Este documento constitui um instrumento de documentação e não vincula as instituições

►B ►C1 **DECISÃO DA COMISSÃO**

de 16 de Outubro de 2009

que determina medidas destinadas a facilitar a utilização de procedimentos informatizados através de «balcões únicos», nos termos da Directiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno

[notificada com o número C(2009) 7806]

(Texto relevante para efeitos do EEE)

(2009/767/CE) ◄

(JO L 274 de 20.10.2009, p. 36)

Alterado por:

		Jornal Oficial		
		n.°	página	data
►M1	Decisão 2010/425/UE da Comissão de 28 de Julho de 2010	L 199	30	31.7.2010
►M2	Regulamento (UE) n.º 519/2013 da Comissão de 21 de fevereiro de 2013	L 158	74	10.6.2013

Retificada por:

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

▼B
▼C1

DECISÃO DA COMISSÃO

de 16 de Outubro de 2009

que determina medidas destinadas a facilitar a utilização de procedimentos informatizados através de «balcões únicos», nos termos da Directiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno

[notificada com o número C(2009) 7806]

(Texto relevante para efeitos do EEE)

(2009/767/CE)

A COMISSÃO DAS COMUNIDADES EUROPEIAS,

Tendo em conta o Tratado que institui a Comunidade Europeia,

Tendo em conta a Directiva 2006/123/CE do Parlamento Europeu e do Conselho, de 12 de Dezembro de 2006, relativa aos serviços no mercado interno ([1]), e, nomeadamente, o seu artigo 8.º, n.º 3,

Considerando o seguinte:

(1) As obrigações de simplificação administrativa impostas aos Estados-Membros, nos termos do capítulo II da Directiva 2006/123/CE, em especial os seus artigos 5.º e 8.º, incluem a obrigação de simplificar os procedimentos e as formalidades aplicáveis ao acesso a uma actividade de serviços e ao seu exercício e a obrigação de assegurar que esses procedimentos e formalidades possam ser facilmente cumpridos pelos prestadores de serviços, à distância e por via electrónica, através de «balcões únicos».

(2) O cumprimento de procedimentos e formalidades através de «balcões únicos» deverá poder ser realizado a nível transfronteiras entre Estados-Membros, conforme estabelecido no artigo 8.º da Directiva 2006/123/CE.

(3) Para dar cumprimento à obrigação de simplificar os procedimentos e as formalidades e de facilitar a utilização transfronteiras dos «balcões únicos», os procedimentos por via electrónica devem assentar em soluções simples, incluindo no que se refere à utilização de assinaturas electrónicas. Nos casos em que, após uma adequada avaliação dos riscos de procedimentos e formalidades concretos, se considere necessário um alto grau de segurança ou equivalência a uma assinatura manuscrita, poderão ser exigidos aos prestadores de serviços, em relação a determinados procedimentos e formalidades, assinaturas electrónicas avançadas baseadas num certificado qualificado, com ou sem um dispositivo seguro de criação de assinaturas.

([1]) JO L 376 de 27.12.2006, p. 36.

▼C1

(4) O quadro comunitário para as assinaturas electrónicas foi definido pela Directiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999 relativa a um quadro legal comunitário para as assinaturas electrónicas ([1]). A fim de facilitar a utilização transfronteiras eficaz de assinaturas electrónicas avançadas baseadas num certificado qualificado, a confiança nestas assinaturas deverá ser reforçada, independentemente do Estado-Membro onde estiver estabelecido o signatário ou o prestador de serviços de certificação que emite o certificado qualificado. Para tal, deve facilitar-se o acesso à informação necessária para a validação das assinaturas electrónicas, de uma forma fiável, em especial a informação relativa aos prestadores de serviços de certificação que são controlados/acreditados em cada Estado-Membro e aos serviços que estes fornecem.

(5) É necessário garantir que os Estados-Membros divulguem publicamente este tipo de informação através de um padrão de referência harmonizado, a fim de facilitar a sua utilização e de assegurar um nível de pormenor adequado que permita ao destinatário validar a assinatura electrónica,

ADOPTOU A PRESENTE DECISÃO:

Artigo 1.º

Utilização e aceitação de assinaturas electrónicas

1. Quando se justifique, com base numa adequada avaliação dos riscos envolvidos e em conformidade com o artigo 5.º, n.os 1 e 3, da Directiva 2006/123/CE, os Estados-Membros podem exigir que, para o cumprimento de determinados procedimentos e formalidades através de balcões únicos nos termos do artigo 8.º da Directiva 2006/123/CE, o prestador de serviços utilize assinaturas electrónicas avançadas baseadas num certificado qualificado, com ou sem um dispositivo seguro de criação de assinaturas, conforme estabelecido pela Directiva 1999/93/CE e por esta regido.

2. Os Estados-Membros deverão aceitar todas as assinaturas electrónicas avançadas baseadas num certificado qualificado, com ou sem um dispositivo seguro de criação de assinaturas, para o cumprimento dos procedimentos e formalidades referidos no n.º 1, sem prejuízo da possibilidade de os Estados-Membros limitarem essa aceitação às assinaturas electrónicas avançadas baseadas num certificado qualificado e criadas por um dispositivo seguro de criação de assinaturas, se tal for conforme com a avaliação de riscos referida no n.º 1.

3. Os Estados-Membros não devem fazer depender a aceitação de assinaturas electrónicas avançadas baseadas num certificado qualificado, com ou sem um dispositivo seguro de criação de assinaturas, de requisitos que levantem obstáculos à utilização, pelos prestadores de serviços, de procedimentos por via electrónica através de balcões únicos.

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

▼C1

4. O n.º 2 não obsta a que os Estados-Membros aceitem assinaturas electrónicas que não sejam assinaturas electrónicas avançadas baseadas num certificado qualificado, com ou sem um dispositivo seguro de criação de assinaturas.

Artigo 2.º

Elaboração, manutenção e publicação de listas aprovadas

1. Cada Estado-Membro deve elaborar, manter e publicar, de acordo com as especificações técnicas apresentadas no anexo, uma «lista aprovada» contendo um mínimo de informação sobre os prestadores de serviços de certificação que emitem certificados qualificados destinados ao público e que são controlados/acreditados por esse Estado-Membro.

▼M1

2. Os Estados-Membros devem elaborar e publicar as suas listas aprovadas em formato legível pelos utilizadores e em formato que permita o tratamento por computador, de acordo com as especificações constantes do anexo.

2-A. Os Estados-Membros assinam electronicamente as suas listas aprovadas em formato que permita o tratamento por computador e publicam-nas em formato legível pelos utilizadores através de, pelo menos, um canal seguro, de modo a garantir a sua autenticidade e integridade.

3. Os Estados-Membros comunicam à Comissão as seguintes informações:

a) o organismo ou organismos responsáveis pela elaboração, manutenção e publicação das listas aprovadas em formato legível pelos utilizadores e em formato que permita o tratamento por computador;

b) os locais em que se encontram publicadas as listas aprovadas em formato legível pelos utilizadores e em formato que permita o tratamento por computador;

c) o certificado de chave pública utilizado para garantir o canal seguro através do qual as listas aprovadas são publicadas em formato legível pelos utilizadores, ou, caso as listas nesse formato sejam assinadas electronicamente, o certificado de chave pública utilizado para esse efeito;

d) o certificado de chave pública utilizado para assinar electronicamente as listas aprovadas em formato que permita o tratamento por computador;

e) quaisquer alterações das informações referidas nas alíneas a) a d).

4. A Comissão disponibiliza a todos os Estados-Membros, através de um canal seguro para um servidor *Web* autenticado, as informações referidas no n.º 3, tal como notificadas pelos Estados-Membros, tanto em formato legível pelos utilizadores como em formato que permita o tratamento por computador.

▼C1

Artigo 3.º

Aplicação

A presente decisão é aplicável com efeitos a partir de 28 de Dezembro de 2009.

Artigo 4.º

Destinatários

Os Estados-Membros são os destinatários da presente decisão.

▼C1

ANEXO

ESPECIFICAÇÕES TÉCNICAS PARA UM PADRÃO DE REFERÊNCIA HARMONIZADO PARA A «LISTA APROVADA DE PRESTADORES DE SERVIÇOS DE CERTIFICAÇÃO CONTROLADOS/ACREDITADOS»

INTRODUÇÃO

1. **Generalidades**

A finalidade do Padrão de Referência Harmonizado para a «Lista Aprovada de Prestadores de Serviços de Certificação controlados/acreditados» dos Estados-Membros é estabelecer uma forma comum de cada Estado-Membro fornecer informação sobre o estado de controlo/acreditação dos serviços de certificação dos Prestadores de Serviços de Certificação ([1]) (PSC) controlados/acreditados por esse Estado-Membro relativamente ao cumprimento das disposições relevantes da Directiva 1999/93/CE. Isso inclui a prestação de informação sobre o histórico do estado de controlo/acreditação dos serviços de certificação controlados/acreditados.

A informação obrigatória a incluir na Lista Aprovada (LA) deve incluir um mínimo de informação sobre os PSC controlados/acreditados que emitem Certificados Qualificados (CQ) ([2]) em conformidade com o disposto na Directiva 1999/93/CE (artigo 3.º, n.os 2 e 3, e artigo 7.º, n.º 7, alínea a)), incluindo informação sobre o CQ que suporta uma assinatura electrónica e sobre se essa assinatura foi ou não criada por um Dispositivo Seguro de Criação de Assinaturas (SSCD) ([3]).

Na Lista Aprovada pode ser incluída, a nível nacional e a título facultativo, informação adicional sobre outros PSC controlados/acreditados que não emitem CQ mas que prestam serviços relacionados com assinaturas electrónicas (por exemplo, PSC que emitem «Tokens» de Validação Cronológica, PSC que emitem certificados não Qualificados, etc.).

Esta informação destina-se essencialmente a apoiar a validação de Assinaturas Electrónicas Qualificadas (AEQ) e Assinaturas Electrónicas Avançadas (AEA) ([4]) suportadas por um Certificado Qualificado ([5]) ([6]).

O Padrão de Referência Harmonizado proposto é compatível com uma aplicação baseada nas especificações da ETSI TS 102 231 ([7]), que são utilizadas para a elaboração, publicação, localização, acessibilidade, autenticação e aprovação deste tipo de listas.

([1]) Ver definição no artigo 2.º, n.º 11, da Directiva 1999/93/CE.
([2]) Ver definição no artigo 2.º, n.º 10, da Directiva 1999/93/CE.
([3]) Ver definição no artigo 2.º, n.º 6, da Directiva 1999/93/CE.
([4]) Ver definição no artigo 2.º, n.º 2, da Directiva 1999/93/CE.
([5]) Neste documento, a sigla «AEA_{CQ}» é utilizada para referir uma AEA acompanhada por um CQ.
([6]) Refira-se que existem diversos serviços electrónicos baseados em AEA simples, cuja utilização transfronteiriça também seria facilitada desde que os serviços de certificação correspondentes (p. ex. a emissão de certificados não-qualificados) sejam incluídos nos serviços controlados/acreditados abrangidos por um Estado-Membro na parte sobre informação voluntária da sua Lista Aprovada.
([7]) ETSI TS 102 231 – Assinaturas e Infra-Estruturas Electrónicas (Electronic Signatures and Infrastructures (ESI)): Prestação de informação harmonizada sobre o estado de confiança do serviço.

▼C1

2. **Orientações para a edição de entradas na LA**

2.1. *Uma LA centrada nos serviços de certificação controlados/acreditados*

Serviços de Certificação e Prestadores de Serviços de Certificação relevantes numa Lista única

A Lista Aprovada de um Estado-Membro é definida como «Lista do Estado de Controlo/Acreditação dos serviços de certificação dos Prestadores de Serviços de Certificação que são controlados/acreditados pelo Estado-Membro referenciado relativamente ao cumprimento das disposições aplicáveis da Directiva 1999/93/CE».

A referida Lista Aprovada deve abranger:

— **todos os Prestadores de Serviços de Certificação**, tal como definidos no artigo 2.º, n.º 11, da Directiva 1999/93/CE, ou seja, «entidade ou pessoa singular ou colectiva que emite certificados ou presta outros serviços relacionados com assinaturas electrónicas»;

— **que são controlados/acreditados** relativamente ao cumprimento das disposições aplicáveis da Directiva 1999/93/CE.

Ao ter em conta as definições e disposições estabelecidas na Directiva 1999/93/CE, em especial no que se refere aos PSC relevantes e aos seus sistemas de controlo/acreditação facultativa, devem distinguir-se dois grupos de PSC: os PSC que emitem CQ destinados ao público (PSCQC) e os PSC que não emitem CQ destinados ao público mas que prestam «outros serviços (acessórios) relacionados com assinaturas electrónicas»:

— **PCS que emitem CQ(s):**

— Estes PSC devem ser controlados pelo Estado-Membro onde se encontrem estabelecidos (se estiverem estabelecidos num Estado-Membro) e também podem ser acreditados relativamente ao cumprimento das disposições estabelecidas na Directiva 1999/93/CE, incluindo os requisitos constantes do anexo I (aplicáveis aos CQ) e do anexo II (aplicáveis aos PSC que emitem CQ). Os PSC que emitem CQ(s) e que são acreditados num Estado-Membro devem ainda estar sujeitos a um sistema adequado de controlo desse Estado-Membro, a menos que não se encontrem estabelecidos nesse Estado-Membro.

