information values» doivent être utilisées 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 l'organisme de contrôle ou d'accréditation) que, pour un service listé et identifié par un «Sdi», pour l'un quelconque des QC, la déclaration de conformité Qc, l'OID QCP, la déclaration QcSSCD ou l'OID QCP+ soit absent, mais qu'il est garanti que certains des certificats d'entité de fin 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 à différents CSP_{QC} ou à d'autres informations spécifiques au CSPQC se trouvant dans le QC, directement ou indirectement, lisible en machine ou non), l'utilisation d'un «Sdi» approprié n'est pas suffisante et le champ «Sie» doit être utilisé afin que des informations concernant la prise en charge par un SSCD soient explicitement mentionnées. Il est possible que différentes «SSCD support information values» doivent être utilisées pour un même «Sdi» lorsque le champ «Sie» est utilisé.

▼C1

Le principe général par défaut veut que, pour chaque CSP figurant sur la liste de confiance, il y ait une entrée relative au service par certificat X.509v3 pour un service de vérification de type CA/QC, c'est-à-dire une autorité de certification délivrant (directement) des QC. Dans certaines circonstances soigneusement déterminées et dans des conditions strictement surveillées, l'organisme de contrôle/accréditation d'un État membre peut décider d'utiliser le certificat X.509v3 d'une CA Racine ou de niveau supérieur (c'est-à-dire une autorité de certification qui ne délivre pas directement des QC d'entité de fin mais qui certifie une hiérarchie de CA jusqu'aux CA qui délivre les QC aux entités finales) comme «Sdi» d'une entrée donnée de la liste des services fournis par un CSP de la liste. Les États membres doivent soigneusement examiner les conséquences (avantages et inconvénients) liées à l'utilisation d'un certificat X.509v3 d'une CA Racine ou de niveau supérieur comme «Sdi» d'une entrée relative aux services de la liste de confiance et les assumer. 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.

Pour illustrer les lignes directrices générales pour la création et la modification des entrées, on peut prendre l'exemple suivant: 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 mais aucune mention relative à une éventuelle prise en charge par un SSCD, le fait de faire uniquement figurer le «Sdi» de la CA Racine dans la liste signifierait, suivant les règles exposées ci-dessus, que tout QC délivré par cette hiérarchie de CA Racine ne repose pas sur un SSCD. Si, en fait, ces QC reposent bien sur un SSCD, 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 TSL doit utiliser le champ «Sie» et les extensions «Qualifications» associées, par exemple des certificats de filtrage grâce à des OID spécifiques à des CSP_{QC} pouvant 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 ajouter des informations explicites de «SSCD support information» en ce qui concerne les certificats filtrés par l'utilisation de «Qualifiers».

Les lignes directrices générales pour l'utilisation des applications, services ou produits liés aux signatures électroniques reposant sur la mise en œuvre TSL d'une liste de confiance, conformément aux présentes spécifications techniques, sont les suivantes:

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

— indique que tous les certificats d'entité de fin 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 grâce aux déclarations Qc appropriées (c'est-à-dire QcC, QcSSCD) et/ou aux OID QCP(+) définies par l'ETSI (et que cela est garanti par l'organisme de contrôle/accréditation, voir ci-dessus les lignes directrices générales pour la création et la modification des entrées).

Note: En l'absence d'information «Sie» de qualification ou si le certificat d'entité de fin qui est déclaré être un QC n'est pas identifié plus précisément par une entrée «Sie» liée, les informations lisibles en machine se trouvant dans le QC sont contrôlées/accréditées comme des informations exactes. Cela signife qu'il est garanti que l'utilisation (ou non) des déclarations Qc appropriées (c'est-à-dire QcC, QcSSCD) et/ou d'OID QCP(+) définis par l'ETSI est conforme à ce qui est annoncé par le CSP_{QC},

▼C1

— et si des informations «Sie» de qualification sont présentes, 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 qualification, construite sur le principe d'une séquence de filtres qui identifient un ensemble supplémentaire de certificats et fournissent des informations supplémentaires en ce qui concerne la prise en charge par un SSCD et/ou la personne morale (c'est-à-dire les certificats qui contiennent un OID spécifique dans l'extension de politique 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.) doivent être examinés en fonction de l'ensemble suivant de «qualifiers», qui compensent l'absence d'informations dans les QC correspondants, c'est-à-dire:

— qu'ils indiquent la prise en charge par un SSCD éventuelle:

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

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

  — la valeur «QCSSCDStatusAsInCert» signifie 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

— qu'ils indiquent la délivrance à une personne morale:

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

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

Il convient de couvrir également les cas dans lesquels les réponses CRL et OCSP sont signées par des clés autres que celles qui proviennent d'une CA délivrant des QC («CA/QC»). Pour ce faire, il est possible, dans la liste de confiance de faire figurer ces services avec un «Service type identifier» complété par une extension «additionalServiceInformation» qui signale un service OCSP ou CRL faisant partie de la fourniture des QC, par exemple avec un type de service de «OCSP/QC» ou «CRL/QC», 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 se trouvant dans la hiérarchie d'un service CA/QC figurant sur une 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») utilisant les types de services par défaut ETSI TS 102 231 OCSP et CRL.

Il faut noter que la mise en œuvre TSL de la liste de confiance doit comprendre des services de révocation lorsque les informations liées ne sont pas présentes dans le champ AIA des certificats finaux ou lorsqu'elles ne sont pas signées par une CA qui fait partie des CA de la liste.

2.5. *Transition vers un profil de QC interopérable*

Il faut, en règle générale, essayer de simplifier (réduire) le plus possible le nombre d'entrées de services («Sdi» différents). Toutefois, il convient de garder à l'esprit la nécessité de maintenir une identification correcte des services liés à la délivrance des QC et à la fourniture d'informations de confiance relatives à l'éventuelle existence d'une prise en charge par un SSCD sur laquelle reposeraient les QC, lorsque cette information ne se trouve pas dans le QC délivré.

▼C1

Idéalement, le recours au champ «Sie» et à l'extension «Qualification» devrait être (strictement) limité aux cas particuliers qui doivent être résolus de cette manière, car les QC pourraient contenir suffisamment d'informations relatives au statut qualifié déclaré et à l'absence ou à l'existence déclarée d'un SSCD.

Les États membres devraient, dans la mesure du possible, veiller à l'adoption et à l'utilisation de profils de QC interopérables.

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

La structure du modèle commun de liste de confiance proposé aux États membres comprendra les catégories d'informations suivantes:

1) informations sur la liste de confiance et son régime en matière de délivrance;

2) une séquence de champs contenant des informations d'identification dénuées d'ambiguïté sur chaque CSP contrôlé/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, ce qui signifie qu'aucun CSP n'est soit contrôlé soit accrédité dans l'État membre associé dans le cadre de la liste de confiance;

3) pour chaque CSP de la liste, une séquence de champs contenant des informations d'identification dénuées d'ambiguïté sur un service contrôlé/accrédité fourni par le CSP (cette séquence doit comporter au minimum une entrée);

4) pour chaque service de certification contrôlé/accrédité de la liste, l'identification du statut en cours du service et l'historique de ce statut.

Dans le cas d'un CSP délivrant des QC, l'identification dénuée d'ambiguïté d'un service de certification contrôlé/accrédité devant figurer dans la liste doit tenir compte des cas où le certificat qualifié ne contient pas suffisamment d'informations 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 CA qualifiée délivrant des certificats uniques pour délivrer plusieurs types de certificats d'entité de fin, qualifiés et non qualifiés.

Le nombre d'entrées dans la liste par CSP reconnu peut être réduit lorsqu'il existe un ou plusieurs services CA de niveau supérieur, par exemple dans le cas d'une hiérarchie commerciale de CA allant de la CA Racine aux CA délivrant les certificats. Même dans ce type de cas, cependant, il est impératif de maintenir et de garantir le principe consistant à faire en sorte qu'il existe un lien dénué d'ambiguïté entre le service de certification CSP_{QC} et l'ensemble de certificats à identifier.

1. *Informations sur la liste de confiance et son régime en matière de délivrance*

Cette catégorie comportera notamment les informations suivantes:

— une étiquette de liste de confiance facilitant l'identification de la liste de confiance au cours des recherches électroniques et permettant aussi de confirmer son objet lorsqu'elle est sous forme directement lisible,

— un format de liste de confiance et un identifiant de version de format,

— un numéro d'ordre (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,

▼C1

— des informations sur le propriétaire de 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) auquel 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 (historique),

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

— la date et l'heure de publication de la liste de confiance et de la prochaine mise à jour prévue.

2. *Informations d'identification dénuées d'ambiguïté sur chaque CSP reconnu dans le cadre du système*

Dans cet ensemble d'informations figureront au moins:

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

— l'adresse et les coordonnées du CSP,

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

3. *Pour chaque CSP de la liste, une séquence de champs contenant des informations d'identification dénuées d'ambiguïté sur un service 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:

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

— la dénomination (commerciale) de ce service de certification,

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

— des informations complémentaires sur le service de certification (par exemple, informations mentionnées directement ou par référence à un site à partir duquel ces informations peuvent être téléchargées, informations d'accès relatives au service),

— pour les services CA/QC, une séquence facultative de n-uplets d'information, chacun de ces n-uplets fournissant:

  i) les critères à utiliser pour identifier plus précisément (filtrer), sous le service de certification identifié «Sdi», le service spécifique (c'est-à-dire l'ensemble de certificats qualifiés) pour lequel des informations supplémentaires sont requises/fournies en ce qui concerne la mention d'une prise en charge par un SSCD (et/ou la délivrance à une personne morale), et

  ii) les informations associées («qualifiers») indiquant si l'ensemble de certificats qualifiés fourni par ce service identifié plus précisément repose 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).

▼C1

4. *Pour chaque service de certification de la liste, l'identification du statut en cours du service et l'historique de ce statut*

Dans cet ensemble d'informations figureront au moins:

— un identifiant du statut en cours,

— la date et l'heure de début du statut en cours,

— l'historique de ce statut.

4. **Sigles et définitions**

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	Une autorité de certification est un CSP. Elle peut utiliser les clés de signature privées de plusieurs CA techniques, un certificat étant associé à chacune d'elles, afin de délivrer des certificats d'entité finale. Une CA est une autorité à laquelle un ou plusieurs utilisateurs font confiance pour la création et la délivrance de certificats. De manière facultative, la CA peut créer les clés des utilisateurs (ETSI TS 102 042). La CA est supposée identifiée via les informations d'identification présentes dans le champ Issuer du certificat de la CA servant à certifier la clé publique associée à la clé de signature privée de la CA et qui, en pratique, est utilisée par la CA pour délivrer des certificats d'entités. Une CA peut utiliser plusieurs clés de signature. Chaque clé de signature d'une CA est identifiée par un identifiant unique dans le champ Authority Key Identifier du certificat de la CA.
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	«Contrôle» est utilisé au sens de 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.

▼C1

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 102 231.
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 102 231).
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 CRL, les jetons d'horodatage et les réponses OCSP.
Signature électronique qualifiée	QES	Une AdES identifiée par un QC et créée par un SSCD 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.

CHAPITRE I

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

Dans la partie suivante du document,

— 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 est 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]).

►M1 Les présentes spécifications sont fondées sur les spécifications et les prescriptions d'ETSI TS 102 231 v.3.1.2. Lorsque aucune prescription n'est prévue dans les présentes spécifications, les prescriptions d'ETSI TS 102 231 v.3.1.2 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 102 231 tout en étant complétées par les spécifications dudit document en ce qui concerne la forme. En cas de contradiction entre les présentes spécifications et celles d'ETSI TS 102 231, les présentes spécifications DOIVENT être appliquées.

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

▼C1

La prise en charge des langues DOIT être mise en œuvre, au minimum pour l'anglais (EN), et éventuellement pour une ou plusieurs langues nationales supplémentaires.

L'indication de la date et de l'heure DOIT être conforme à la clause 5.1.4 d'ETSI TS 102 231.

L'utilisation des URI DOIT être conforme à la clause 5.1.5 d'ETSI TS 102 231.

Information sur le système de délivrance de la liste de confiance

Tag

TSL tag (clause 5.2.1)

Ce champ est OBLIGATOIRE et DOIT être conforme à la clause 5.2.1 d'ETSI TS 102 231.

▼M1

_____

▼C1

Scheme Information

TSL version identifier (clause 5.3.1)

Ce champ est OBLIGATOIRE et DOIT avoir la valeur «3» (entier). TSL sequence number (clause 5.3.2)

TSL sequence number (clause 5.3.2)

▼M1

Ce champ est OBLIGATOIRE. Il DOIT spécifier le numéro de séquence de la TSL. Cette valeur entière, commençant à «1» pour la première publication de la TSL, DOIT être incrémentée à chaque nouvelle publication de la TSL. Elle NE DOIT PAS être réinitialisée à «1» lorsque le «TSL version identifier» ci-dessus est incrémenté.

▼C1

TSL type (clause 5.3.3)

▼M1

Ce champ est OBLIGATOIRE. Il indique le type de TSL. Sa valeur DOIT être http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

Note: afin de respecter la clause 5.3.3 d'ETSI TS 102 231 et d'indiquer le type spécifique de TSL en se référant à l'existence des présentes spécifications régissant l'établissement de l'implémentation TSL des listes de confiance des États membres ([1]), et de permettre à un analyseur syntaxique de déterminer laquelle des formes des champs suivants ([2]) est employée lorsque ces champs ont des sens spécifiques (ou différents) selon le type de TSL représenté (en l'occurrence, une liste de confiance d'un État membre), l'URI spécifique ci-dessus DOIT être enregistré et décrit comme suit:

([1]) Autrement dit, les «listes 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» (les «listes de confiance»).

([2]) Autrement dit, les champs spécifiés par les spécifications ETSI TS 102 231, *Electronic Signatures and Infrastructures: Provision of harmonized Trust-service status information*, telles que «profilées» par les présentes spécifications aux fins de la mise en place des listes de confiance des États membres.

▼M1

URI: (Generic) http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic

▼C1

Description: une implémentation TSL d'une liste indiquant le statut, en matière de contrôle ou d'accréditation, de services de certification fournis par des prestataires de services de certification qui sont contrôlés ou accrédités par les États membres référencés, en ce qui concerne le respect des dispositions pertinentes de la directive 1999/93/CE, par un processus de surveillance directe (volontaire ou réglementaire).

Scheme operator name (clause 5.3.4)

Ce champ est OBLIGATOIRE. Il DOIT spécifier le nom de l'organisme de l'État membre chargé d'établir, de publier et de tenir à jour la liste de confiance nationale. Il DOIT spécifier le nom officiel sous lequel agit l'entité juridique ou mandatée (par exemple dans le cas d'agences gouvernementales administratives) associée à cet organisme. Ce nom DOIT être celui employé dans l'acte officiel d'enregistrement ou d'autorisation et auquel toute communication doit être adressée. Il DOIT être une séquence de chaînes de caractères multilingues, qui DOIT être implémentée avec l'anglais (EN) en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales.

Note: un pays PEUT avoir des organismes de contrôle et d'accréditation distincts, et même des organismes différents pour différentes activités liées à l'exploitation. ►M1 Il revient à chaque État membre de désigner l'exploitant du système de l'implémentation TSL 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 TL, y compris dans les informations spécifiques au système fournies par le «Scheme information URI» (clause 5.3.7).

▼M1

L'exploitant nommé du système (clause 5.3.4) est l'entité qui signe la TSL.

▼C1

Scheme operator address (clause 5.3.5)

Ce champ est OBLIGATOIRE. Il DOIT spécifier l'adresse de l'entité juridique ou mandatée spécifiée dans le champ «Scheme operator name» (clause 5.3.4) pour les communications tant postales qu'électroniques. Il DOIT contenir «PostalAddress» (c'est-à-dire le nom et le numéro de la rue, la ville, [la région ou la province], [le code postal] et le code pays ISO 3166-1 alpha-2) d'une manière qui soit conforme à la clause 5.3.5.1, ainsi que «ElectronicAddress» (c'est-à-dire l'adresse électronique et/ou l'URI du site web) d'une manière qui soit conforme à la clause 5.3.5.2.

Scheme name (clause 5.3.6)

Ce champ est OBLIGATOIRE. Il indique le nom du système. Il DOIT contenir une séquence de chaînes de caractères multilingues, avec l'anglais (EN) en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales, définie comme suit:

▼C1

— la version anglaise (EN) DOIT être une chaîne de caractères structurée comme suit:

CC:EN_name_value

où:

— «CC» est le code pays ISO 3166-1 alpha-2 utilisé dans le champ «Scheme territory field» (clause 5.3.10),

— «:» est utilisé en tant que séparateur,

▼M1

— «EN_name_value» «Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in directive 1999/93/EC and its implementation in the referenced Member State's laws,»

▼C1

— les éventuelles versions dans les langues nationales des États membres DOIVENT chacune être une chaîne de caractères structurée comme suit:

CC:name_value

où

— «CC» est le code pays ISO 3166-1 alpha-2 utilisé dans le champ «Scheme territory field» (clause 5.3.10),

— «:» est utilisé en tant que séparateur,

— «name_value» est la traduction officielle, dans la langue nationale, de «EN_name_value» ci-dessus, à savoir, pour la langue française: «Liste du statut, en matière de contrôle ou d'accréditation, des services de certification fournis par des prestataires de services de certification, contrôlés ou accrédités par l'État membre visé exploitant du système, en ce qui concerne le respect des dispositions pertinentes de la directive 1999/93/CE.»

Le nom du système est nécessaire pour identifier de manière unique, par son nom, le système visé par le «Scheme information URI», et pour garantir que lorsque l'exploitant de système exploite plusieurs systèmes, ils portent tous un nom distinct.

Les États membres et les exploitants de système DOIVENT s'assurer que lorsqu'un État membre ou un exploitant de système exploite plusieurs systèmes, un nom distinct est donné à chacun d'eux.