— O sistema de «controlo» aplicável (ou o sistema de «acreditação facultativa») é definido pela Directiva 1999/93/CE e deve cumprir os seus requisitos relevantes, em especial os estipulados no artigo 3.º, n.º 3, no artigo 8.º, n.º 1, no artigo 11.º e no considerando 13 (ou no artigo 2.º, n.º 13, no artigo 3.º, n.º 2, no artigo 7.º, n.º 1, alínea a), no artigo 8.º, n.º 1, no artigo 11.º e nos considerandos 4 e 11 a 13).

— **PCS que não emitem CQ(s):**

— Estes PCS podem ser incluídos no âmbito de um sistema de «acreditação facultativa» (como definido na Directiva 1999/93/CE e em cumprimento desta) e/ou no âmbito de um «sistema de aprovação reconhecido», definido a nível nacional e aplicado numa base nacional, para o controlo do cumprimento das disposições estabelecidas na Directiva e, possivelmente, das disposições nacionais referentes à prestação de serviços de certificação (na acepção do artigo 2.º, n.º 11, da Directiva).

— Alguns dos objectos físicos ou binários (lógicos) gerados ou emitidos em resultado da prestação de um serviço de certificação podem ter direito a uma «qualificação» específica, com base no cumprimento das disposições e requisitos estabelecidos a nível nacional, mas o significado dessa «qualificação» poderá limitar-se apenas ao plano nacional.

▼C1

A Lista Aprovada de cada Estado-Membro deve incluir um mínimo de informação sobre os PSC controlados/acreditados que emitem Certificados Qualificados destinados ao público, em conformidade com o disposto na Directiva 1999/93/CE (artigo 3.º, n.os 2 e 3, e artigo 7.º, n.º 7, alínea a)), informação sobre o CQ que suporta uma assinatura electrónica e sobre se essa assinatura foi ou não criada por um Dispositivo Seguro de Criação de Assinaturas.

Na Lista Aprovada pode ser incluída, a nível nacional e a título facultativo, informação adicional sobre outros serviços controlados/acreditados de PSC que não emitem CQ destinados ao público (por exemplo, PSC que prestam Serviços de Validação Cronológica e que emitem «Tokens» de Validação Cronológica, PSC que emitem certificados não Qualificados, etc.).

A Lista Aprovada tem por finalidade:

— enumerar e fornecer informação fiável sobre o estado de controlo/acreditação dos serviços de certificação dos Prestadores de Serviços de Certificação, que são controlados/acreditados pelo Estado-Membro responsável por elaborar e manter a Lista, em cumprimento das disposições aplicáveis estabelecidas na Directiva 1999/93/CE;

— facilitar a validação de assinaturas electrónicas suportadas pelos serviços de certificação controlados/acreditados dos PSC incluídos na lista.

Um conjunto único de valores para o estado de Controlo/Acreditação

Cada Estado-Membro deverá elaborar e manter actualizada uma LA única, que indique o estado de controlo e/ou acreditação dos serviços de certificação dos PSC que são controlados/acreditados por esse Estado-Membro.

O facto de um serviço estar a ser nesse momento controlado ou acreditado é parte do seu estado actual. Para além disso, o estado de controlo ou acreditação pode estar «em curso», «em cessação», «cessado» ou mesmo «revogado». Ao longo da sua vida útil, o mesmo serviço de certificação pode transitar do estado de controlo para o estado de acreditação e vice versa ([1]).

A Figura 1 descreve o fluxo previsto entre possível estado de controlo e possível estado de acreditação, em relação a um único serviço de certificação:

([1]) Por exemplo, um prestador de serviços de certificação estabelecido num Estado-Membro que preste serviços de certificação que sejam, à partida, controlados pelo Estado-Membro (Organismo de Supervisão) poderá, após algum tempo, decidir aplicar a acreditação voluntária para o serviço de certificação objecto de supervisão. Por outro lado, um prestador de serviços de certificação estabelecido noutro Estado-Membro poderá decidir não suspender um serviço de certificação acreditado e passá-lo do estado de acreditação para o estado de supervisão, por motivos de ordem empresarial ou económica.

▼C1

Fluxo previsto do estado de controlo/acreditação de um serviço único de um PSC

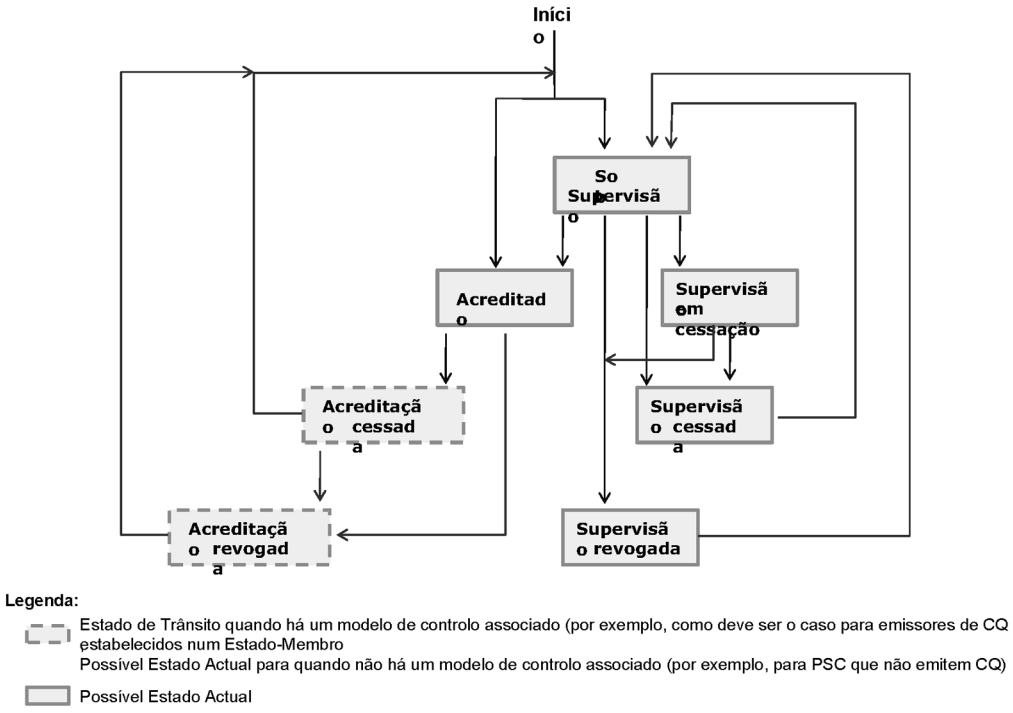


Figura 1

Um serviço de certificação que emite CQ(s) deve ser controlado (se estabelecido num Estado-Membro) e pode ser acreditado facultativamente. O valor do estado desse serviço, se incluído numa Lista Aprovada, pode ter qualquer um dos valores de estado acima representados como «valor actual do estado». No entanto, deve salientar-se que tanto «Acreditação cessada» como «Acreditação revogada» devem ser valores de «estado transitório» apenas no caso de serviços de PSCQC estabelecidos num Estado-Membro, uma vez que esses serviços devem ser controlados por defeito (mesmo quando não estão ou deixaram de estar acreditados).

Exige-se que os Estados-Membros, que estão a elaborar ou já elaboraram um «sistema de aprovação reconhecido», definido a nível nacional e aplicado numa base nacional para o controlo do cumprimento, por parte dos PCS que não emitem CQ, das disposições estabelecidas na Directiva 1999/93/CE e das eventuais disposições nacionais referentes à prestação de serviços de certificação (na acepção do artigo 2.º, n.º 11, da Directiva), incluam esse sistema de aprovação numa das duas categorias seguintes:

— «acreditação facultativa», tal como definida e regulamentada pela Directiva 1999/93/CE (artigo 2.º, n.º 13, artigo 3.º, n.º 2, artigo 7.º, n.º 1, alínea a), artigo 8.º, n.º 1, artigo 11.º e considerandos 4 e 11 a 13);

— «controlo», conforme estipulado na Directiva 1999/93/CE e aplicado através de disposições e requisitos nacionais, em conformidade com as leis nacionais.

▼C1

Por conseguinte, um serviço de certificação que não emite CQ(s) pode ser controlado ou acreditado facultativamente. O valor do estado desse serviço, se incluído numa Lista Aprovada, pode ter qualquer um dos valores de estado acima representados como «valor actual do estado» (ver Figura 1).

A Lista Aprovada deve conter informação sobre o(s) sistemas(s) de controlo/ /acreditação subjacente(s), em especial:

— Informação sobre o sistema de controlo aplicável a todos os PSC_{QC};

— Quando aplicável, informação sobre o sistema nacional de «acreditação facultativa» aplicável a todos os PSC_{QC};

— Quando aplicável, informação sobre o sistema de controlo aplicável a todos os PSC que não emitem CQ;

— Quando aplicável, informação sobre o sistema nacional de «acreditação facultativa» aplicável a todos os PSC que não emitem CQ(s).

Os dois últimos conjuntos de informação têm uma importância fundamental para que os terceiros de confiança avaliem a qualidade e o grau de segurança dos sistemas de controlo/acreditação aplicados a nível nacional aos PSC que não emitem CQ(s). Quando a informação sobre o estado de controlo/acreditação respeitante aos PSC que não emitem CQ(s) é fornecida na LA, os atrás referidos conjuntos de informação deverão ser fornecidos ao nível da LA, através da utilização do «Scheme information URI» (cláusula 5.3.7 — informação fornecida pelos Estados-Membros), «Scheme type/community/rules» (cláusula 5.3.9 — através do uso de um texto comum a todos os Estados-Membros e de informação específica facultativa fornecida por um Estado-Membro) e «TSL policy/legal notice» (cláusula 5.3.11 — um texto comum a todos os Estados-Membros baseado na Directiva 1999/93/CE, juntamente com a possibilidade de cada Estado-Membro acrescentar texto/referências específicos desse Estado-Membro). A informação adicional sobre «qualificação», definida ao nível dos sistemas nacionais de controlo/acreditação de PSC que não emitem CQ(s), pode ser fornecida ao nível do serviço, quando aplicável e requerido (por exemplo, para distinguir entre vários níveis de qualidade/segurança), usando a extensão «additionalServiceInformation» (cláusula 5.8.2) como parte da «Service information extension» (cláusula 5.5.9). As especificações pormenorizadas constantes do capítulo I apresentam mais informação sobre as especificações técnicas correspondentes.

Apesar de um Estado-Membro poder encarregar organismos diferentes do controlo e da acreditação dos serviços de certificação nesse Estado-Membro, espera-se que seja utilizada uma entrada única para cada serviço de certificação (identificada pela sua «Service digital identity» de acordo com os termos da ETSI TS 102 231 [1]) e que o seu estado de controlo/acreditação seja actualizado em consequência. O significado dos estados anteriormente indicados é descrito na cláusula 5.5.4 das especificações técnicas apresentadas no capítulo I.

2.2. *Entradas na LA destinadas a facilitar a validação de AEQ e AEA_{CQ}*

A parte mais difícil da criação da LA é a organização da parte obrigatória da LA, designadamente a «Lista de serviços» por PSC que emitem CQ(s), de modo a reflectir correctamente a situação exacta de emissão de cada serviço de certificação emissor de CQ(s) e a garantir que a informação fornecida em cada entrada é suficiente para facilitar a validação de AEQ e de AEA_{CQ} (quando combinada com o conteúdo do CQ da entidade final emitido pelo PSC no quadro do serviço de certificação registado nesta entrada).

[1] ETSI TS 102 231 — Assinaturas e Infra-Estruturas Electrónicas [Electronic Signatures and Infrastructures (ESI)]: Prestação de informação harmonizada sobre o estado de confiança do serviço.

▼C1

Dado que não existe um perfil verdadeiramente interoperativo e transfronteiriço para o CQ, a informação exigida poderá incluir outras informações além da «Service digital identity» de uma única (Root) CA, em especial informação que identifique o estatuto de CQ do certificado emitido, e que indique se as assinaturas por ele suportadas foram ou não criadas por um SSCD. O organismo que, num Estado-Membro, tenha sido indicado para elaborar, editar e manter a LA (ou seja, o operador do sistema, segundo a ETSI TS 102 231) deve, por conseguinte, ter em conta o perfil actualizado e o conteúdo do certificado em cada CQ emitido, para cada PSC_{CQ} incluído na LA.

Sempre que possível, cada CQ emitido deverá incluir a declaração de QcCompliance ([1]) definida pelo ETSI, sempre que se afirma tratar-se de um CQ, e a declaração QcSSCD definida pelo ETSI, sempre que se afirma que este é suportado por um SSCD para criar assinaturas electrónicas, e/ou que cada CQ emitido inclui um dos QCP/QCP + Identificadores de Objecto (OID) de política de certificados definidos pela ETSI TS 101 456 ([2]). A utilização pelos PSC que emitem CQ(s) de normas diferentes como referência, o vasto leque de interpretações dessas normas e, ainda, o desconhecimento da existência e da precedência de algumas especificações técnicas e normas convencionadas, deram origem a diferenças no conteúdo real dos CQ(s) actualmente emitidos (por exemplo, a utilização ou não das QcStatements definidas pelo ETSI) e, consequentemente, impedem que os destinatários confiem facilmente no certificado do signatário (e na cadeia/caminho que lhe estão associados) para avaliar, pelo menos numa forma processável por computador, se é afirmado ou não que o certificado que suporta uma assinatura electrónica é um CQ e se este está ou não associado a um SSCD, através do qual a assinatura foi criada.