Scheme information URI (clause 5.3.7)

Ce champ est OBLIGATOIRE et DOIT spécifier le ou les URI où les utilisateurs (les parties qui s'appuient sur le certificat) peuvent obtenir des informations spécifiques sur le système, avec l'anglais (EN) en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales. Il DOIT contenir une séquence de pointeurs multilingues, avec l'anglais (EN) en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales. Le ou les URI référencés DOIVENT fournir un chemin vers des «informations adéquates sur le système».

Ces «informations adéquates sur le système» DOIVENT comprendre au minimum:

— des informations introductives générales, 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:

▼C1

«The present list is the TSL implementation of [*name of the relevant Member State*] "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,

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3,2 and Art. 7.1(a)), including 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 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 Art. 3,3, Art. 8,1, Art. 11 (respectively, Art.2.13, Art. 3,2, Art 7.1(a), Art. 8,1, Art. 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 and the present TSL implementation 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 sur le système de surveillance applicable aux CSP_{QC},

([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 tels systèmes de surveillance et d'accréditation. Ces informations doivent être fournies au niveau de la TL 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 visant la directive 1999/93/CE, chaque État membre ayant la possibilité d'ajouter des textes ou des références qui lui soient spécifiques) prévus par le présent document. Des informations supplémentaires sur les systèmes de contrôle et d'accréditation pour les CSP ne délivrant pas de QC peuvent être fournies au niveau du service, le cas échéant (par exemple pour distinguer plusieurs niveaux de qualité ou de sécurité) par l'utilisation du «Scheme service definition URI» (clause 5.5.6).

▼C1

— 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 surveillance applicable aux CSP qui ne délivrent pas de QC,

— le cas échéant, des informations sur le système national d'accréditation volontaire applicable aux CSP qui ne délivrent 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 du 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. Elles DOIVENT comprendre:

— 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.

Status determination approach (clause 5.3.8)

Ce champ est OBLIGATOIRE et DOIT indiquer l'identifiant de la méthode de détermination du statut. L'URI suivant DOIT être utilisé, tel qu'il est enregistré et décrit ci-après:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate

Description: pour un État membre donné, le statut des services de la liste est déterminé par l'exploitant du système, ou pour son compte, conformément à une méthode appropriée qui permet la «surveillance» (et, le cas échéant, l'«accréditation volontaire») de prestataires de services de certification qui sont établis sur son territoire (ou, dans le cas de l'«accréditation volontaire», dans un pays tiers) et qui délivrent au public des certificats qualifiés conformément à l'article 3, paragraphe 3 [respectivement article 3, paragraphe 2, ou article 7, paragraphe 1, point a)] de la directive 1999/93/CE et, le cas échéant, qui permet le «contrôle» ou l'«accréditation volontaire» de prestataires de services de certification ne délivrant pas de certificats qualifiés conformément à un ou plusieurs «systèmes d'approbation reconnus» définis, établis et mis en œuvre au niveau national pour le contrôle de la conformité de services de CSP ne délivrant pas de QC avec les dispositions de ladite directive, éventuellement complétées par des dispositions nationales en ce qui concerne la fourniture de tels services de certification.

▼C1

Scheme type/community/rules (clause 5.3.9)

Ce champ est OBLIGATOIRE et DOIT contenir au moins les URI enregistrés suivants:

— un URI commun aux listes de confiance de tous les États membres pointant vers un texte descriptif qui DOIT s'appliquer à toutes les TL:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— qui informe de la participation du système de l'État membre (identifié par le «TSL type» (clause 5.3.3) et le «Scheme name» (clause 5.3.6) à un système de systèmes (en l'occurrence, une TSL pointant vers tous les États membres qui publient et tiennent à jour une TL ayant la forme d'une TSL),

— qui informe les utilisateurs des règles selon lesquelles les services inclus dans la liste DOIVENT être évalués et qui permettent de déterminer de quel type de TSL (voir clause 5.3.3) il s'agit,

— qui fournit aux utilisateurs une description de la manière d'utiliser et d'interpréter le contenu de l'implémentation TSL de la liste de confiance. Ces règles d'usage DOIVENT être communes aux listes de confiance de tous les États membres indifféremment du type de service listé et indifféremment du ou des systèmes de contrôle ou d'accréditation.

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 TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's TSL implementation of their 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 a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in directive 1999/93/EC [Art. 3.3, 3.2 and Art. 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.

▼C1

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 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 Art. 3.3, Art. 8.1, Art. 11 [respectively, Art. 2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 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 and the present TSL implementation 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 Art. 2.11 of the directive). 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 TSL implementation of the Trusted List

The general user guidelines for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/EC 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 ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C1

Note: If no “Sie”“Qualification” information is present or if an end-entity certificate that is claimed to be a QC is not “further identified” through a related “Sie” entry, 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. QcC, QcSSCD) 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”“Qualification” information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this “Sie”“Qualification” entry, 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 “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 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 tie”. 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 TSL implementation of the Member States’ Trusted Lists.»

▼C1

— 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/eSigDir-1999-93-EC-TrustedList/schemerules/CC

où CC = le code pays ISO 3166-1 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 dans 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 l'implémentation TSL 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 d'accréditation prévoient éventuellement un traitement distinct en ce qui concerne les CSP ne délivrant pas de QC et la manière dont le «Scheme service definition URI» (clause 5.5.6) et la «Service information extension» sont utilisés à cette fin.

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

Scheme territory (clause 5.3.10)

Dans le cadre des présentes spécifications, ce champ est OBLIGATOIRE et DOIT indiquer le pays où le système est établi (code pays ISO 3166-1 alpha-2).

TSL policy/legal notice (clause 5.3.11)

Dans le cadre des présentes spécifications, ce champ est OBLIGATOIRE et DOIT indiquer les règles du système ou fournir des informations sur son statut juridique ou sur 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 TL.

Il DOIT s'agir d'une chaîne de caractères multilingue (au format texte seul) composée de deux parties:

— une première partie obligatoire, commune aux TL de tous les États membres, avec l'anglais (EN) 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 the 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.»

▼C1

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].»

— une seconde partie facultative, spécifique à chaque TL, avec l'anglais (EN) 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).

Historical information period (clause 5.3.12)

Ce champ est OBLIGATOIRE. Il DOIT indiquer la durée (sous la forme d'un nombre entier) pendant laquelle les données historiques de la TSL sont fournies. Ce nombre entier exprime un nombre de jours, et dans le cadre des présentes spécifications, il DOIT être supérieur ou égal à 3653 (autrement dit, l'implémentation TSL des TL des États membres doit contenir des données historiques portant sur au moins dix ans). Des valeurs plus élevées doivent tenir dûment compte des prescriptions juridiques en matière de conservation des données dans l'État membre indiqué dans le «Scheme Territory» (clause 5.3.10).

Pointers to other TSLs (clause 5.3.13)

Dans le cadre des présentes spécifications, ce champ est OBLIGATOIRE. Il doit comprendre, dès lors qu'il est disponible, le pointeur vers la liste, compilée par la CE et conforme à ETSI TS 102 231, de tous les liens (pointeurs) vers toutes les implémentations TSL des listes de confiance des États membres. Les spécifications d'ETSI TS 102 231, clause 5.3.13, s'appliquent si l'utilisation, facultative, de l'identité numérique est rendue obligatoire, celle-ci représentant l'émetteur de la TSL désignée par le pointeur, formatée conformément à la clause 5.5.3.

Note: en attendant la liste, compilée par la CE et conforme à ETSI TS 102 231, des liens vers les implémentations TSL des TL des États membres, ce champ NE DOIT PAS être utilisé.

List issue date and time (clause 5.3.14)

Ce champ est OBLIGATOIRE et DOIT indiquer la date et l'heure (UTC exprimé en heure Zulu) où la TSL a été émise en utilisant la valeur de date et d'heure telle que spécifiée par ETSI TS 102 231, clause 5.1.4.

Next update (clause 5.3.15)

Ce champ est OBLIGATOIRE et DOIT indiquer la date et l'heure (UTC exprimé en heure Zulu) d'émission de la prochaine TSL, ou «null» pour indiquer une TSL fermée, en utilisant la valeur de date et d'heure telle que spécifiée par ETSI TS 102 231, clause 5.1.4.

Au cas où aucun TSP ni service couvert par le système ne changent entre-temps, la TSL DOIT être réémise lorsque sa date d'expiration est atteinte.

Dans le cadre des présentes spécifications, la différence entre la date et l'heure du «Next update» et la «List issue date and time» ne doit pas dépasser six (6) mois.

▼C1

Distribution points (clause 5.3.16)

Ce champ est OPTIONNEL. S'il est utilisé, il DOIT préciser où l'implémentation TSL en cours de la TL est publiée et où il est possible de trouver des actualisations de la TSL en cours. Si plusieurs points de distribution sont indiqués, ils DOIVENT fournir des versions identiques de la TSL en cours ou de sa version actualisée. Lorsque ce champ est utilisé, il est formaté en tant que séquence non vide de chaînes, chacune de celles-ci étant conforme à RFC 3986 ([1]).

Scheme extensions (clause 5.3.17)

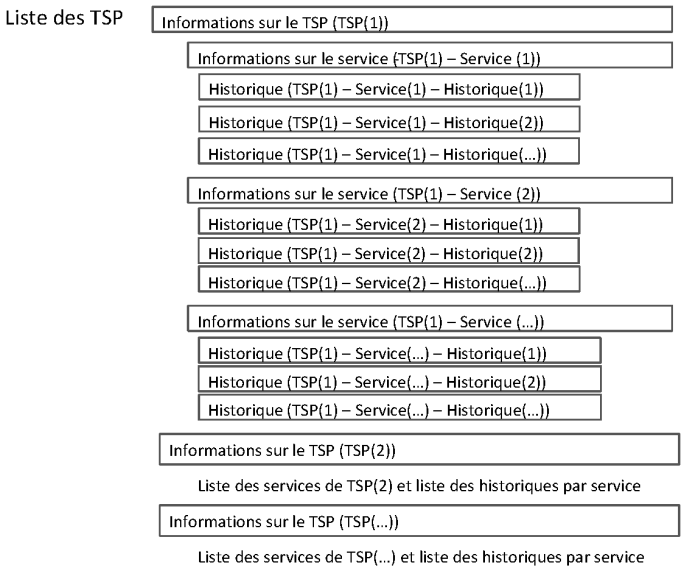
Ce champ est OPTIONNEL. Il n'est pas utilisé dans le cadre de la présente spécification.

List of Trust Service Providers

Ce champ est OPTIONNEL.

Si aucun CSP n'est ou n'a été contrôlé ou accrédité dans le cadre du système dans un État membre, ce champ DOIT être absent. Il est convenu, toutefois, que même en l'absence de CSP contrôlé ou accrédité par le système dans un État membre, celui-ci DOIT néanmoins implémenter une TSL, ce champ étant absent. L'absence de CSP dans la liste DOIT être interprétée comme signifiant qu'aucun CSP n'est contrôlé ni accrédité dans l'État membre indiqué par «Scheme Territory».

Si un ou plusieurs services de CSP sont ou ont été contrôlés ou accrédités conformément au système, le champ DOIT contenir une séquence identifiant chaque CSP fournissant un ou plusieurs de ces services contrôlés ou accrédités, avec des informations sur le statut contrôlé ou accrédité et l'historique du statut de chaque service du CSP (dans la figure ci-dessous, TSP = CSP).



([1]) IETF RFC 3986: *Uniform Resource Identifiers (URI): Generic syntax*.

▼C1

La liste des TSP est organisée comme dans la figure ci-dessus. Pour chaque TSP, la liste comporte une série de champs contenant des informations sur le TSP («TSP Information») suivie d'une liste de services. Pour chacun de ces services, la liste comporte une série de champs contenant des informations sur le service («Service information») et une série de champs contenant des informations sur l'historique du statut d'approbation du service («Service approval history»).

TSP Information

TSP(1)

TSP name (clause 5.4.1)

Ce champ est OBLIGATOIRE. Il DOIT indiquer le nom de l'entité juridique responsable des services du CSP qui sont ou ont été contrôlés ou accrédités conformément au système. Il contient une série de pointeurs multilingues, avec l'anglais (EN) en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales. Ce nom DOIT être celui employé dans les actes officiels d'enregistrement et auquel toute communication officielle doit être adressée.

TSP trade name (clause 5.4.2)

Ce champ est OPTIONNEL. S'il est présent, il DOIT indiquer un nom alternatif utilisé par le CSP pour s'identifier dans le cadre spécifique de la prestation des services qui figurent dans la présente TSL sous «TSP name» (clause 5.4.1).

Note: Lorsqu'un CSP qui est une seule entité juridique fournit des services en utilisant des appellations commerciales différentes ou dans des cadres différents, il peut y avoir autant d'entrées de CSP que de tels cadres spécifiques (par exemple une entrée pour chaque nom ou appellation commerciale). Une alternative consiste à ne lister qu'une seule fois chaque CSP (entité juridique) et à fournir des informations spécifiques sur chaque service. Il revient aux exploitants de système de chaque État membre de discuter et de convenir avec le CSP de la démarche la plus appropriée.

TSP address (clause 5.4.3)

Ce champ est OBLIGATOIRE. Il DOIT spécifier l'adresse de l'entité juridique ou de l'organisme mandaté spécifié dans le champ «TSP Name» (clause 5.4.1) pour les communications tant postales qu'électroniques. Il DOIT contenir «PostalAddress» (c'est-à-dire le nom et le numéro de la rue, la ville, [la région ou la province], [le code postal] et le code pays ISO 3166-1 alpha-2) d'une manière qui soit conforme à la clause 5.3.5.1, ainsi que «ElectronicAddress» (c'est-à-dire l'adresse électronique et/ou l'URI du site web) d'une manière qui soit conforme à la clause 5.3.5.2.

TSP information URI (clause 5.4.4)

Ce champ est OBLIGATOIRE. Il DOIT indiquer l'URI où les utilisateurs (les parties qui s'appuient sur le certificat) peuvent obtenir des informations spécifiques sur les CSP. Il DOIT contenir une séquence de pointeurs multilingues, avec l'anglais (EN) en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales. L'URI indiquée DOIT fournir un chemin vers des informations décrivant les conditions générales applicables aux services fournis par le CSP ainsi que les pratiques, les aspects juridiques, la politique en matière de service à la clientèle et les autres informations juridiques qui s'appliquent à l'ensemble des services figurant dans l'entrée du CSP dans la TSL.

Note: Lorsqu'un CSP qui est une seule entité juridique fournit des services en utilisant différentes appellations commerciales ou qu'il les fournit dans des contextes différents, et que ceux-ci sont représentés par autant d'entrées du TSP qu'il y a de contextes spécifiques, ce champ DOIT fournir des informations relatives à l'ensemble spécifique de services figurant sous une entrée TSP/TradeName particulière.

▼C1

TSP information extensions (clause 5.4.5)

Ce champ est OPTIONNEL. S'il est présent, il PEUT être utilisé par l'exploitant de système, conformément à ETSI TS 102 231 (clause 5.4.5) pour fournir des informations spécifiques devant être interprétées conformément aux règles du système spécifique.

List of Services

Ce champ est OBLIGATOIRE et DOIT contenir une séquence indiquant chacun des services reconnus du CSP et, pour chacun de ces services, son statut d'approbation et l'historique de ce statut. Au moins un service doit figurer dans le champ (même si les informations qui s'y rapportent sont exclusivement historiques).

La conservation de l'historique des services figurant dans la liste étant OBLIGATOIRE au titre des présentes spécifications, cet historique DOIT être conservé même si le statut actuel du service rend superflue, en principe, cette conservation (par exemple lorsque le service n'est plus disponible). Par conséquent, un CSP DEVRA être inclus, même lorsque son seul service figurant dans la liste a un tel statut, afin de conserver l'historique.

Service Information

TSP(1) Service(1)

Service type identifier (clause 5.5.1)

▼M1

Ce champ est OBLIGATOIRE. Il DOIT spécifier l'identification du type de service conformément au type des spécifications TSL en vigueur (c'est-à-dire «/eSigDir-1999-93-EC-TrustedList/TSLType/generic»).

▼C1

Lorsque le service listé se rapporte à la délivrance de certificats qualifiés, l'URI indiqué DOIT être http://uri.etsi.org/TrstSvc/Svctype/CA/QC (une autorité de certification délivrant des certificats qualifiés).

Lorsque le service listé se rapporte à la délivrance de jetons de service de confiance qui ne sont pas des QC et qui ne prennent pas en charge la délivrance de QC, l'URI indiqué DOIT être l'un des URI en rapport avec ce domaine définis dans ETSI 102 231 et figurant dans sa clause D.2. Cette règle DOIT être appliquée, y compris pour des jetons de service de confiance qui font l'objet d'un contrôle ou d'une accréditation en ce qui concerne le respect de certaines qualifications conformément aux dispositions de droit interne de certains États membres (comme c'est le cas pour les jetons d'horodatage qualifiés en Allemagne et en Hongrie); l'URI indiqué DOIT être l'un des URI définis dans la clause D.2 d'ETSI 102 231 en rapport avec ce domaine (par exemple TSA pour des jetons d'horodatage qualifiés définis au niveau national). Le cas échéant, cette qualification spécifique nationale des jetons de service de confiance PEUT être indiquée dans l'entrée du service, et l'extension additionalServiceInformation (clause 5.8.2) de la clause 5.5.9 («Service information extension») DOIT être utilisée à cette fin.

▼C1

Le principe général par défaut est qu'il DOIT y avoir une entrée par certificat X.509v3 (par exemple pour un service de certification de type CA/QC) sous les services de certification figurant dans la liste d'un CSP figurant dans la liste de confiance (par exemple une autorité de certification délivrant directement des QC). Dans certains cas soigneusement étudiés et dans le respect de conditions de gestion et d'approbation strictes, un organisme de contrôle ou d'accréditation d'un État membre PEUT décider d'utiliser le certificat X.509v3 d'une CA racine ou de niveau supérieur (par exemple une autorité de certification ne délivrant pas directement des QC à des entités finales mais certifiant une hiérarchie de CA jusqu'aux CA délivrant des QC à des entités finales) en tant que «Sdi» d'une entrée de la liste des services d'un CSP figurant dans la liste. Les avantages et les désavantages de l'utilisation d'un tel certificat X.509v3 d'une CA racine ou de niveau supérieur en tant que valeur «Sdi» de services TL doit faire l'objet d'une évaluation approfondie et d'une approbation des États membres [1]. En outre, lorsqu'ils ont recours à une telle exception autorisée au principe par défaut, les États membres DOIVENT fournir une documentation qui facilite l'établissement du chemin de certification et la vérification.