Preencher os campos «Service type identifier» («Sti»), «Service name» («Sn») e «Service digital identity» («Sdi») ([3]) com informação fornecida no campo «Service information extensions» («Sie») permite que o padrão de referência harmonizado proposto para a LA determine integralmente um tipo específico de certificado qualificado, emitido por um PSC incluído na lista de serviços de certificação que emitem CQ(s), e forneça informação sobre se este é ou não suportado por um SSCD (quando essa informação não constar do CQ emitido). A informação específica «Service current status» («Scs») está, evidentemente, associada a esta entrada. Este processo está representado na Figura 2 (adiante).

Incluir um serviço na lista indicando apenas o «Sdi» de uma (Root) CA significaria que é garantido (pelo PCS emissor de CQ(s) e, também, pelo Organismo de Controlo/Acreditação encarregado do controlo/acreditação desse PCS) que qualquer certificado de entidade final emitido no âmbito dessa (Root) CA (hierarquia) contém suficiente informação definida pelo ETSI e susceptível de ser processada por computador para se avaliar se se trata ou não de um CQ, e se este é ou não suportado por um SSCD. Por exemplo, no caso de a última afirmação não ser verdadeira (por exemplo, o CQ não contém nenhuma indicação processável por computador e normalizada do ETSI sobre se este é ou não suportado por um SSCD), listar apenas o «Sdi» dessa (Root) CA leva apenas a concluir que os CQ(s) emitidos no âmbito da hierarquia desta (Root) CA não são suportados por nenhum SSCD. Para se poder considerar que esses DC(s) são suportados por um SSCD, a «Sie» deverá ser utilizada para indicar este facto (o que também indica que é garantido pelo PSC emissor e controlado/acreditado, respectivamente, pelo Organismo de Controlo ou de Acreditação).

([1]) Veja-se ETSI TS 101 862 — Assinaturas e Infra-Estruturas Electrónicas [Electronic Signatures and Infrastructures (ESI)]: Características dos Certificados Qualificados.

([2]) ETSI TS 101 456 — Assinaturas e Infra-Estruturas Electrónicas [Electronic Signatures and Infrastructures (ESI)]; Requisitos para os organismos de certificação emissores de certificados qualificados.

([3]) Ou seja, e como mínimo, um certificado X.509 v3 da ACQ (Autoridade de Certificação Qualificada) emissora ou de uma AC superior no percurso de certificação.

▼C1

Princípios gerais — Regras de edição — Entradas de PSC_{QC} (serviços listados)

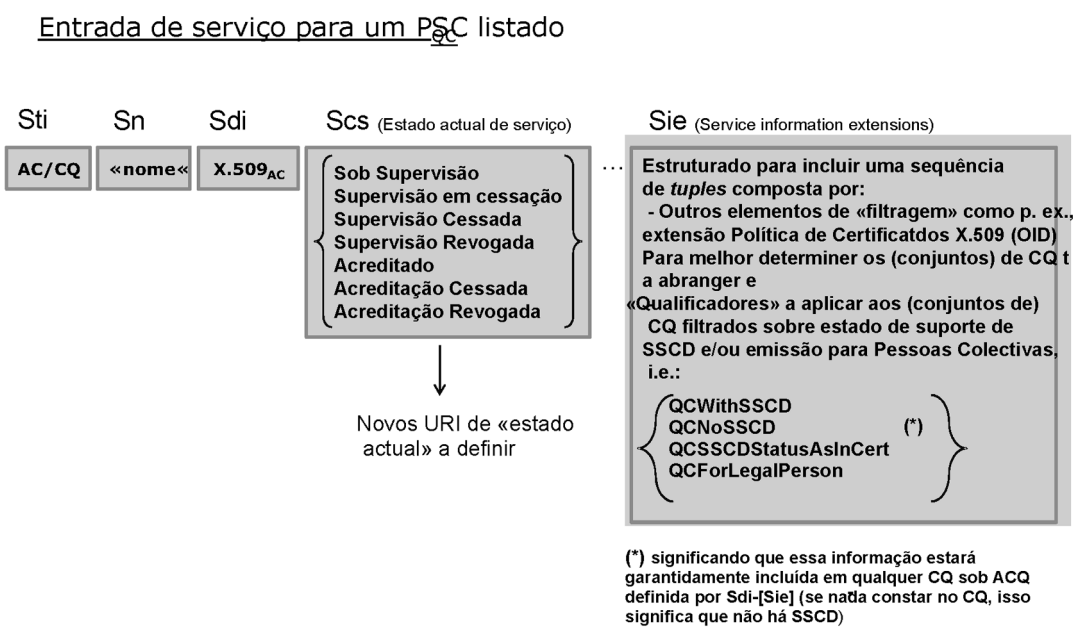


Figura 2:

Entrada de serviço de um PSC que emite CQ(s) incluído na LA executada em formato TSL

As presentes especificações técnicas do padrão de referência harmonizado para a LA permitem utilizar uma combinação de cinco partes principais de informação na entrada de serviço:

— O «Service type identifier» («Sti») [Identificador do tipo de serviço], por exemplo, que identifica uma AC que emite CQ(s) («AC/CQ»);

— O «Service name» («Sn») [Nome do serviço];

— A «Service digital identity» («Sdi») [Identidade digital do serviço] — informação que identifica um serviço listado, por exemplo o certificado X.509v3 (no mínimo) de uma AC que emite CQ(s);

— Para os serviços AC/CQ, informação facultativa «Service information extensions» («Sie») [Extensões de informação do serviço] que permitirá a inclusão de uma sequência de um ou mais tuplos, cada um dos quais indica:

  — Os critérios a utilizar para identificar, a um nível superior (filtro), o serviço de certificação específico ide «Sdi» (ou seja, um conjunto de certificados qualificados) para o qual é requerida/fornecida informação complementar no que se refere à indicação do suporte por um SSCD (e/ou a emissão para uma Pessoa Colectiva); e

  — A informação associada («qualificadores») sobre se o conjunto de certificados qualificados, emitidos por um serviço identificado a um nível superior, é ou não suportado por um SSCD, ou sobre se esta informação associada é incluída no CQ sob uma forma normalizada processável por computador, e/ou informação referente ao facto de esses CQ(s) serem emitidos para Pessoas Colectivas (por defeito, estes devem ser considerados como tendo sido emitidos apenas para Pessoas Singulares).

▼C1

— A informação sobre o «current status» [estado actual] desta entrada de serviço, que forneça informação sobre:

— Se é ou não um serviço controlado ou acreditado, e

— O estado de controlo/acreditação em si.

2.3. *Edição e utilização de orientações para entradas de serviço de PSC_{CQ}*

As **orientações gerais de edição** são:

1. Quando é garantido (garantia prestada por um PSC_{CQ} e controlada/acreditada por um Organismo de Controlo (OC)/Organismo de Acreditação (OA) que, no que se refere a um serviço listado identificado por um «Sdi», qualquer CQ suportado por um SSCD contém de facto a declaração de QcCompliance definida pelo ETSI, e contém de facto a declaração QcSSCD e/ou QCP + Identificador de Objecto (OID), a utilização de um «Sdi» adequado é suficiente e o campo «Sie» pode ser utilizado em opção e não precisa de incluir a informação sobre suporte por SSCD.

2. Quando é garantido (garantia prestada por um PSC_{CQ} e controlada/acreditada por um OC/OA) que, no que se refere a um serviço listado identificado por um «Sdi», qualquer CQ não suportado por um SSCD contém de facto a declaração de QcCompliance e/ou QCP + OID, e que este é de um tipo que não requer a inclusão da declaração QcSSCD ou QCP + OID, a utilização de um «Sdi» adequado é suficiente e o campo «Sie» pode ser utilizado em opção e não precisa de conter a informação sobre suporte por um SSCD (o que significa que não é suportado por um SSCD)

3. Quando é garantido (garantia prestada por um PSC_{CQ} e controlada/acreditada por um OC/OA) que, no que se refere a um serviço listado identificado por um «Sdi», qualquer CQ contém de facto a declaração de QcCompliance e que alguns desses CQ(s) devem ser suportados por um SSCD e outros não (por exemplo, essa distinção pode ser feita por OID específicas de Políticas de Certificados de um PSC ou através de outra informação específica do PSC contida no CQ, directa ou indirectamente, processável por computador ou não), mas que o CQ não contém NEM a declaração QcSSCD NEM o QCP(+) OID do ETSI, a utilização de um «Sdi» adequado pode não ser suficiente E o campo «Sie» deve ser utilizado para indicar informação explícita de suporte por um SSCD, juntamente com uma potencial extensão de informação que identifique o grupo de certificados abrangidos. Isto poderá requerer a inclusão de «valores de informação sobre suporte por um SSCD» diferentes para o mesmo «Sdi», quando se fizer uso do campo «Sie».

4. Quando é garantido (garantia prestada por um PSC_{CQ} e controlada/acreditada por um OC/OA) que, no que se refere a um serviço listado identificado por um «Sdi», nenhum CQ contém a declaração de QcCompliance, o QCP OID, a declaração QcSSCD ou o QCP + OID mas se garante que alguns dos certificados de entidade final emitidos ao abrigo deste «Sdi» devem ser entendidos como CQ e/ou como suportados por um SSCD, e outros não (por exemplo, essa distinção pode ser feita por OID específicas de Políticas de Certificados de um PSC_{CQ} ou através de outra informação específica do PSC_{CQ} contida no CQ, directa ou indirectamente, processável por computador ou não), a utilização de um «Sdi» adequado não será suficiente E o campo «Sie» deve ser utilizado para indicar informação explícita de suporte por um SSCD. Isto poderá requerer a inclusão de «valores de informação sobre suporte por um SSCD» diferentes para o mesmo «Sdi» quando se fizer uso do campo «Sie».

▼C1

Como princípio geral por defeito, um PSC incluído na Lista Autorizada deve ter uma entrada de serviço por cada certificado X.509v3 para um tipo de serviço de certificação AC/CQ, ou seja, uma Autoridade de Certificação que emite (directamente) CQ(s). Em algumas situações cuidadosamente ponderadas e em condições cuidadosamente geridas, o Organismo de Controlo/Organismo de Acreditação de um Estado-Membro pode decidir utilizar o certificado X.509v3 de uma Root AC ou de uma AC de nível superior (ou seja, uma Autoridade de Certificação que não emite directamente CQ(s) de entidade final mas que certifica uma hierarquia de AC(s) até às AC(s) que emitem CQ para entidades finais) como o «Sdi» de uma única entrada na lista de serviços de um PSC incluído na LA. As consequências (vantagens e desvantagens) de usar esse X.509v3 da Root AC ou AC de nível superior como valores do «Sdi» de entradas de serviço da LA deve ser cuidadosamente analisada e aprovada pelos Estados-Membros. Além disso, sempre que utilizar esta excepção autorizada ao princípio por defeito, o Estado-Membro deve fornecer a documentação necessária para facilitar a construção e verificação do caminho de certificação.

Para ilustrar as orientações gerais de edição, pode apresentar-se o seguinte exemplo: No caso de um PSC_{CQ} que utiliza uma Root AC sob a qual várias AC(s) emitem CQ(s) e certificados não qualificados, mas para a qual os CQ(s) incluem apenas a declaração de QcCompliance mas não qualquer indicação de se são suportados por um SSCD, listar o «Sdi» da Root AC significará, nos termos das regras anteriormente explicadas, que qualquer CQ emitido ao abrigo dessa hierarquia de Root AC NÃO é suportado por um SSCD. Se esses CQ(s) forem realmente suportados por um SSCD, será altamente recomendável utilizar a declaração QcSSCD nos CQ(s) emitidos no futuro. Entretanto (até o último CQ que não contém esta informação ter expirado), a TSL deverá utilizar o campo «Sie» e a extensão «Qualifications» que lhe está associada, por exemplo, filtrando certificados através do(s) OID definido(s) para PSC_{CQ} específicos eventualmente utilizados pelo PSC_{CQ} para fazer a distinção entre tipos diferentes de CQ(s) (alguns suportados por um SSCD e outros não) e incluindo «informação sobre suporte por um SSCD» explícita no que se refere aos certificados filtrados através do uso de «Qualificadores».

As **orientações gerais de utilização** para aplicações, serviços ou produtos associados às assinaturas electrónicas e dependentes da aplicação TSL de uma Lista Autorizada em conformidade com as presentes Especificações Técnicas são as seguintes:

Uma entrada «Sti» de uma «AC/CQ» (tal como uma entrada AC/CQ qualificada a um nível superior como «RootAC/CQ» através do recurso à extensão «Sie» additionalServiceInformation)

— indica que, a partir da AC identificada pelo «Sdi» (tal como dentro da hierarquia da CA que começa pela RootAC identificada pelo «Sdi»), todos os certificados de entidade final emitidos são CQ(s), **desde** que isso seja afirmado no certificado através do uso das QcStatements adequadas (ou seja, QcC, QcSSCD) e/ou de OID QCP(+) definidos pelo ETSI (e que isto seja garantido pelo Organismo de Controlo/Acreditação, ver atrás «orientações gerais de edição»)

Nota: se não for apresentada qualquer informação «qualificação»«Sie» ou se um certificado de entidade final que pretenda ser um CQ não for «identificado a um nível superior», através de uma entrada «Sie» relacionada, a informação «processável por computador» contida no CQ é controlada/acreditada como precisa. Isto significa que a utilização (ou não) das QcStatements adequadas (ou seja, QcC, QcSSCD) e/ou de OID QCP(+) definidos pelo ETSI será garantidamente conforme com aquilo que é afirmado pelo PSC_{CQ}.