Note: Les TSP tels que les émetteurs OCSP et les émetteurs de CRL faisant partie de services de certification CSPQC et devant utiliser des paires de clés distinctes pour signer respectivement les réponses OCSP et les CLS PEUVENT également être listés dans le présent modèle de TSL en utilisant la combinaison d'URI suivante:

— Valeur «Service type identifier» (clause 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

combinée avec la valeur d'extension additionalServiceInformation (clause 5.8.2) de «Service information extension» (clause 5.5.9) suivante:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Description: un prestataire de service de certification exploitant un service OCSP faisant partie d'un service d'un CSP délivrant des certificats qualifiés.

— Valeur «Service type identifier» (clause 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

combinée avec la valeur d'extension additionalServiceInformation (clause 5.8.2) de «Service information extension» (clause 5.5.9) suivante:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Description: un prestataire de service de certification exploitant un CRL faisant partie d'un service d'un CSP délivrant des certificats qualifiés.

— Valeur «Service type identifier» (clause 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

[1] L'utilisation d'un certificat X.509v3 d'un CA racine en tant que valeur «Sdi» pour un service listé obligera l'exploitant du système à examiner les services de certification sous la CA racine dans leur ensemble en ce qui concerne leur «supervision/accreditation status». En conséquence, par exemple, un changement de statut d'une seule CA de la liste, dans la hiérarchie racine, impliquera ce même changement de statut pour l'ensemble de la hiérarchie.

▼C1

combinée avec la valeur d'extension additionalServiceInformation (clause 5.8.2) de «Service information extension» (clause 5.5.9) suivante:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Description: une autorité de certification racine à partir de laquelle un chemin de certification peut être établi jusqu'à une autorité de certification délivrant des certificats qualifiés.

— Valeur «Service type identifier» (clause 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/TSA

combinée avec la valeur d'extension additionalServiceInformation (clause 5.8.2) de «Service information extension» (clause 5.5.9) suivante:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Description: un service d'horodatage faisant partie d'un service d'un prestataire de services de certification délivrant des certificats qualifiés qui délivre des TST pouvant être employés dans le cadre de la procédure de vérification de la signature qualifiée afin de vérifier et d'étendre la validité de la signature lorsque le QC est révoqué ou expiré.

Service name (clause 5.5.2)

Ce champ est OBLIGATOIRE et DOIT indiquer le nom sous lequel le CSP spécifié dans «TSP name» (clause 5.4.1) fournit le service spécifié dans «Service type identifier» (clause 5.5.1). Il DOIT contenir une séquence de chaînes de caractères multilingues, avec l'anglais (EN) en tant que langue obligatoire, éventuellement complété par une ou plusieurs langues nationales.

Service digital identity (clause 5.5.3)

Ce champ est OBLIGATOIRE et DOIT spécifier au moins une représentation d'un identifiant numérique propre au service dont le type est spécifié dans «Service type identifier» (clause 5.5.1), grâce auquel le service peut être identifié sans ambiguïté.

Dans les présentes spécifications, l'identifiant numérique utilisé dans ce champ DOIT être le certificat X.509v3 pertinent, qu'il s'agisse d'une représentation de la ou des clé(s) publique(s) que le CSP utilise pour fournir le service dont le type est spécifié par le «Service type identifier» (clause 5.5.1) [c.-à-d. la clé utilisée par une CA Racine/QC, la clé utilisée pour signer les certificats ([1]), ou bien pour émettre des jetons d'horodatage, signer des CRL ou signer des réponses OCSP]. Ce certificat X.509v3 connexe DOIT être utilisé en tant qu'identifiant numérique minimal exigé [c.-à-d. la représentation de la ou des clé(s) publique(s) que le CSP utilise pour fournir le service listé]. Des identifiants supplémentaires PEUVENT être utilisés comme suit, mais ils DOIVENT tous couvrir la même identité (c.-à-d. le certificat X.509v3 connexe):

([1]) Il peut s'agir du certificat d'une CA délivrant des certificats d'entité finale (par exemple CA/PKC, CA/QC) ou du certificat d'une CA racine de confiance d'où un chemin peut être trouvé jusqu'aux certificats qualifiés d'entité finale. En fonction du fait que ces informations et celles qui figurent dans chaque certificat d'entité finale délivré sous cette racine de confiance peuvent ou non être utilisées pour déterminer sans ambiguïté les caractéristiques appropriées de n'importe quel certificat qualifié, il se peut que ces informations («Service digital identity») doivent être complétées par des données «Service information extensions» (voir clause 5.5.9).

▼C1

a) le nom distingué (DN) du certificat qui peut être utilisé pour vérifier les signatures électroniques du service CSP spécifié dans «Service type identifier» (clause 5.5.1);

b) l'identifiant de clé publique connexe (c.-à-d. SubjectKeyIdentifier X.509v3 ou valeur SKI);

c) la clé publique connexe.

Le principe général par défaut est que l'identifiant numérique (c.-à-d. le certificat X.509v3 connexe) NE DOIT PAS figurer plus d'une fois dans la liste de confiance; autrement dit, il DOIT y avoir une seule entrée par certificat X.509v3 pour un service de certification sous les services de certification figurant dans la liste d'un CSP figurant dans la liste de confiance. Inversement, un certificat X.509v3 unique DOIT être utilisé dans une entrée de service unique en tant que valeur «Sdi».

Note(1): Le seul cas où le principe général par défaut ci-dessous ne peut s'appliquer est celui où un certificat X.509v3 unique est utilisé lors de la délivrance de différents types de jetons de service de confiance pour lesquels s'appliquent différents systèmes de contrôle ou d'accréditation; par exemple, un certificat X.509v3 unique est utilisé par un CSP d'une part pour délivrer des QC sous un système de contrôle approprié et, d'autre part, pour délivrer des certificats non qualifiés sous un statut de contrôle ou d'accréditation différent. Dans ce cas et cet exemple, on utiliserait deux entrées comportant des valeurs «Sti» différentes (respectivement CA/QC et CA/PKC dans l'exemple donné) et la même valeur «Sdi» (le certificat X.509v3 connexe).

Les implémentations sont tributaires du ASN.1 ou du XML et DOIVENT se conformer aux spécifications ETSI TS 102 231 (pour l'ASN.1, voir l'annexe A d'ETSI TS 102 231 et pour le XML, voir l'annexe B d'ETSI TS 102 231).

Note(2): Lorsqu'il est nécessaire de fournir des informations de «qualification» supplémentaires par rapport à l'entrée du service spécifié, alors l'exploitant du système DOIT, le cas échéant, envisager l'utilisation de l'extension «additionalServiceInformation» (clause 5.8.2) du champ «Service information extension» (clause 5.5.9), en fonction du but poursuivi par la fourniture de ces informations de «qualification» supplémentaires. De plus, l'exploitant du système peut, de manière facultative, utiliser la clause 5.5.6 («Scheme service definition URI»).

Service current status (clause 5.5.4)

Ce champ est OBLIGATOIRE et DOIT spécifier l'identifiant du statut du service via l'un des URI suivants:

▼C2

— **Under Supervision** (**Contrôlé**) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— **Supervision of Service in Cessation** (**Contrôle du service en voie d'interruption**) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

— **Supervision Ceased** (**Contrôle interrompu**) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **Supervision Revoked** (**Contrôle révoqué**) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **Accredited (Accrédité)** (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);

— **Accreditation Ceased** (**Accréditation interrompue**) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— **Accreditation Revoked** (**Accréditation révoquée**) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Les statuts précités DOIVENT être interprétés comme suit dans le contexte des présentes spécifications de la liste de confiance:

— ***Contrôlé:*** Le service spécifié dans «Service digital identity» (clause 5.5.3) fourni par le prestataire de service de certification (CSP) identifié dans «TSP name» (clause 5.4.1) est actuellement contrôlé par l'État membre spécifié dans «Scheme territory» (clause 5.3.10) où le CSP est établi, en ce qui concerne le respect des dispositions de la directive 1999/93/CE.

▼M1

— ***Contrôle du service en cours de suspension:*** Le service spécifié dans «Service digital identity» (clause 5.5.3) fourni par le CSP identifié dans «TSP name» (clause 5.4.1) est actuellement en cours de suspension, mais est toujours contrôlé, jusqu'à la suspension ou la révocation du contrôle. Au cas où une personne morale différente de celle spécifiée dans «TSP name» a endossé la responsabilité de mener à bien cette phase de suspension, l'identification de cette personne morale nouvelle ou de réserve (CSP de réserve) DOIT être fournie dans «Scheme service definition URI» (clause 5.5.6) et dans l'extension «TakenOverBy» (clause L.3.2) de l'entrée du service.

▼C1

— ***Contrôle suspendu:*** La validité de l'évaluation de contrôle a expiré sans que le service spécifié dans «Service digital identity» (clause 5.5.3) ait été réévalué. Le service n'est actuellement plus contrôlé depuis la date du statut en cours, le service devant être considéré comme ayant cessé toute activité.

— ***Contrôle révoqué:*** Après avoir été antérieurement contrôlé, le service du CSP et, potentiellement, le CSP lui-même a cessé de respecter les dispositions prévues par la directive 1999/93/CE, déterminées par l'État membre spécifié dans le «Scheme territory» (clause 5.3.10) où le CSP est établi. Le service a par conséquent été invité à cesser ses activités et doit être considéré comme étant suspendu pour la raison précitée.

Note(1): La valeur de statut «Contrôle révoqué» peut être un statut définitif même si le CSP a complètement cessé son activité; il n'est pas nécessaire, dans ce cas, de passer au statut «Contrôle du service en cours de suspension» ou au statut «Contrôle suspendu». En fait, la seule manière de changer le statut «Contrôle révoqué» est de revenir à la conformité aux dispositions prévues par la directive 1999/93/CE conformément au système de contrôle approprié en vigueur dans l'État membre qui possède la TL, et de regagner le statut «Contrôlé». Les statuts «Contrôle du service en cours de suspension» ou «Contrôle suspendu» ne sont attribués que lorsqu'un CSP cesse de lui-même de fournir les services soumis au contrôle, et non lorsque le contrôle a été révoqué.

— ***Accrédité:*** Une évaluation d'accréditation a été effectuée par l'organisme d'accréditation au nom de l'État membre spécifié dans le «Scheme territory» (clause 5.3.10) et le service spécifié dans la «Service digital identity» (clause 5.5.3) fourni par le CSP [1] identifié dans «TSP name» (clause 5.4.1) est reconnu conforme aux dispositions de la directive 1999/93/CE.

[1] Il faut remarquer que ce CSP accrédité peut être établi dans un État membre autre que celui indiqué dans le «Scheme territory» de l'implémentation TSL de la TL ou dans un pays tiers [voir article 7, paragraphe 1, point a), de la directive 1999/93/CE].

▼C1

Note(2): Lorsqu'ils sont utilisés dans la situation d'un CSP délivrant des QC qui est établi sur le «Scheme territory» (clause 5.3.10), les deux statuts «Accréditation révoquée» et «Accréditation suspendue» DOIVENT être considérés comme des «statuts transitoires» et NE DOIVENT PAS être utilisés comme valeur de «Service current status» étant donné que, s'ils sont utilisés, ils DOIVENT être suivis immédiatement, dans les informations «Service Approval History» ou dans le «Service current status», par un statut «Contrôlé», potentiellement suivi d'un quelconque autre statut de contrôle défini ci-dessus, comme l'illustre la figure 1. En cas d'utilisation dans la situation d'un CSP qui ne délivre pas de QC, lorsqu'il existe un seul système d'«accréditation volontaire» associé, sans système de contrôle associé, ou dans la situation d'un CSP qui délivre des QC mais n'est pas établi sur le «Scheme territory» (clause 5.3.10) (par exemple, dans un pays tiers), les statuts «Accréditation révoquée» et «Accréditation suspendue» PEUVENT être utilisés en tant que valeur pour «Service current status»:

— ***Accréditation suspendue:*** La validité de l'évaluation d'accréditation a expiré sans que le service spécifié dans «Service digital identity» (clause 5.5.3) ait été réévalué.

— ***Accréditation révoquée:*** Après avoir été reconnu conforme aux critères du système, le service spécifié dans «Service digital identity» (clause 5.5.3) fourni par le prestataire de service de certification (CSP) spécifié dans «TSP name» (clause 5.4.1) et potentiellement le CSP lui-même, ont cessé de respecter les dispositions prévues par la directive 1999/93/CE.

Note(3): Il faut utiliser exactement les mêmes valeurs de statut pour les CSP qui délivrent des QC et pour les CSP qui ne délivrent pas de QC (par ex. prestataires de service d'horodatage délivrant des TST, CSP délivrant des certificats non qualifiés, etc.). Le «Service Type identifier» (clause 5.5.1) doit être utilisé pour établir la distinction entre systèmes de contrôle et d'accréditation applicables.

Note(4): Des informations de «qualification» liées au statut supplémentaires, définies au niveau des systèmes nationaux de contrôle ou d'accréditation pour les CSP ne délivrant pas de QC PEUVENT être fournies au niveau du service, le cas échéant (par exemple pour distinguer plusieurs niveaux de qualité ou de sécurité). Les exploitants de système DOIVENT utiliser l'extension «additionalServiceInformation» (clause 5.8.2) du champ «Service information extension» (clause 5.5.9) en fonction du but poursuivi par la fourniture de ces informations de «qualification» supplémentaires. De plus, l'exploitant du système peut, de manière facultative, utiliser la clause 5.5.6 («Scheme service definition URI»).

Current status starting date and time (clause 5.5.5)

Ce champ est OBLIGATOIRE et DOIT spécifier la date et l'heure où le statut d'approbation en cours est devenu effectif (valeurs de date et heure définies dans ETSI TS 102 231 clause 5.1.4).

Scheme service definition URI (clause 5.5.6)

Ce champ est OPTIONNEL et, s'il est présent, DOIT spécifier le ou les URI où les parties qui s'appuient sur le certificat peuvent obtenir des informations spécifiques au service fournies par l'exploitant du système sous la forme d'une séquence de pointeurs multilingues (avec l'anglais EN en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales).

Lorsqu'ils sont utilisés, le ou les URI référencés DOIVENT fournir un chemin vers des informations décrivant le service selon les spécifications du système. Il PEUT notamment s'agir des éléments suivants, le cas échéant:

a) un URI indiquant l'identité du CSP de réserve, dans la situation du contrôle d'un service en voie d'interruption où un CSP de réserve est impliqué (voir «Service current status» — clause 5.5.4);

▼C1

b) un URI conduisant à des documents contenant des informations supplémentaires liées à l'utilisation d'une qualification spécifique définie à l'échelon national pour un service contrôlé ou accrédité fournissant des jetons de service de confiance dans le cadre de l'utilisation du champ «Service information extension» (clause 5.5.9) avec une extension «additionalServiceInformation» telle que définie à la clause 5.8.2.

Service supply points (clause 5.5.7)

Ce champ est OPTIONNEL et, s'il est présent, DOIT spécifier le ou les URI où les parties qui s'appuient sur le certificat peuvent accéder au service au moyen d'une séquence de chaînes de caractères dont la syntaxe DOIT être conforme à RFC 3986.

TSP service definition URI (clause 5.5.8)

Ce champ est OPTIONNEL et, s'il est présent, DOIT spécifier le ou les URI où les parties qui s'appuient sur le certificat peuvent obtenir des informations spécifiques au service fournies par le TSP sous la forme d'une séquence de pointeurs multilingues (avec l'anglais EN en tant que langue obligatoire, éventuellement complétée par une ou plusieurs langues nationales). Le ou les URI référencés DOIVENT fournir un chemin vers des informations décrivant le service tel que spécifié par le TSP.

Service information extensions (clause 5.5.9)

Dans le contexte des présentes spécifications, ce champ est OPTIONNEL mais DOIT être présent lorsque les informations fournies dans la «Service digital identity» (clause 5.5.3) ne suffisent pas pour identifier sans ambiguïté les certificats qualifiés délivrés par ce service ou lorsque les informations présentes dans les certificats qualifiés correspondants ne permettent pas de déterminer par machine si ces QC reposent ou non sur un SSCD ([1]).

Dans le contexte des présentes spécifications, lorsque son usage est OBLIGATOIRE, par exemple pour les services CA/QC, un champ d'information optionnel «Service information extensions» («Sie») DOIT être utilisé et structuré, conformément à l'extension «Qualifications» définie dans ETSI TS 102 231 Annexe L.3.1, sous la forme d'une séquence d'un ou plusieurs n-uplets, chaque n-uplet fournissant:

— les informations à utiliser pour identifier plus précisément (filtrer), sous le service de certification identifié «Sdi», le service spécifique (c.-à-d. l'ensemble de certificats qualifiés) pour lequel des informations supplémentaires sont requises/fournies en ce qui concerne la prise en charge ou non par un SSCD (et/ou la délivrance à une personne morale), et

— les informations associées («qualifiers») indiquant si cet ensemble de certificats qualifiés identifié plus précisément repose ou non sur un SSCD [lorsque cette information est «QCSSCDStatusAsInCert», cela signifie que ces informations associées font partie du QC sous une forme normalisée ETSI, lisible en machine ([2])], 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).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD) signifie que le CSP garantit et que l'État membre contrôle (dans le cas d'un modèle de contrôle) ou vérifie par des audits (dans le cas d'un modèle d'accréditation), respectivement via son organisme de contrôle ou son organisme d'accréditation, que tout QC délivré au titre du service (QCA) indiqué dans «Service digital identity» (clause 5.5.3) et identifié plus précisément par les informations (filtres) ci-dessus utilisées pour préciser, sous le service de certification identifié «Sdi», l'ensemble précis de certificats qualifiés pour lequel ces informations supplémentaires sont requises en ce qui concerne la prise en charge ou non par un SSCD, EST pris en charge par un SSCD (c.-à-d. que la clé privée associée à la clé publique dans le certificat est stockée dans un dispositif sécurisé de création de signature conforme à l'annexe III de la directive 1999/93/CE).