▼C1

— **e SE** a informação «Sie»«Qualification» estiver presente, então, além do recurso à atrás referida regra de interpretação por defeito sobre o uso, os certificados que são identificados através da utilização desta entrada «Sie»«Qualification», que é construída com base no princípio de uma sequência de «filtros» que identificam um conjunto de certificados a um nível superior e fornecem alguma informação adicional sobre «suporte por um SSCD» e/ou «Pessoa colectiva como sujeito» (por exemplo, os certificados que contêm um OID específico na extensão Política de Certificados, e/ou que têm um padrão «Key usage» específico, e/ou filtrados através do uso de um valor específico que deve aparecer num campo ou numa extensão específicos de um certificado, etc.), deverão ser considerados de acordo com o conjunto de «qualificadores» que se seguem e que compensam a falta de informação no CQ correspondente, a saber:

— para indicar o suporte por um SSCD:

  — o valor do qualificador «QCWithSSCD», que significa «CQ suportado por um SSCD», ou

  — o valor do qualificador «QCNoSSCD», que significa «CQ não suportado por um SSCD», ou

  — o valor do qualificador «QCSSCDStatusAsInCert», que significa que a informação sobre o suporte por um SSCD está garantidamente incluída em qualquer CQ, na informação «Sdi»-«Sie» fornecida nesta entrada AC/CQ;

  e/ou

— para indicar emissão em favor de uma Pessoa Colectiva:

  — o valor do qualificador «QCForLegalPerson», que significa «Certificado emitido em favor de uma Pessoa Colectiva»

2.4. *Serviços que suportam os serviços «AC/CQ» mas que não são partes do «Sdi»«AC/CQ»*

Deverão também ser abrangidos os casos em que as respostas das LRC e dos OCSP são assinadas por chaves diferentes da chave de uma AC que emite CQ(s) («AC/CQ»). Estes casos podem resolvidos listando esses serviços como tal na execução TSL da LA (ou seja, com um «Service type identifier» [Identificador de tipo serviço] qualificado a nível superior por uma extensão «additionalServiceInformation», que reflicta um serviço de OCSP ou LRC como sendo parte no fornecimento de CQ(s), por exemplo com um tipo de serviço de «OCSP/CQ» ou «LRC/CQ», respectivamente), uma vez que estes serviços podem ser considerados como parte dos serviços controlados/acreditados «qualificados» relacionados com a prestação de serviços de certificação de CQ(s). Como é evidente, os respondedores OCSP ou os Emissores de LRC cujos certificados sejam assinados por AC(s) hierarquicamente dependentes de um serviço AC/CQ listado deverão ser considerados «válidos» e conformes com o valor do estado do serviço AC/CQ listado.

Aos serviços de certificação que emitam certificados não qualificados (do tipo de serviço «AC/PKC») e que usem por defeito os tipos de serviço ETSI TS102 231 OCSP e LRC poderá aplicar-se uma disposição semelhante.

Saliente-se que a execução TSL da LA DEVE incluir serviços de revogação, quando a informação associada não é apresentada no campo AIA dos certificados finais ou quando não é assinada por uma AC incluída na lista das AC.

2.5. *Avançar para um perfil de CQ interoperativo*

Como regra geral, deve tentar-se simplificar (reduzir) tanto quanto possível o número de entradas de serviços («Sdi» diferentes). Isto deve, porém, ser contrabalançado pela identificação correcta dos serviços que estão relacionados com a emissão de CQ(s) e com a prestação de informação fiável sobre se esses CQ(s) são ou não suportados por um SSCD, quando essa informação é omissa no CQ emitido.

▼C1

Sempre que possível, a utilização do campo «Sie» e da extensão «Qualification» deverá ser (rigorosamente) restringida aos casos específicos que é preciso resolver desta forma, uma vez que os CQ(s) deverão conter informação suficiente referente ao alegado estatuto de qualificado e à alegação de serem ou não suportados por um SSCD.

Os Estados-Membros deverão, na medida do possível, impor a adopção e a utilização de perfis de CQ interoperativos.

3. **Estrutura do Padrão de Referência Harmonizado para a Lista Aprovada**

A estrutura do Padrão de Referência Harmonizado proposto para a Lista Aprovada de cada Estado-Membro incluirá as seguintes categorias de informação:

1. Informação sobre a Lista Aprovada e respectivo sistema de emissão;

2. Uma sequência de campos contendo informação de identificação inequívoca sobre todos os PSC controlados/acreditados incluídos no sistema (esta sequência é facultativa, ou seja, quando não for utilizada a lista será considerada vazia, o que significa que não há nenhum PSC controlado ou acreditado no Estado-Membro associado, no que se refere ao âmbito da Lista Aprovada);

3. Para cada PSC listado, uma sequência de campos contendo a identificação inequívoca do serviço de certificação controlado/acreditado prestado por esse PSC (esta sequência deve ter no mínimo uma entrada);

4. Por cada serviço de certificação controlado/acreditado incluído na lista, a identificação do estado actual do serviço e o histórico desse estado.

Nos casos de PSC que emitem CQ(s), a identificação inequívoca de um serviço de certificação controlado/acreditado a incluir na lista deve ter em conta as situações em que o certificado qualificado não disponibiliza informação suficiente sobre o seu estado de «qualificado» e sobre o seu hipotético suporte por um SSCD, em especial para fazer face ao facto adicional de a maioria dos PSC (comerciais) recorrer a uma única AC Qualificada para a emissão de vários tipos de certificados de entidade final, qualificados e não qualificados.

O número de entradas na lista por PSC reconhecido pode ser reduzido, quando existam um ou vários serviços de AC de nível Superior, por exemplo nos casos de uma hierarquia comercial de AC(s) da Root CA até às AC(s) emissoras. No entanto, mesmo nestes casos, o princípio de garantir a ligação inequívoca entre o serviço de certificação de um PSCCQ e o conjunto de certificados que se pretende sejam identificados como CQ(s) tem de ser mantido e assegurado.

1. *Informação sobre a Lista Aprovada e respectivo sistema de emissão*

Fará parte desta categoria a seguinte informação:

— Um **tag [etiqueta]** de Lista Aprovada que facilite a identificação da Lista Aprovada durante as pesquisas electrónicas e, também, para confirmar as suas finalidades quando em forma legível por pessoas;

— Um **formato e identificador da versão de formato** da Lista Aprovada;

— Um **número de sequência (ou de versão)** da Lista Aprovada;

— Um **tipo de informação** da Lista Aprovada (por exemplo, para identificar o facto de esta Lista Aprovada fornecer informação sobre o estado de controlo/ /acreditação dos serviços de certificação dos PSC controlados/acreditados pelo Estado-Membro referenciado, em cumprimento do disposto na Directiva 1999/93/CE);

▼C1

— **Informação sobre o proprietário** da Lista Aprovada (por exemplo, nome, endereço, contactos, etc. do Organismo do Estado-Membro encarregado de elaborar, publicar com segurança e actualizar a Lista Aprovada);

— **Informação sobre o(s) sistema(s) subjacente(s) de controlo/acreditação** a que a Lista Aprovada está associada, incluindo, sem que esta enumeração tenha carácter exaustivo:

  — o país a que se aplica,

  — informação sobre ou referência ao endereço onde se pode encontrar informação sobre o(s) sistema(s) (modelo do sistema, regras, critérios, comunidade aplicável, tipo, etc.),

  — período de conservação de informação (histórica).

— **Política e/ou aviso legal, obrigações, responsabilidades** da Lista Aprovada;

— **Data e hora da emissão e previsão da próxima actualização** da Lista Aprovada.

2. *Informação de identificação inequívoca sobre todos os PCS reconhecidos pelos sistema*

Este conjunto de informação incluirá pelo menos o seguinte:

— O nome da organização PSC tal como figura nos registos legais oficiais (podendo incluir a identificação de utilizador da organização PSC, de acordo com as práticas do Estado-Membro);

— O endereço e contactos do PSC;

— Informação complementar sobre o PSC, apresentada directamente ou através de referência a um endereço de onde essa informação pode ser descarregada.

3. *Por cada PSC listado, uma sequência de campos contendo a identificação inequívoca do serviço de certificação prestado por esse PSC e controlado/acreditado no âmbito da Directiva 1999/93/CE*

Este conjunto de informação incluirá pelo menos os dados seguintes, relativamente a cada serviço de certificação de um PSC incluído na lista:

— Um identificador do tipo de serviço de certificação (por exemplo, identificador que indique que o serviço de certificação do PSC controlado/acreditado é uma Autoridade de Certificação que emite CQ);

— Denominação (comercial) desse serviço de certificação;

— Um identificador único e inequívoco desse serviço de certificação;

— Informação complementar sobre o serviço de certificação (por exemplo apresentada directamente ou através da referência de um endereço de onde essa informação pode ser descarregada, informação de acesso ao serviço).

— Para os serviços AC/CQ, uma sequência facultativa de tuplos de informação, cada um dos quais indicando

  i. Os critérios a utilizar numa identificação de nível superior (filtro) desse serviço de certificação específico, no âmbito do serviço de certificação identificado pela «Sdi» (ou seja, um conjunto de certificados qualificados), em relação ao qual é requerida/fornecida informação complementar no que se refere à indicação do SSCD de suporte (e/ou emissão para uma Pessoa Colectiva); e

  ii. Os «qualificadores» associados que fornecem informação sobre se o conjunto dos certificados qualificados emitidos pelo serviço identificado ao nível superior é ou não suportado por um SSCD, e/ou informação sobre se esses CQ são emitidos para Pessoas Colectivas (por defeito, devem ser considerados como tendo sido emitidos para Pessoas Singulares).

▼C1

4. *Para cada serviço de certificação incluído na lista, a identificação do estado actual do serviço e o histórico desse estado.*

Este conjunto de informação incluirá pelo menos o seguinte:

— Um identificador do Estado Actual

— Data e hora do início do Estado Actual;

— Informação histórica sobre esse estado.

4. **Definições e Abreviaturas**

Para os fins do presente documento, são aplicáveis as seguintes definições e siglas:

Termo	Sigla	Definição
Prestador de Serviços de Certificação	PSC	Como definido no artigo 2.º, n.º 11, da Directiva 1999/93/CE
Autoridade de Certificação	AC	Uma AC é um PSC e pode usar várias chaves técnicas privadas de assinatura de AC, cada uma das quais com um certificado associado, para emitir certificados para entidades finais. Uma AC é uma autoridade na qual um ou mais utilizadores confiam para criar e atribuir certificados. A título facultativo, a Autoridade de Certificação pode criar as chaves dos utilizadores [ETSI TS 102 042]. A AC deve ser identificada através da informação de identificação presente no campo Emissor do certificado da AC relacionado com (que certifica) a chave pública associada à chave de assinatura privada da AC, que esta utiliza de facto para emitir certificados para entidades. Uma AC pode ter várias chaves de assinatura. A chave de assinatura de cada AC é inequivocamente identificada por um identificador único como parte do campo Authority Key Identifier do certificado da AC.
Autoridade de Certificação que emite Certificados Qualificados	AC/CQ	Uma AC que cumpre os requisitos estipulados no anexo II da Directiva 1999/93/CE e emite certificados qualificados que cumprem os requisitos estipulados no anexo I da Directiva 1999/93/CE.
Certificado	Certificado	Como definido no artigo 2.º, n.º 9, da Directiva 1999/93/CE
Certificado Qualificado	CQ	Como definido no artigo 2.º, n.º 10, da Directiva 1999/93/CE
Signatário	Signatário	Como definido no artigo 2.º, n.º 3, da Directiva 1999/93/CE
Controlo	Controlo	«Controlo» é utilizado na acepção da Directiva 1999/93/CE (artigo 3.º, n.º 3). A Directiva exige que os Estados-Membros elaborem um sistema adequado que permita o controlo dos PSC estabelecidos nos seus territórios que emitam certificados qualificados destinados ao público, garantindo o controlo do cumprimento das disposições estabelecidas na Directiva.
Acreditação Facultativa	Acreditação	Como definido no artigo 2.º, n.º 13, da Directiva 1999/93/CE
Lista Aprovada	LA	Designa a lista que indica o estado de controlo/acreditação dos serviços de certificação dos Prestadores de Serviços de Certificação, que sejam controlados/acreditados pelo Estado-Membro relativamente ao cumprimento das disposições estabelecidas pela Directiva 1999/93/CE.

▼C1

Termo	Sigla	Definição
Lista de estado dos serviços de confiança	TSL	Modelo de lista assinada utilizado como base para a apresentação de informação sobre o estado de serviço autorizado, em conformidade com as especificações estabelecidas na ETSI TS 102 231.
Serviço de confiança		Serviço que reforça a confiança e a segurança relativamente às transacções electrónicas (que habitualmente mas não necessariamente utiliza técnicas criptográficas ou envolve material confidencial) (ETSI TS 102 231).
Fornecedor de Serviços de Confiança	TSP	Organismo de que depende um ou mais Serviço(s) de Confiança (electrónico(s)) (Esta designação é utilizada numa acepção mais vasta do que PSC).
«Token» de Serviço de Confiança	TrST	Objecto físico ou binário (lógico) gerado ou emitido em resultado do recurso a um Serviço de Confiança. Exemplos de TrST binários são certificados, LCR, «Tokens» de Validação Cronológica e respostas do Protocolo OCSP.
Assinatura Electrónica Qualificada	AEQ	AEA suportada por um CQ e criada por um SSCD, como definido no artigo 2.º da Directiva 1999/93/CE
Assinatura Electrónica Avançada	AEA	Como definido no artigo 2.º, n.º 2, da Directiva 1999/93/CE
Assinatura Electrónica Avançada suportada por um Certificado Qualificado	AEA_{CQ}	Significa uma Assinatura Electrónica que satisfaz os requisitos de uma AEA e é suportada por um CQ, como definido no artigo 2.º da Directiva 1999/93/CE
Dispositivo Seguro de Criação de Assinaturas	SSCD	Como definido no artigo 2.º, n.º 6, da Directiva 1999/93/CE

CAPÍTULO I

ESPECIFICAÇÕES PORMENORIZADAS RELATIVAS AO MODELO COMUM PARA A «LISTA APROVADA DE PRESTADORES DE SERVIÇOS DE CERTIFICAÇÃO CONTROLADOS/ACREDITADOS»

Na parte seguinte do presente documento, as palavras-chave «DEVE», «NÃO DEVE», «OBRIGATÓRIO», «DEVERÁ», «NÃO DEVERÁ», «DEVERIA», «NÃO DEVERIA», «RECOMENDADO», «PODE», e «FACULTATIVO» devem ser interpretadas tal como se descreve no RFC 2119 ([1]).

►**M1** As presentes especificações baseiam-se nas especificações e nos requisitos constantes da ETSI TS 102231 v.3.1.2. Nos casos em que as presentes especificações não apresentem nenhum requisito específico, DEVERÃO aplicar-se na íntegra os requisitos da ETSI TS 102231 v.3.1.2. ◄ Quando as presentes especificações estabelecerem requisitos específicos, estes DEVERÃO prevalecer sobre os requisitos correspondentes da ETSI TS 102 231, sendo complementados pelas especificações de formato estabelecidas na ETSI TS 102 231. Em caso de discrepâncias entre as presentes especificações e as especificações da ETSI TS 102 231, as especificações normativas SERÃO as presentes.

([1]) IETF RFC 2119: «Palavras-chave para utilização em RFC para indicar níveis de requisitos».

▼C1

O suporte linguístico DEVERÁ ser aplicado e apresentado pelo menos em inglês (EN) e eventualmente também numa ou mais línguas nacionais.

A indicação de data e hora DEVERÁ ser conforme com a cláusula 5.1.4 da ETSI TS 102 231.

A utilização de URI (identificadores de recursos uniformes) DEVERÁ ser conforme com a cláusula 5.1.5 da ETSI TS 102 231.

Informação sobre Sistema de Emissão da Lista Aprovada

Tag

TSL tag (cláusula 5.2.1)

Este campo É OBRIGATÓRIO E DEVERÁ ser conforme com a cláusula 5.2.1 da ETSI TS 102 231.

▼M1

———————

▼C1

Scheme Information

TSL version identifier (cláusula 5.3.1)

Este campo É OBRIGATÓRIO e DEVERÁ ser ajustado para «3» (número inteiro).

TSL sequence number (cláusula 5.3.2)

▼M1

Este campo é OBRIGATÓRIO. DEVERÁ especificar o número de sequência da TSL. A começar do «1», na primeira versão da TSL, o valor deste número inteiro DEVERÁ ser incrementado em cada versão posterior da TSL. O valor «1» NÃO DEVERÁ ser reposto quando o «TSL version identifier» acima referido for aumentado.

▼C1

TSL type (cláusula 5.3.3)

▼M1

Este campo É OBRIGATÓRIO e especificará o tipo de TSL. DEVERÁ apontar para http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Genérico).

▼C1

Nota: Para dar cumprimento à cláusula 5.3.3 da ETSI TS 102 231 e para indicar o tipo específico de TSL, referindo simultaneamente a existência das presentes especificações, que regem a organização da aplicação TSL da Lista Aprovada ([1]) dos Estados-Membros e permitem que um analisador sintáctico determine a forma previsível de qualquer dos campos ([2]) seguintes, quando esses campos têm significados específicos (ou alternativos) consoante o tipo de TSL representado (neste caso, uma Lista Aprovada de um Estado-Membro), o URI específico atrás referido DEVERÁ ser registado e descrito como se segue:

([1]) Ou seja, a «Lista de Estado de Acreditação/Supervisão de serviços de certificação de Prestadores de Serviços de Certificação, que sejam controlados/acreditados pelo Estado-Membro referido relativamente ao cumprimento das disposições pertinentes previstas na Directiva 1999/93/CC» (abreviadamente, a «Lista Autorizada»).

([2]) Quer dizer os campos especificados na ETSI TS 102 231 — Assinaturas e Infra-Estruturas Electrónicas (Electronic Signatures and Infrastructures (ESI): Prestação de informação harmonizada sobre o estado de confiança do serviço e cujo «perfil» é definido nas actuais especificações para determinar o estabelecimento da Lista Aprovada dos Estados-Membros.

▼M1

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

▼C1

Descrição: A aplicação TSL de uma lista do estado de controlo/acreditação dos serviços de certificação de prestadores de serviços de certificação que são controlados/acreditados pelo Estado-Membro referenciado, proprietário da aplicação TSL, quanto ao cumprimento das disposições aplicáveis fixadas pela Directiva 1999/93/CE, através de um processo de supervisão directa (voluntária ou normativa).

Scheme operator name (cláusula 5.3.4)

Este campo é OBRIGATÓRIO. DEVERÁ especificar o nome do Organismo do Estado-Membro encarregado de elaborar, publicar e manter actualizada a Lista Aprovada Nacional. DEVERÁ especificar a denominação formal sob a qual opera a entidade jurídica associada a este Organismo ou a entidade por ele mandatada (por exemplo, serviços administrativos governamentais). DEVE tratar-se da denominação utilizada no registo ou na autorização legal formal e à qual deve ser dirigida qualquer comunicação formal. DEVERÁ ser uma Sequência de cadeias de caracteres multilingues e DEVERÁ ser executada com o inglês (EN) como língua obrigatória e, eventualmente, com uma ou mais língua(s) nacional(is).

Nota: Os países PODEM ter Organismos de Controlo e de Acreditação distintos e até outros organismos além destes para realizar quaisquer outras actividades operacionais relacionadas. ►M1 Cabe a cada Estado-Membro designar o operador do Sistema de aplicação TSL da LA do Estado-Membro. ◄ Considera-se que (quando houver organismos separados) o Organismo de Controlo, o Organismo de Acreditação e o Operador do Sistema terão obrigações e responsabilidades próprias.

Todos os casos em que haja vários organismos com responsabilidades de controlo, de acreditação e de operacionalização, estes DEVERÃO ser sempre indicados e identificados como tal na informação sobre o Sistema, como parte da LA, incluindo na informação específica sobre o sistema indicada pelo «Scheme information URI» (cláusula 5.3.7).

▼M1

O operador do Sistema designado (cláusula 5.3.4) é a entidade que deverá assinar a TSL.

▼C1

Scheme operator address (cláusula 5.3.5)

Este campo é OBRIGATÓRIO. DEVERÁ especificar os endereços postal e para comunicações electrónicas da entidade jurídica ou organização mandatada identificada no campo «Scheme operator name» (cláusula 5.3.4). DEVERÁ incluir o «PostalAddress» (ou seja, nome da rua, localidade, [estado ou província], [código postal] e código para a representação do nome do país ISO 3166-1 alfa-2), em conformidade com a cláusula 5.3.5.1; e o «ElectronicAddress» (ou seja, endereço de correio electrónico e/ou URI do sítio web), em conformidade com a cláusula 5.3.5.2.

Scheme name (cláusula 5.3.6)

Este campo É OBRIGATÓRIO e especificará a denominação sob a qual o sistema opera. DEVERÁ ser uma sequência de cadeias de caracteres multilingues (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)), definida como se segue:

▼C1

— A versão EN DEVERÁ ser uma cadeia de caracteres estruturada como se segue:

CC:EN_name_value

em que

— «CC» = o Código de País ISO 3166-1 alfa-2 utilizado no campo «Scheme territory» (cláusula 5.3.10);

— «:» = é usado como separador;

▼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

— As versões nas línguas nacionais dos Estados-Membros DEVERÃO ser cadeias de caracteres estruturadas como se segue:

CC:nome_valor

em que

— «CC» = o Código de País ISO 3166-1 alfa-2 utilizado no campo «Scheme territory» (cláusula 5.3.10);

— «:» = é usado como separador;

— «nome_valor» = Tradução oficial na língua nacional do atrás referido «EN_name_value».

A denominação do sistema é obrigatória, para identificar de forma exclusiva, pelo nome, o sistema a que a «Scheme information URI» se refere, e também para garantir que, no caso de o operador do sistema gerir mais do que um sistema, foi dado a cada um deles um nome distinto.

Os Estados-Membros e os operadores de Sistema DEVERÃO assegurar-se de que, quando um Estado-Membro ou um Operador de Sistema gerem mais do que um sistema, foi dado a cada um deles um nome distinto.

Scheme information URI (cláusula 5.3.7)

Este campo é OBRIGATÓRIO e DEVERÁ especificar o(s) URI(s) onde os utilizadores (terceiros de confiança) podem obter informação específica sobre o sistema (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)). DEVERÁ ser uma sequência de apontadores multilingues (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)). O(s) URI(s) referenciados DEVEM disponibilizar um caminho para a informação que descreve a «informação adequada sobre o sistema».

A «informação adequada sobre o sistema» DEVERÁ incluir, no mínimo:

— Informações introdutórias gerais comuns a todos os Estados-Membros, no que se refere ao âmbito e aos antecedentes da Lista Aprovada e ao(s) sistema(s) subjacentes de controlo/acreditação. O texto comum a utilizar é o seguinte:

▼C2

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.

▼C1

— Informação específica sobre o(s) sistema(s) de controlo/acreditação subjacente, em especial ([1]):

— Informação sobre o sistema de controlo aplicável a todos os PSC_{QC};

([1]) Os dois últimos conjuntos de informação assumem uma importância fundamental para que os terceiros de confiança possam avaliar o nível de qualidade e de segurança destes sistemas de controlo/acreditação. Estes conjuntos de informação deverão ser fornecidos ao nível da LA enquanto estiver a ser utilizado o presente «Scheme information URI» (cláusula 5.3.7 – informação prestada pelo Estado-Membro), «Scheme type/community/ /rules» (cláusula 5.3.9 – através da utilização de um texto comum a todos os Estados-Membros) e «TSL policy/legal notice» (cláusula 5.3.11 – um texto comum a todos os Estados-Membros baseado na Directiva 1999/93/CE, conjugado com a capacidade dos Estados-Membros para acrescentarem texto/referências específicas de cada um). Se necessário e requerido, poderá ser prestada informação complementar sobre sistemas nacionais de controlo/acreditação para PSC que não emitam CQ ao nível de serviço (por exemplo, para distinguir vários níveis de qualidade/segurança), através do recurso ao «Scheme service definition URI» (cláusula 5.5.6)

▼C1

— Quando aplicável, informação sobre o sistema nacional de acreditação facultativa aplicável a todos os PSC_{QC};

— Quando aplicável, informação sobre o sistema de controlo aplicável a todos os PSC que não emitem CQ;

— Quando aplicável, informação sobre o regime nacional de acreditação facultativa aplicável a todos os PSC que não emitem CQ;

— Esta informação específica DEVERÁ incluir, relativamente a cada um dos sistemas subjacentes atrás enumerados, pelo menos o seguinte:

— Descrição geral;

— Informação sobre o processo adoptado pelo Organismo de Controlo/Acreditação para controlar/acreditar PSC e pelos PSC para serem controlados/acreditados;

— Informação sobre os critérios segundo os quais os PSC são controlados/acreditados.

— Quando aplicável, informação específica sobre as «qualificações» específicas que alguns dos objectos físicos ou binários (lógicos) gerados ou emitidos em resultado da prestação de um serviço de certificação podem ter direito a receber, com base no cumprimento das disposições e requisitos estabelecidos a nível nacional, incluindo o significado de tal «qualificação», e sobre as disposições e requisitos nacionais associados.

Informação complementar específica sobre e sistema do Estado-Membro PODE ser prestada facultativamente como aditamento. Essa informação DEVERÁ incluir:

— Informação sobre os critérios e as regras usados para seleccionar supervisores/auditores e para definir de que forma os PSC são supervisionados (controlados)/acreditados (auditados) por eles;

— Outros contactos e informações gerais referentes ao funcionamento do sistema.