([1]) Voir le point 2.2 du présent document.

([2]) Cela renvoie à une combinaison appropriée de déclaration de conformité Qc définie par l'ETSI, de déclarations QcSSCD [ETSI TS 101 862] ou d'un QCP/QCP+ OID défini par l'ETSI [ETSI TS 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD) signifie que le CSP garantit et que l'État membre contrôle (dans le cas d'un modèle de contrôle) ou vérifie par des audits (dans le cas d'un modèle d'accréditation), respectivement via son organisme de contrôle ou son organisme d'accréditation, que tout QC délivré au titre du service (CA Racine/QC ou CA/QC) indiqué dans «Service digital identity» (clause 5.5.3) et identifié plus précisément par les informations (filtres) ci-dessus utilisées pour préciser, sous le service de certification identifié «Sdi», l'ensemble précis de certificats qualifiés pour lequel ces informations supplémentaires sont requises en ce qui concerne la prise en charge ou non par un SSCD, N'EST PAS pris en charge par un SSCD (c.-à-d. que la clé privée associée à la clé publique dans le certificat n'est pas stockée dans un dispositif sécurisé de création de signature conforme à l'annexe III de la directive 1999/93/CE).

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert) signifie que le CSP garantit et que l'État membre contrôle (dans le cas d'un modèle de contrôle) ou vérifie par des audits (dans le cas d'un modèle d'accréditation), respectivement via son organisme de contrôle ou son organisme d'accréditation, que tout QC délivré au titre du service (CA/QC) indiqué dans «Service digital identity» (clause 5.5.3) et identifié plus précisément par les informations (filtres) ci-dessus utilisées pour préciser, sous le service de certification identifié «Sdi», l'ensemble précis de certificats qualifiés pour lequel ces informations supplémentaires sont requises en ce qui concerne la prise en charge ou non par un SSCD, DOIT contenir l'information lisible en machine précisant si oui ou non le QC est pris en charge par un SSCD.

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): signifie que le CSP garantit et que l'État membre contrôle (dans le cas d'un modèle de contrôle) ou vérifie par des audits (dans le cas d'un modèle d'accréditation), respectivement via son organisme de contrôle ou son organisme d'accréditation, que tout QC délivré au titre du service (QCA) indiqué dans «Service digital identity» (clause 5.5.3) et identifié plus précisément par les informations (filtres) ci-dessus utilisées pour préciser, sous le service de certification identifié «Sdi», l'ensemble précis de certificats qualifiés pour lequel ces informations supplémentaires sont requises en ce qui concerne la délivrance à des personnes morales EST délivré à des personnes morales.

Ces «qualifiers» ne sont à utiliser que comme extension, si le type du service est http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Ce champ est spécifique à l'implémentation (ASN.1 ou XML) et DOIT respecter les spécifications d'ETSI TS 102 231, Annexe L.3.1.

▼M1

Dans le contexte d'une implémentation XML, le contenu spécifique de ces informations supplémentaires doit être codé à l'aide des fichiers xsd figurant à l'annexe C d'ETSI TS 102 231.

▼C1

Service Approval History

Ce champ est OPTIONNEL mais DOIT être présent si «Historical information period» (clause 5.3.12) est différent de zéro. Donc, dans le cadre des présentes spécifications, le système DOIT conserver des données historiques. Dans le cas où il est prévu de conserver les données historiques, mais où le service n'a pas d'historique antérieur à son statut en cours (autrement dit, il s'agit du premier statut enregistré, ou bien l'exploitant du système n'a pas conservé de données historiques), ce champ DOIT être vide. Autrement, pour tout changement du statut du service de TSP survenu au cours de la période de fourniture des données historiques telle que spécifiée dans la clause 5.3.12 d'ETSI TS 102 231, les informations relatives au statut d'approbation antérieur DOIVENT être fournies par ordre chronologique décroissant de date et heure de changement de statut (c.-à-d. la date et l'heure auxquelles le statut d'approbation suivant est entré en vigueur).

▼C1

Le contenu du champ DOIT être une séquence de données historiques telle que définie ci-après:

TSP(1) Service(1) History(1)

Service type identifier (clause 5.6.1)

Ce champ est OBLIGATOIRE et DOIT spécifier l'identifiant du type de service, avec le format et la signification utilisés dans «TSP Service Information — Service type identifier» (clause 5.5.1).

Service name (clause 5.6.2)

Ce champ est OBLIGATOIRE et DOIT spécifier le nom sous lequel le CSP a fourni le service indiqué dans «TSP Service Information — Service type identifier» (clause 5.5.1), avec le format et la signification utilisés dans «TSP Service Information — Service name» (clause 5.5.2). Cette clause n'impose pas que le nom soit le même que celui spécifié dans la clause 5.5.2. Un changement de nom PEUT être l'une des circonstances imposant un nouveau statut.

▼M1

Service digital identity (clause 5.6.3)

Ce champ est OBLIGATOIRE et DOIT spécifier au moins une représentation de l'identifiant numérique (en l'occurrence, le certificat X.509v3) utilisé dans «TSP Service information – Service digital identity» (clause 5.5.3) avec le format et la signification définis dans ETSI TS 102 231, clause 5.5.3.

Note: pour chaque valeur du certificat X.509v3 utilisée dans la clause 5.5.3 «Sdi» d'un service, il ne doit y avoir qu'une seule entrée de service dans une liste de confiance par valeur «Sti:Sie/additionalServiceInformation». Les informations «Sdi» (clause 5.6.3) utilisées dans les informations de l'historique du statut du service associées à une entrée de service et les informations «Sdi» (clause 5.5.3) utilisées dans cette entrée du service DOIVENT se rapporter à la même valeur du certificat X.509v3. Lorsqu'un service listé modifie sa «Sdi» (renouvellement du certificat X.509v3 ou des clés du certificat d'une CA/PKC ou d'une CA/QC, par exemple) ou crée une nouvelle «Sdi» pour ce service, même avec des valeurs identiques pour les «Sti», «Sn» et [«Sie»] associés, l'exploitant du système DOIT créer une entrée relative au service différente des précédentes.

▼C1

Service previous status (clause 5.6.4)

Ce champ est OBLIGATOIRE et DOIT spécifier l'identifiant du statut antérieur du service, avec le format et la signification utilisés dans «TSP Service Information — Service current status» (clause 5.5.4).

Previous status starting date and time (clause 5.6.5)

Ce champ est OBLIGATOIRE et DOIT spécifier la date et l'heure auxquelles le statut antérieur en question est entré en vigueur, avec le format et la signification utilisés dans «TSP Service Information — Service current status starting date and time» (clause 5.5.5).

Service information extensions (clause 5.6.6)

Ce champ est OPTIONNEL et PEUT être utilisé par les exploitants de système pour fournir des informations spécifiques sur le service, avec le format et la signification utilisés dans «TSP Service Information — Service information extensions» (clause 5.5.9).

▼C1

TSP(1) Service(1) History(2)

Idem pour TSP(1) Service(1) Historique(2) (avant Historique 1)

…

TSP(1) Service(2)

Idem pour TSP(1) Service 2 (le cas échéant)

TSP(1)Service(2)Historique(1)

…

TSP(2) Information

Idem pour TSP 2 (le cas échéant)

Idem pour TSP 2 Service 1

Idem pour TSP 2 Service 1 Historique 1

…

▼M1

Signed TSL

L'implémentation TSL directement lisible de la liste de confiance, établie en vertu des présentes spécifications et en particulier du chapitre IV, DEVRAIT être signée par le «Scheme operator name» (clause 5.3.4) pour que l'authenticité et l'intégrité en soient garanties ([1]). Le format de la signature DEVRAIT être PAdES part 3 (ETSI TS 102 778-3 ([2])) mais PEUT être PAdES part 2 (ETSI TS 102 778-2 ([3])) dans le contexte du modèle de confiance spécifique établie au moyen de la publication des certificats utilisés pour signer les listes de confiance.

L'implémentation TSL destinée à un traitement électronique de la liste de confiance, établie en vertu des présentes spécifications, DOIT être signée par le «Scheme operator name» (clause 5.3.4) pour que l'authenticité et l'intégrité en soient garanties. Le format de l'implémentation TSL destinée à un traitement électronique de la liste de confiance, établie en vertu des présentes spécifications, DOIT être le XML et DOIT être conforme aux spécifications définies aux annexes B et C d'ETSI TS 102 231.

Le format de la signature DOIT être XAdES BES ou EPES, tel que défini dans les spécifications ETSI TS 101 903 pour les implémentations XML. Cette implémentation de signature électronique DOIT satisfaire aux exigences prévues à l'annexe B de ETSI TS 102 231 ([4]). Des exigences générales supplémentaires concernant cette signature figurent dans les sections suivantes.