Status determination approach (cláusula 5.3.8)

Este campo é OBRIGATÓRIO e DEVERÁ especificar o identificador da abordagem de determinação do estado. O seguinte URI específico DEVERÁ ser utilizado, tal como abaixo é registado e descrito:

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

Descrição: O estado dos serviços listados é determinado pelo Operador do Sistema ou por conta deste, segundo um sistema adequado, para um determinado Estado-Membro que preveja o «controlo» (e, quando aplicável, a «acreditação facultativa») dos prestadores de serviços de certificação estabelecidos no seu território (ou estabelecidos num país terceiro, no caso da «acreditação facultativa») e que emitem certificados qualificados destinados ao público, em conformidade com o artigo 3.º, n.º 3, (ou o artigo 3.º, n.º 2, ou o artigo 7.º, n.º 1, alínea a)) da Directiva 1999/93/CE do Parlamento Europeu e do Conselho, e que, quando aplicável, preveja o «controlo»/«acreditação facultativa» dos prestadores de serviços de certificação que não emitem certificados qualificados, em conformidade com um (ou mais) «sistema(s) de homologação reconhecido(s)» aplicado(s) a nível nacional para o controlo do cumprimento, por parte dos PSC que não emitem CQ, das disposições fixadas pela Directiva 1999/93/CE e eventualmente alargadas pelas disposições nacionais no que se refere à prestação desses serviços de certificação.

▼C1

Scheme type/community/rules (cláusula 5.3.9)

Este campo é OBRIGATÓRIO e DEVERÁ conter pelo menos as seguintes URI registadas:

— Uma URI comum às Listas Aprovadas de todos os Estados-Membros, apontando para um texto descritivo que DEVERÁ ser aplicável a todas as LA:

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

— Pela qual é anunciada a participação do sistema do Estado-Membro (identificada através dos campos «TSL type» (cláusula 5.3.3) e «Scheme name» (cláusula 5.3.6) num sistema de sistemas (ou seja, uma TSL que lista apontadores para todos os Estados-Membros que publicam e mantêm uma LA sob a forma de TSL);

— Na qual os utilizadores podem encontrar políticas/regras segundo as quais os serviços incluídos na lista DEVERÃO ser avaliados e a partir das quais pode ser determinado o tipo de TSL (ver cláusula 5.3.3);

— Na qual os utilizadores podem encontrar a descrição do modo de utilizar e interpretar o conteúdo da aplicação TSL da Lista Aprovada. Estas regras de utilização DEVERÃO ser comuns a todas as Listas Aprovadas dos Estados-Membros, independentemente do tipo de listado e seja(m) qual(is) for(em) o(s) sistema(s) de controlo/acreditação.

Texto descritivo:

▼C2

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.

▼C2

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/CE 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)

▼C2

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

Please refer to the Technical specifications for a Common Template for the ‘Trusted List of supervised/accredited Certification Service Providers’ in the Annex of Commission Decision 2009/767/CE for further details on the fields, description and meaning for the TSL implementation of the Member States’ Trusted Lists.

▼C1

— Um URI específico da Lista Aprovada de cada Estado-Membro, apontando para um texto descritivo que DEVERÁ ser aplicável à LA desse Estado-Membro:

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

onde «CC» = o Código de País ISO 3166-1 alfa-2 utilizado no campo «Scheme territory» (cláusula 5.3.10);

— No qual os utilizadores podem encontrar a política/regras específicas do Estado-Membro referenciado, segundo as quais os serviços incluídos na lista DEVERÃO ser avaliados, dando cumprimento ao sistema adequado de controlo do Estado-Membro e aos sistemas de acreditação facultativa.

— No qual os utilizadores podem encontrar uma descrição específica do Estado-Membro referenciado sobre o modo de utilizar e interpretar o conteúdo da aplicação TSL da Lista Aprovada, no que se refere à certificação de serviços não relacionados com a emissão de CQ. Esse URI pode ser usado para indicar uma hipotética granularidade nos sistemas nacionais de controlo/acreditação em relação aos PSC que não emitem CQ, e o modo como para isso são usados o «Scheme service definition URI» (cláusula 5.5.6) e o campo «Service information extension».

Os Estados-Membros PODEM definir URI(s) adicional(is) a partir do atrás referido URI específico de cada Estado-Membro (ou seja, URI(s) definido(s) a partir desse URI hierárquico específico).

Scheme territory (cláusula 5.3.10)

No âmbito das presentes especificações, este campo é OBRIGATÓRIO e DEVERÁ especificar o país onde o sistema está estabelecido (Código de País ISO 3166-1 alfa-2).

TSL policy/legal notice (cláusula 5.3.11)

No âmbito das presentes especificações, este campo é OBRIGATÓRIO e DEVERÁ especificar a política do sistema ou apresentar um aviso legal sobre o estatuto jurídico do sistema ou os requisitos legais cumpridos pelo sistema relativamente à jurisdição em que o sistema é estabelecido e/ou quaisquer limitações e condições a que a manutenção e publicação da LA esteja sujeita.

Este campo DEVERÁ ser uma cadeia de caracteres multilingue (texto não encriptado) composta por duas partes:

— A primeira parte, obrigatória, comum às LA de todos os Estados-Membros (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)), indicando que o quadro jurídico aplicável é a Directiva 1999/93/CE e a sua correspondente aplicação na legislação do Estado-Membro indicado no campo «Scheme Territory».

Versão inglesa do texto comum:

«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

Texto na(s) língua(s) nacional(is) de um Estado-Membro: [tradução (traduções) oficial(is) do texto inglês atrás apresentado].

— A segunda parte, facultativa, exclusiva de cada LA (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)), apresentando referências aos quadros jurídicos nacionais aplicáveis (por exemplo, em especial no que se refere aos sistemas nacionais de controlo/acreditação de PSC que não emitem CQ).

Historical information period (cláusula 5.3.12)

Este campo é OBRIGATÓRIO e DEVERÁ especificar a duração (número inteiro) do período sobre o qual é fornecida informação histórica na TSL. Este valor de número inteiro deve ser apresentado em número de dias e, no âmbito das presentes especificações, DEVERÁ ser superior ou igual a 3 653 (ou seja, isto significa que a aplicação TSL das LA dos Estados-Membros DEVE conter informação histórica sobre um mínimo de dez anos). Os valores superiores deveriam ter devidamente em conta os requisitos jurídicos em matéria de retenção de dados no Estado-Membro indicado no «Scheme Territory» (cláusula 5.3.10).

Pointers to other TSLs (cláusula 5.3.13)

No âmbito das presentes especificações, este campo é OBRIGATÓRIO e, sempre que este estiver disponível, DEVERÁ incluir o apontador para um formulário compatível ETSI TS 102 231 da lista, compilada pela CE, de ligações (apontadores) para todas as aplicações TSL das Listas Aprovadas dos Estados-Membros. Deverão ser aplicadas as especificações da ETSI TS 102 231, cláusula 5.3.13, na indicação da utilização da identidade digital facultativa, que representa o emissor da TSL para o qual se aponta, formatado de acordo com a cláusula 5.5.3.

Nota: Este campo NÃO DEVERÁ ser utilizado, enquanto se estiver a aguardar a lista, compilada pela CE, das ligações para as aplicações TSL das LA dos Estados-Membros compatíveis com a ETSI TS 102 23.

List issue date and time (cláusula 5.3.14)

Este campo é OBRIGATÓRIO e DEVERÁ especificar a data e a hora (UTC [tempo universal coordenado] expresso em [hora] Zulu) em que a TSL foi emitida, utilizando o valor de data e hora tal como especificado na ETSI TS 102 231, cláusula 5.1.4.

Next update (cláusula 5.3.15)

Este campo é OBRIGATÓRIO e DEVERÁ especificar a data e a hora limites (UTC [tempo universal coordenado] expresso em [hora] Zulu) em que a próxima TSL será emitida — ou anulada, para indicar uma TSL fechada (utilizando o valor de data e hora tal como especificado na ETSI TS 102 231, cláusula 5.1.4).

No caso de não haver alterações ao estado provisório de qualquer TSP ou serviço abrangido pelo sistema, a TSL DEVE ser reemitida até à hora a que expirar a última TSL emitida.

No âmbito das presentes especificações, a diferença entre a data e hora da «Next update» e a «List issue date and time» NÃO DEVERÁ exceder **seis (6)** meses.

▼C1

Distribution points (cláusula 5.3.16)

Este campo é FACULTATIVO. Se for utilizado, DEVERÁ especificar as localizações onde a aplicação TSL da LA actual está publicada e onde podem ser encontradas as actualizações da TSL existente. Se forem indicados pontos de distribuição múltiplos, todos eles DEVEM fornecer cópias idênticas da TSL existente ou da sua versão actualizada. Quando utilizado, este campo é formatado como uma sequência não vazia de cadeias (de caracteres), todas elas conformes com a RFC 3986 ([1]).

Scheme extensions (cláusula 5.3.17)

Este campo é FACULTATIVO e não é utilizado no âmbito destas especificações.

List of Trust Service Providers

Este campo é FACULTATIVO.

Este campo NÃO DEVERÁ estar presente, no caso de não haver nem ter havido nenhum PSC controlado/acreditado no âmbito do sistema, num Estado-Membro. No entanto, foi acordado que, mesmo quando um Estado-Membro não tiver nenhum PSC controlado nem acreditado no âmbito do sistema, os Estados-Membros DEVERÃO aplicar uma TSL com este campo ausente. A ausência de qualquer PSC na lista SIGNIFICARÁ que não há nenhum PSC controlado/acreditado no país especificado no campo «Scheme Territory».

No caso de um ou mais serviços de PSC serem ou terem sido controlados/acreditados pelo sistema, este campo DEVERÁ conter uma sequência que identifique cada PSC que preste um ou mais desses serviços controlados/acreditados, com pormenores sobre o estado de controlo/acreditação e o histórico do estado de cada serviço do PSC (TSP = PSC na Figura que se segue).

Lista de TSP

Informação sobre o TSP (TSP (1))
Informação sobre o Serviço (Serviço (1)-TSP(1))
Informação sobre o Histórico (Histórico(1) Serviço(1) TSP(1)
Informação sobre o Histórico (Histórico(2) Serviço(1) TSP(1)
Informação sobre o Histórico (Histórico[…] Serviço(1) TSP(1)
Informação sobre o Serviço (Serviço (2)-TSP(1))
Informação sobre o Histórico (Histórico(1) Serviço(2) TSP(1)
Informação sobre o Histórico (Histórico(2) Serviço(2) TSP(1)
Informação sobre o Histórico (Histórico[…] Serviço(2) TSP(1)
Informação sobre o Serviço (Serviço […]-TSP(1))
Informação sobre o Histórico (Histórico(1) Serviço[…] TSP(1)
Informação sobre o Histórico (Histórico(2) Serviço[…] TSP(1)
Informação sobre o Histórico (Histórico[…] Serviço[…] TSP(1)
Informação sobre o TSP (TSP (2))
Lista de Serviços do TSP(2) e lista de informação histórica por Serviço
Informação sobre o TSP (TSP […])
Lista de Serviços do TSP[…] e lista de informação histórica por Serviço

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

▼C1

A lista dos TSP é organizada como indicado na Figura anterior. Para cada TSP, há uma sequência de campos contendo informação sobre esse TSP («TSP Information»), seguida por uma lista de Serviços. Para cada um dos Serviços assim listados, há uma sequência de campos contendo informação sobre esse Serviço («Service Information»), e uma sequência de campos sobre o histórico do estado de aprovação do Serviço («Service approval history»).

TSP Information

TSP(1)

TSP name (cláusula 5.4.1)

Este campo é OBRIGATÓRIO e DEVERÁ especificar a denominação da **entidade jurídica** responsável pelos serviços dos PSC que são ou foram controlados ou acreditados no âmbito do sistema. É composto por uma sequência de cadeias de caracteres multilingues (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)). Esta denominação DEVE ser a denominação utilizada nos registos legais formais e à qual deve ser dirigida qualquer comunicação formal.

TSP trade name (cláusula 5.4.2)

Este campo é FACULTATIVO e, quando presente, DEVERÁ especificar uma designação alternativa com a qual o PSC se identifica, no quadro específico dos serviços por si prestados e que figurem nesta TSL sob a entrada «TSP name» (cláusula 5.4.1).

Nota: Quando uma única entidade jurídica PSC presta serviços sob denominações comerciais diferentes ou em âmbitos específicos diferentes, poderá haver tantas entradas relativas a esse PCS quantos os âmbitos específicos (por exemplo, entradas Denominação/Denominação comercial). Uma alternativa consiste em listar todos e quaisquer PSC (entidade jurídica) apenas uma vez e fornecer informação específica sobre o âmbito do Serviço. Cabe ao Operador do Sistema do Estado-Membro debater e acordar com o PSC qual a abordagem mais apropriada.

TSP address (cláusula 5.4.3)

Este campo é OBRIGATÓRIO e DEVERÁ especificar o endereço da entidade jurídica ou da organização mandatada identificada no campo «TSP name» (cláusula 5.4.1), tanto para comunicações postais como para comunicações electrónicas. DEVERÁ incluir o «PostalAddress» (ou seja, nome da rua, localidade, [estado ou província], [código postal] e código para a representação do nome do país ISO 3166-1 alfa-2), em conformidade com a cláusula 5.3.5.1; e o «ElectronicAddress» (ou seja, endereço de correio electrónico e/ou URI do sítio Web), em conformidade com a cláusula 5.3.5.2.

TSP information URI (cláusula 5.4.4)

Este campo é OBRIGATÓRIO e DEVERÁ especificar o(s) URI(s) onde os utilizadores (por exemplo, terceiros de confiança) podem obter informação específica sobre o PSC. DEVERÁ ser uma sequência de apontadores multilingues (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)). O(s) URI(s) referenciado(s) DEVE(M) indicar um caminho para a informação que descreve os termos e condições gerais do PSC, as suas práticas, questões jurídicas, as suas políticas de assistência a clientes e outras informações de carácter geral aplicáveis a todos os serviços enumerados sob a entrada desse PSC na TSL.

Nota: Quando uma única entidade jurídica PSC prestar serviços sob denominações comerciais diferentes ou em âmbitos específicos diferentes, e esse facto se reflectir em tantas entradas TSP quantos os âmbitos específicos, este campo DEVERÁ especificar a informação relativa ao conjunto específico de serviços listados sob uma entrada exclusiva TSP/Denominação comercial da entidade.

▼C1

TSP information extensions (cláusula 5.4.5)

Este campo é FACULTATIVO e, quando presente, PODE ser usado pelo operador de sistema para, dando cumprimento às especificações da ETSI TS 102 231 (cláusula 5.4.5), fornecer informação específica, a ser interpretada de acordo com as regras do sistema específico.

List of Services

Este campo é OBRIGATÓRIO e DEVERÁ conter uma sequência que identifique cada um dos serviços reconhecidos do PSC e o estado de aprovação (e o histórico desse estado) desse mesmo serviço. Deve ser indicado pelo menos um serviço (mesmo que a informação existente seja inteiramente histórica).

Uma vez que a preservação da informação sobre o histórico dos serviços listados é OBRIGATÓRIA no âmbito das presentes especificações, essa informação histórica DEVE ser preservada mesmo quando o estado actual do serviço não requeira que este seja listado (por exemplo, o serviço foi retirado). Portanto, DEVE ser incluído um PSC mesmo quando o seu único serviço listado estiver nesse estado, de modo a preservar o histórico.

Service Information

TSP(1) Service(1)

Service type identifier (cláusula 5.5.1)

▼M1

Este campo é OBRIGATÓRIO e DEVERÁ especificar o identificador do tipo de serviço de acordo com o tipo das presentes especificações TSL (ou seja, «/eSigDir-1999-93-EC-TrustedList/TSLtype/generic»).

▼C1

Quando o serviço listado diz respeito à emissão de Certificados Qualificados, o URI citado DEVERÁ ser http://uri.etsi.org/TrstSvc/Svctype/CA/QC (uma Autoridade de Certificação que emite Certificados Qualificados).

Quando o serviço listado diz respeito è emissão de Tokens de Serviço de Confiança que não sejam CQ e que não suportem a emissão de CQ, o URI citado DEVERÁ ser um dos URI(s) definidos na ETSI 102 231 e listados na sua cláusula D.2, relacionados com este campo. Isto SERÁ válido mesmo para os Tokens de Serviço de Confiança que são controlados/acreditados para satisfazer algumas qualificações específicas, em conformidade com as leis nacionais dos Estados-Membros (por exemplo, o chamado «Token» de Data/Hora Qualificado da Alemanha e da Hungria), o URI citado DEVERÁ ser um dos URI(s) definidos na ETSI 102 231 e listados na sua cláusula D.2, relacionados com este campo (por exemplo, TSA para os «Tokens» de Validação Cronológica Qualificados definidos a nível nacional). Quando aplicável, essa qualificação específica nacional dos «Tokens» de Serviço de Confiança PODE ser apresentada na entrada do serviço; a extensão additionalServiceInformation (cláusula 5.8.2) na cláusula 5.5.9 («Service information extension») DEVERÁ ser utilizada para este fim.

▼C1

Como princípio geral por defeito, HAVERÁ uma entrada por cada certificado X.509v3 (por exemplo, para um serviço de certificação de tipo AC/CQ) dentro do grupo de serviços de certificação de um PSC incluído na Lista Autorizada (por exemplo, uma Autoridade de Certificação que emite (directamente) CQ). Em algumas situações cuidadosamente ponderadas e em condições autorizadas e geridas com critério, o Organismo de Controlo/Organismo de Acreditação de um Estado-Membro PODE decidir utilizar o certificado X.509v3 de uma Root AC ou de uma AC de nível superior (por exemplo, uma Autoridade de Certificação que não emite directamente CQ para entidades finais mas que certifica uma hierarquia de AC até ao nível das AC que emitem CQ para entidades finais) como «Sdi» de uma única entrada na lista de serviços de um PSC listado. As consequências (vantagens e desvantagens) de usar esse certificado X.509v3 de uma Root AC ou AC de nível superior como valor do «Sdi» das entradas de serviços de LA deve ser cuidadosamente analisada e aprovada pelos Estados-Membros ([1]). Além disso, quando utiliza esta excepção autorizada ao princípio por defeito, o Estado-Membro DEVE fornecer a documentação necessária para facilitar a construção do caminho de certificação e verificação.

Nota: Os TSP, como respondedores do Protocolo OCSP e Emissores de CRL que fazem parte dos serviços de certificação dos PSC_{QC}, e que estão dependentes do uso de pares de chaves distintos, respectivamente para assinar respostas do Protocolo OCSP e CRL(s), PODEM também ser incluídos no presente modelo TSL, utilizando a seguinte combinação de URI(s):

— Valor «Service type identifier» (cláusula 5.5.1):

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

combinado com o valor da seguinte «Service information extension» (cláusula 5.5.9) extensão additionalServiceInformation (cláusula 5.8.2):

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

Descrição: entidade prestadora de informação sobre o estado do certificado que opera um servidor OCSP como parte de um serviço de um PSC que emite Certificados Qualificados.

— Valor «Service type identifier» (cláusula 5.5.1):

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

combinado com o valor da seguinte «Service information extension» (cláusula 5.5.9) extensão additionalServiceInformation (cláusula 5.8.2):

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

Descrição: entidade prestadora de informação sobre o estado do certificado e que opera uma CRL como parte de um serviço de um PSC que emite Certificados Qualificados.

— Valor «Service type identifier» (cláusula 5.5.1):

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

([1]) A utilização de um certificado Root CA X.509v3 como valor «Sdi» para um serviço incluído numa lista vai obrigar o Operador de Sistema a ter em conta o conjunto de serviços de certificação abrangidos por essa Root CA no seu todo, no que se refere ao «estado de controlo/acreditação». P. ex., qualquer modificação do estado requerida por uma AC incluída na hierarquia de raiz vai obrigar toda a hierarquia a assumir essa modificação de estado.

▼C1

combinado com o valor da seguinte «Service information extension» (cláusula 5.5.9) extensão additionalServiceInformation (cláusula 5.8.2):

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

Descrição: Autoridade de Certificação de Raiz a partir da qual pode ser estabelecido um caminho de certificação até uma Autoridade de Certificação que emite Certificados Qualificados.

— Valor «Service type identifier» (cláusula 5.5.1):

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

combinado com o valor da seguinte «Service information extension» (cláusula 5.5.9) extensão additionalServiceInformation (cláusula 5.8.2):

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

Descrição: serviço de validação cronológica como parte de um serviço de um prestador de serviços de certificação emissor de Certificados Qualificados que emita TST que podem ser utilizados no processo de verificação de assinaturas qualificadas, para determinar e alargar a validade da assinatura quando o CQ é revogado ou expira.

Service name (cláusula 5.5.2)

Este campo é OBRIGATÓRIO e DEVERÁ especificar a denominação sob a qual o PSC identificado em «TSP name» (cláusula 5.4.1) presta o serviço identificado em «Service type identifier» (cláusula 5.5.1). DEVERÁ ser uma sequência de cadeias de caracteres multilingues (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)).

Service digital identity (cláusula 5.5.3)

Este campo é OBRIGATÓRIO e DEVERÁ especificar pelo menos uma representação de um identificador digital exclusivo do serviço cujo tipo é especificado em «Service type identifier» (cláusula 5.5.1) e pelo qual o serviço pode ser inequivocamente identificado.

Nas presentes especificações, o identificador digital utilizado neste campo DEVERÁ ser o Certificado X.509v3 relevante, que é uma representação da(s) chave(s) pública(s) que o PSC utiliza para prestar o serviço cujo tipo é especificado pelo «Service type identifier» (cláusula 5.5.1) (ou seja, a chave utilizada pela RootAC/CQ, a chave utilizada para assinar certificados [1] ou, em alternativa, emitir «Tokens» de Validação Cronológica ou assinar CRL(s) ou assinar as respostas do Protocolo OCSP). Este Certificado X.509v3 associado DEVERÁ ser utilizado como o identificador digital mínimo requerido (pois é uma representação da(s) chave(s) pública(s) que o PSC utiliza para prestar o serviço listado). PODEM ser utilizados identificadores adicionais como adiante se indica mas todos eles DEVEM referir-se à mesma identidade (ou seja, ao Certificado X.509v3 associado):

[1] Isto poderá ser o certificado de uma AC emissora de certificados de entidade final (p. ex. AC/PKC, AC/CQ) ou o certificado de uma Root CA autorizada a partir da qual se possa traçar o caminho até aos certificados de entidade final qualificados. Consoante se possa ou não utilizar esta informação e a informação disponível em qualquer certificado de entidade final emitido no âmbito desta raiz autorizada para determinar, de forma indiscutível, as características adequadas de qualquer certificado qualificado, esta informação («Service digital identity») poderá necessitar de ser complementada por dados de «Service information extensions» (ver cláusula 5.5.9).

▼C1

a) O nome distinto (DN) do certificado, que pode ser utilizado para verificar assinaturas electrónicas do serviço do PSC especificado em «Service type identifier» (cláusula 5.5.1);

b) O identificador de chave pública associado (ou seja, X.509v3 SubjectKeyIdentifier ou valor do SKI);

c) A chave pública associada.

Como princípio geral por defeito, o identificador digital (ou seja, o certificado X.509v3 associado) NÃO DEVERÁ estar presente mais de uma vez na Lista Autorizada, ou seja, HAVERÁ só uma entrada por cada certificado X.509v3 para um serviço de certificação englobado nos serviços de certificação enumerados de um PSC incluído na Lista Autorizada. Reciprocamente, DEVERÁ ser utilizado um único certificado X.509v3 como valor do «Sdi» numa única entrada de serviço.

Nota (1): O único caso relativamente ao qual o atrás referido princípio geral por defeito pode não ser aplicado é a situação em que um certificado X.509v3 único é utilizado para emitir tipos diferentes de «Tokens» de Serviços de Confiança aos quais se aplicam sistemas diferentes de controlo/acreditação; por exemplo: um PSC utiliza um único certificado X.509v3, por um lado, para emitir CQ no âmbito de um sistema adequado de controlo e, por outro lado, para emitir certificados não qualificados com um estatuto diferente de controlo/acreditação. Neste caso e exemplo, seriam utilizadas duas entradas com valores de «Sti» diferentes (por exemplo, AC/CQ e AC/PKC, respectivamente, no exemplo apresentado) e com o mesmo valor de «Sdi» (o certificado X.509v3 associado).

As aplicações serão de tipo ASN.1 ou XML e DEVERÃO ser conformes com as especificações da ETSI TS 102 231 (quanto ao ASN.1 ver anexo A da ETSI TS 102 231 e quanto ao XML ver anexo B da ETSI TS 102 231).

Nota (2): Quando for preciso fornecer informação complementar sobre «qualificação» no que se refere à entrada de serviço identificada, o Operador do Sistema DEVERÁ, quando apropriado, ponderar a utilização da extensão «additionalServiceInformation» (cláusula 5.8.2) do campo «Service information extension» (cláusula 5.5.9) de acordo com a finalidade da prestação dessa informação complementar sobre «qualificação». Além disso, o Operador do Sistema pode, a título facultativo, utilizar a cláusula 5.5.6 («Scheme service definition URI»).

Service current status (cláusula 5.5.4)

Este campo é OBRIGATÓRIO e DEVERÁ especificar o identificador do estado do serviço através de um dos seguintes URI(s):

▼C2

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

— **Supervision of Service in Cessation (Supervisão do Serviço em Cessação)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

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

— **Supervision Revoked (Supervisão Revogada)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

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

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

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

▼C1

No quadro das presentes especificações da Lista Aprovada, os estados atrás referidos DEVERÃO ser interpretados como se segue:

— ***Sob Supervisão:*** O serviço identificado em «Service digital identity» (cláusula 5.5.3) prestado pelo Prestador de Serviços de Certificação (PSC) identificado em «TSP name» (cláusula 5.4.1) está presentemente a ser controlado, relativamente ao cumprimento das disposições estabelecidas pela Directiva 1999/93/CE, pelo Estado-Membro identificado em «Scheme territory» (cláusula 5.3.10) no qual o PSC está estabelecido.

▼M1

— ***Supervisão de Serviço em Cessação.:*** O serviço identificado em «Service digital identity» (cláusula 5.5.3) prestado pelo PSC identificado em «TSP name» (cláusula 5.4.1) encontra-se em fase de cessação mas continua sujeito a controlo até a supervisão cessar ou ser revogada. No caso de uma pessoa colectiva que não a identificada em «TSP name» ter assumido a responsabilidade de assegurar esta fase de cessação, a identificação dessa nova pessoa colectiva ou dessa pessoa colectiva de recurso (PSC de recurso) DEVERÁ ser apresentada em «Scheme service definition URI» (cláusula 5.5.6) e em «TakenOverBy» (cláusula L.3.2), na entrada de serviço.

▼C1

— ***Supervisão Cessada:*** A validade da avaliação de controlo expirou sem que o serviço identificado em «Service digital identity» (cláusula 5.5.3) tivesse sido reavaliado. Presentemente, o serviço já não se encontra sob supervisão, a partir da data do estado actual, visto que se entende que o serviço deixou de ser prestado.