▼C1

Scheme identification (clause 5.7.2)

Ce champ est OBLIGATOIRE et DOIT spécifier une référence assignée par l'exploitant du système qui identifie de manière unique le système décrit dans les présentes spécifications et la TSL établie, et DOIT être inclus dans le calcul de la signature. Il devrait s'agir d'une chaîne de caractères ou d'une chaîne de bits.

([1]) Dans le cas où l'implémentation TSL directement lisible de la liste de confiance n'est pas signée, son authenticité et son intégrité DOIVENT être garanties par un canal de communication approprié offrant un niveau de sécurité équivalent. Utilisation de TLS (IETF RFC 5246: «The Transport Layer Security (TLS) Protocol Version 1.2») est recommandée à cette fin et les États membres DOIVENT donner aux utilisateurs de la TSL un accès hors bande à l'empreinte du certificat du canal TLS.

([2]) ETSI TS 102 778-3 – Infrastructures et signatures électroniques: profils de signature électronique avancée dans un document PDF; partie 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 – Infrastructures et signatures électroniques: profils de signature électronique avancée dans un document PDF; partie 2: PAdES Basic – Profile based on ISO 32000-1.

([4]) Il est obligatoire de protéger l'exploitant de système qui signe le certificat avec la signature en utilisant l'un des moyens spécifiés par ETSI TS 101 903 et le ds:keyInfo devrait contenir la chaîne de certificat pertinente, le cas échéant.

▼M1

Dans le contexte des présentes spécifications, la référence assignée DOIT inclure «TSL type» (clause 5.3.3), «Scheme name» (clause 5.3.6) et la valeur de l'extension SubjectKeyIdentifier du certificat utilisée par l'exploitant du système pour signer électroniquement la TSL.

▼C1

Signature algorithm identifier (clause 5.7.3)

Ce champ est OBLIGATOIRE et DOIT spécifier l'algorithme de chiffrement qui a été utilisé pour créer la signature. En fonction de l'algorithme utilisé, ce champ PEUT nécessiter des paramètres supplémentaires. Ce champ DOIT être inclus dans le calcul de la signature.

Signature value (clause 5.7.4)

Ce champ est OBLIGATOIRE et DOIT contenir la valeur réelle de la signature numérique. Tous les champs de la TSL (excepté la valeur de la signature elle-même) DOIVENT être inclus dans le calcul de la signature.

TSL extensions (clause 5.8)

expiredCertsRevocationInfo Extension (clause 5.8.1)

Cette extension est OPTIONNELLE. Lorsqu'elle est utilisée, elle DOIT respecter les spécifications d'ETSI TS 102 231, clause 5.8.1.

additionalServiceInformation Extension (clause 5.8.2)

Lorsqu'elle est utilisée, cette extension OPTIONNELLE DOIT être utilisée uniquement au niveau du service et seulement dans le champ défini à la clause 5.5.9 («Service information extension»). Elle sert à fournir des informations supplémentaires sur un service. Il DOIT s'agir d'une séquence d'un ou plusieurs n-uplets, chaque n-uplet contenant:

a) un URI identifiant les informations supplémentaires, par exemple:

   — un URI indiquant une qualification définie à l'échelon national pour un service contrôlé ou accrédité fournissant des jetons de service de confiance, par exemple,

      — un niveau de granularité de sécurité/qualité spécifique en ce qui concerne le système de contrôle ou d'accréditation national pour les CSP qui ne délivrent pas de QC (p. ex. RGS */**/*** en France, un statut de «contrôle» spécifique défini par la législation nationale pour des CSP spécifiques délivrant des QC en Allemagne), voir la Note (4) de «Service current status» — clause 5.5.4,

      — ou un statut juridique spécifique pour un service contrôlé ou accrédité fournissant des jetons de service de confiance (par exemple un «TST qualifié» défini à l'échelon national comme en Allemagne ou en Hongrie),

      — ou la signification d'un identifiant de stratégie spécifique présent dans un certificat X.509v3 fourni dans le champ «Sdi»,

   — ou un URI enregistré tel que spécifié dans «Service type identifier», clause 5.5.1, afin de préciser la participation du service identifié «Sti» en tant que service composant d'un prestataire de service de certification délivrant des QC (p. ex. OCSP-QC, CRL-QC, et RootCA-QC);

b) une chaîne optionnelle contenant la valeur serviceInformation, dont la signification est spécifiée dans le système (p. ex. *, ** ou ***);

c) toute information optionnelle supplémentaire fournie dans un format propre au système.

▼**M1**

Le déréférencement de l'URI DEVRAIT aboutir à des informations directement lisibles (au moins en EN et potentiellement dans une ou plusieurs langues nationales), considérées comme appropriées et suffisantes pour permettre à une partie utilisatrice de comprendre l'extension et expliquant notamment la signification des URI, en spécifiant les valeurs possibles pour serviceInformation et la signification pour chaque valeur.

Qualifications Extension (clause L.3.1)

Description: ce champ est OPTIONNEL mais DOIT être présent lorsque son usage est OBLIGATOIRE, par exemple pour les services RootCA/QC ou CA/QC, et lorsque:

— les informations fournies dans «Service digital identity» sont insuffisantes pour identifier sans ambiguïté les certificats qualifiés délivrés par ce service,

— les informations présentes dans les certificats qualifiés correspondants ne permettent pas l'identification lisible en machine du fait que le QC est oui ou non pris en charge par un SSCD.

Lorsqu'elle est utilisée, cette extension au niveau du service DOIT être utilisée uniquement dans le champ défini dans «Service information extension» (clause 5.5.9) et elle DOIT être conforme aux spécifications de l'annexe L.3.1 de ETSI TS 102 231.

TakenOverBy Extension (clause L.3.2)

Description: cette extension est OPTIONNELLE mais DOIT être présente lorsqu'un service précédemment placé sous la responsabilité légale d'un CSP est repris par un autre TSP et vise à indiquer officiellement la responsabilité légale d'un service et à permettre au logiciel de vérification de communiquer à l'utilisateur des informations juridiques. Les informations fournies dans cette extension DOIVENT être compatibles avec l'utilisation de la clause 5.5.6 et conformes aux spécifications de l'annexe L.3.2 d'ETSI TS 102 231.

▼M1

CHAPITRE II

Au moment d'établir leur liste de confiance, les États membres utilisent:

les codes langue en minuscules et les codes pays en majuscules;

les codes langue et pays conformément au tableau ci-dessous.

Lorsqu'un alphabet latin est utilisé (avec le code langue correspondant), une transcription en alphabet latin, accompagnée des codes langue correspondants indiqués dans le tableau ci-dessous, est ajoutée.

Nom court (langue source)	Nom court (anglais)	Code pays	Code langue	Notes	Transcription en alphabet latin
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Code pays recommandé par l'Union	el-Latn
España	Spain	ES	es	européenne aussi catalan (ca), basque (eu), galicien (gl)	
France	France	FR	fr		
▼M2 Hrvatska	Croatie	HR	hr		
▼M1 Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼M1

Nom court (langue source)	Nom court (anglais)	Code pays	Code langue	Notes	Transcription en alphabet latin
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Code pays recommandé par l'Union	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Transcription en alphabet latin: България – Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

CHAPITRE IV

SPÉCIFICATIONS POUR LA FORME DIRECTEMENT LISIBLE DE L'IMPLÉMENTATION TSL DE LA LISTE DE CONFIANCE

Une forme directement lisible (HR, human readable) de l'implémentation TSL de la liste de confiance DOIT être mise à la disposition du public et accessible par voie électronique. Elle DEVRAIT être fournie sous la forme d'un document PDF (Portable Document Format) conforme à ISO 32000 qui DOIT être formaté conformément au profil PDF/A (ISO 19005).

Le contenu de la forme HR fondée sur PDF/A de l'implémentation TSL de la liste de confiance DEVRAIT respecter les exigences suivantes:

▼M1

— le titre de la version directement lisible des listes de confiance doit être la concaténation des éléments suivants:

  — image optionnelle du drapeau national de l'État membre concerné,

  — espace vide,

  — nom court du pays dans la (les) langue(s) source (conformément à la première colonne du tableau du chapitre II),

  — espace vide,

  — «(»,

  — nom court du pays en anglais (conformément à la deuxième colonne du tableau du chapitre II),

  — «): » utilisé comme parenthèse fermante et séparateur,

  — espace vide,

  — «liste de confiance»,

  — logo optionnel de l'exploitant du système de l'État membre concerné,

▼C1

— la structure de la forme HR DEVRAIT refléter le modèle logique décrit à la section 5.1.2 d'ETSI TS 102 231,

— 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, notamment comme prévu à l'annexe D d'ETSI TS 102 231 ou dans les présentes spécifications pour les URI enregistrés (p. ex. «Une autorité de certification délivrant des certificats à clé publique»),

  — le cas échéant, plusieurs versions en langage naturel telles que prévues dans l'implémentation TSL de la liste de confiance,

— 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

▼C1

— Clé publique

— Règles de certificat

— Identifiant de la clé du sujet

— 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 PEUT être signée électroniquement. Si elle est signée, elle DOIT l'être par l'exploitant du système selon les mêmes spécifications applicables aux signatures que pour l'implémentation TSL de la liste de confiance.