— ***Supervisão Revogada:*** Tendo sido anteriormente controlado, o serviço do PSC, e eventualmente o próprio PSC, deixou de cumprir as disposições estabelecidas pela Directiva 1999/93/CE, conforme foi determinado pelo Estado-Membro identificado em «Scheme territory» (cláusula 5.3.10) no qual o PSC está estabelecido. Por conseguinte, foi pedido ao serviço que cessasse a sua prestação e deve ser considerado como cessado pela razão anterior.

Nota (1): O valor do estado «Supervisão Revogada» pode ser um estado definitivo, mesmo que o PSC cesse por completo a sua actividade; neste caso, não há necessidade de migrar para o estado «Supervisão de Serviço em Cessação» ou para «Supervisão Cessada». Na verdade, a única maneira de alterar o estado «Supervisão Revogada» é passar do não cumprimento novamente para o cumprimento das disposições estabelecidas na Directiva 1999/93/CE, de acordo com o sistema de controlo adequado em vigor no Estado-Membro proprietário da LA, e recuperar o estado «Sob Supervisão». O estado «Supervisão de Serviço em Cessação» ou o estado de «Supervisão Cessada» só se verifica quando o PSC cessa directamente os seus serviços relacionados sob supervisão e não quando a supervisão foi revogada.

— ***Acreditado:*** O Organismo de Acreditação realizou, por conta do Estado-Membro identificado em «Scheme territory» (cláusula 5.3.10), uma avaliação de acreditação, tendo concluído que o serviço identificado em «Service digital identity» (cláusula 5.5.3) prestado pelo PSC ([1]) identificado em «TSP name» (cláusula 5.4.1) cumpria as disposições estabelecidas pela Directiva 1999/93/CE.

([1]) De assinalar que o PSC acreditado pode estar estabelecido num Estado-Membro diferente do EM identificado no «Scheme territory» da aplicação da TSL da LA, ou num país terceiro (ver artigo 7.º, n.º 1, alínea a), da Directiva 1999/93/CE).

▼C1

Nota (2): Quando aplicados ao caso de um PSC emissor de CQ(s), que se encontra estabelecido no «Scheme territory» (cláusula 5.3.10), os dois estados que se seguem — «Acreditação Revogada» e «Acreditação Cessada» — DEVEM ser considerados como «estados transitórios» e NÃO DEVEM ser utilizados como valor para o «Service current status» [estado actual do serviço], visto que, no caso de o serem, DEVEM ser imediatamente seguidos no «Service approval history information» [informação sobre o histórico de aprovação do serviço] ou no «Service current status» por um estado de «Sob supervisão», ao qual se poderá seguir qualquer outro estado de supervisão atrás definido e conforme ilustrado na Figura 1. Quando aplicados ao caso de um PSC que não emite CQ(s) e quando existe apenas um sistema associado de «acreditação voluntária», que não tem associado nenhum sistema de controlo, ou no caso de um PSC emissor de CQ(s) mas que não se encontra estabelecido no «Scheme territory» (cláusula 5.3.10) (por exemplo, num país terceiro), os estados de «Acreditação Revogada» e «Acreditação Cessada» PODEM ser utilizados como um valor para o «Service current status»:

— ***Acreditação Cessada:*** A validade da avaliação de acreditação expirou sem que o serviço identificado em «Service digital identity» (cláusula 5.5.3) tivesse sido reavaliado.

— ***Acreditação Revogada:*** Tendo sido anteriormente considerado conforme com os critérios do sistema, o serviço identificado em «Service digital identity» (cláusula 5.5.3) prestado pelo Prestador de Serviços de Certificação (PSC) identificado em «TSP name» (cláusula 5.4.1) e, eventualmente, o próprio PSC, deixou de cumprir as disposições estabelecidas pela Directiva 1999/93/CE.

Nota (3): Devem ser utilizados valores de estado exactamente iguais para os PSC que emitem CQ e para os PSC que não emitem CQ (por exemplo, Prestadores de Serviços de Validação Cronológica que emitem TST, PSC que emitem certificados não qualificados, etc.). O «Service Type identifier» (cláusula 5.5.1) deverá ser utilizado para fazer a distinção entre os sistemas aplicáveis de controlo/acreditação.

Nota (4): A informação complementar sobre «qualificação» relacionada com o estado, definida ao nível dos sistemas nacionais de controlo/acreditação de PSC que não emitem CQ, PODE ser fornecida a nível do serviço, quando tal for aplicável e requerido (por exemplo, para distinguir entre vários níveis de qualidade/segurança). Os Operadores do Sistema DEVERÃO utilizar a extensão «additionalServiceInformation» (cláusula 5.8.2) do campo «Service information extension» (cláusula 5.5.9) de acordo com a finalidade de fornecer essa informação complementar sobre «qualificação». Além disso, o Operador do Sistema pode, a título facultativo utilizar a cláusula 5.5.6 («Scheme service definition URI»).

Current status starting date and time (cláusula 5.5.5)

Este campo é OBRIGATÓRIO e DEVERÁ especificar a data e a hora em que o estado actual de aprovação passou a vigorar (valor de data e hora como definido na ETSI TS 102 231, cláusula 5.1.4).

Scheme service definition URI (cláusula 5.5.6)

Este campo é FACULTATIVO e, quando presente, DEVERÁ especificar o(s) URI(s) onde os terceiros de confiança podem obter informação específica fornecida pelo Operador do Sistema como uma sequência de apontadores multilingues (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)).

Quando utilizado, o(s) URI(s) referenciados DEVEM disponibilizar um caminho para a informação que descreve o serviço tal como especificado pelo sistema. Em especial, esse caminho PODE incluir, quando aplicável:

a) O URI que indique a identidade do PSC de recurso, no caso de supervisão de um serviço em cessação envolvendo um PSC de recurso (ver «Service current status» – cláusula 5.5.4);

▼C1

b) O URI que conduza a documentos que forneçam informação complementar relacionada com a utilização de qualquer qualificação específica, definida a nível nacional, para um serviço controlado/acreditado que forneça «Tokens» de Serviço de Confiança, conforme com a utilização do campo «Service information extension» (cláusula 5.5.9) com uma extensão «additionalServiceInformation», como definido na cláusula 5.8.2.

Service supply points (cláusula 5.5.7)

Este campo é FACULTATIVO e, quando presente, DEVERÁ especificar o(s) URI(s) onde os terceiros de confiança podem aceder ao serviço através de uma sequência de cadeias de caracteres cuja sintaxe DEVE ser conforme com a RFC 3986.

TSP service definition URI (cláusula 5.5.8)

Este campo é FACULTATIVO e, quando presente, DEVERÁ especificar o(s) URI(s) onde os terceiros de confiança podem obter informação específica sobre o serviço fornecida pelo TSP como uma sequência de apontadores multilingues (com o EN como língua obrigatória e eventualmente com uma ou mais língua(s) nacional(is)). O(s) URI(s) referenciados DEVEM disponibilizar um caminho para a informação que descreva o serviço tal como especificado pelo TSP.

Service information extensions (cláusula 5.5.9)

No quadro das presentes especificações, este campo é FACULTATIVO mas DEVERÁ estar presente quando a informação fornecida em «Service digital identity» (cláusula 5.5.3) não for suficiente para identificar inequivocamente os certificados qualificados emitidos por este serviço e/ou a informação presente nos certificados qualificados em questão não permita uma identificação processável por computador dos factos sobre se o CQ é ou não suportado por um SSCD ([1]).

No quadro das presentes especificações, quando for REQUERIDO, por exemplo para os serviços AC/CQ, DEVERÁ ser utilizado e estruturado um campo de informação facultativo «Service information extensions» («Sie»), conforme com a extensão «Qualificações» definida no anexo L.3.1 da ETSI TS 102 231, como uma sequência de um ou mais tuplos, cada um dos quais fornecendo:

— (filtros) Informação a utilizar para identificar a nível superior, no âmbito do serviço de certificação identificado pelo «Sdi», o serviço específico (ou seja, um conjunto de certificados qualificados) em relação ao qual é requerida/fornecida informação complementar no que se refere à presença ou ausência de SSCD de suporte (e/ou emissão para uma Pessoa Colectiva); e

— A informação associada («qualificadores») sobre se o conjunto de certificados qualificados emitidos por este serviço, identificado a um nível superior, é ou não suportado por um SSCD (quando esta informação é «QCSSCDStatusAsInCert», isso significa que esta informação associada está incluída no CQ num formulário ETSI normalizado processável por computador ([2]) e/ou informação referente ao facto de esses CQ serem emitidos para Pessoas Colectivas (por defeito, estes devem ser considerados como tendo sido emitidos apenas para Pessoas Singulares).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): significa que é garantido pelo PSC e controlado (modelo supervisão) ou auditado (modelo acreditação) pelo Estado-Membro (respectivamente pelo seu Organismo de Controlo ou Organismo de Acreditação) que qualquer CQ, emitido no âmbito do serviço (QCA) identificado em «Service digital identity» (cláusula 5.5.3) e identificado a nível superior pela atrás referida informação (filtros) e utilizado para identificar a nível superior o serviço de certificação identificado pelo «Sdi», que o conjunto exacto de certificados qualificados para os quais é pedida esta informação complementar sobre a presença ou ausência de um SSCD de suporte **SÃO** suportados por um SSCD (ou seja, que a chave privada associada com a chave pública contida no certificado está guardada num Dispositivo Seguro de Criação da Assinaturas conforme com o anexo III da Directiva 1999/93/CE);

([1]) Ver secção 2.2 do presente documento.

([2]) Isto refere-se a uma conjugação adequada da declaração de QcCompliance definida pelo ETSI, declarações QcSSCD [ETSI TS 101 862] ou um OID definido por QCP/QCP + ETSI [ETSI TS 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD): significa que é garantido pelo PSC e controlado (modelo supervisão) ou auditado (modelo acreditação) pelo Estado-Membro (respectivamente pelo seu Organismo de Controlo ou Organismo de Acreditação) que qualquer CQ emitido no quadro do serviço (RootAC/CA ou AC/CQ) identificado em «Service digital identity» (cláusula 5.5.3) e identificado a nível superior pela informação anterior (filtros) utilizada para identificar a nível superior o serviço de certificação identificado pelo «Sdi», que o conjunto exacto de certificados qualificados para os quais é requerida esta informação complementar sobre a presença ou ausência de um SSCD de suporte **NÃO SÃO** suportados por um SSCD (ou seja, que a chave privada associada com a chave pública contida no certificado **não** está guardada num Dispositivo Seguro de Criação de Assinaturas conforme com o anexo III da Directiva 1999/93/CE).

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): significa que é garantido pelo PSC e controlado (modelo supervisão) ou auditado (modelo acreditação) pelo Estado-Membro (respectivamente pelo seu Organismo de Controlo ou Organismo de Acreditação) que qualquer CQ emitido pelo serviço (AC/CQ) identificado em «Service digital identity» (cláusula 5.5.3) e identificado a nível superior pela informação anterior (filtros) utilizada para identificar a nível superior o serviço de certificação identificado pelo «Sdi» que o conjunto exacto de certificados qualificados para os quais é requerida esta informação complementar sobre a presença ou ausência de um SSCD de suporte DEVERÃO conter informação processável por computador sobre se o CQ é ou não suportado por um SSCD;

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): significa que é garantido pelo PSC e controlado (modelo supervisão) ou auditado (modelo acreditação) pelo Estado-Membro (respectivamente pelo seu Organismo de Controlo ou Organismo de Acreditação) que qualquer CQ emitido pelo serviço (QCA) identificado em «Service digital identity» (cláusula 5.5.3) e identificado a nível superior pela informação anterior (filtros) utilizada para identificar a nível superior o serviço de certificação identificado pelo «Sdi» que o conjunto exacto de certificados qualificados para os quais é requerida esta informação complementar sobre a emissão para Pessoas Colectivas **SÃO** emitidos para Pessoas Colectivas.

Estes qualificadores só devem ser utilizados como uma extensão se o tipo de serviço for http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Este campo é específico da aplicação (ASN.1 ou XML) e DEVE ser conforme com as especificações fornecidas na ETSI TS 102 231, Anexo L.3.1.

▼M1

Nos casos de aplicação em XML, o conteúdo específico dessa informação complementar tem de ser codificado utilizando o ficheiro xsd fornecido no anexo C da ETSI TS 102231.

▼C1

Service Approval History

Este campo é FACULTATIVO mas DEVE estar presente se o valor de «Historical information period» (cláusula 5.3.12) for diferente de zero. Por conseguinte, no âmbito das presentes especificações, o sistema DEVE manter informação histórica. No caso de a informação histórica se destinar a ser mantida mas o serviço não tiver histórico anterior ao estado actual (ou seja, no caso do registo de um primeiro estado ou de o operador do sistema não ter conservado o histórico) este campo DEVERÁ ficar vazio. Caso contrário, por cada alteração do estado actual do serviço do TSP verificada dentro do período de informação histórica, especificado na ETSI TS 102 231 cláusula 5.3.12, a informação sobre o estado de aprovação anterior DEVERÁ ser fornecida por ordem decrescente da data e hora da alteração de estado (ou seja, a data e a hora em que o estado de aprovação seguinte passou a ser efectivo).

▼C1

Essa informação DEVERÁ ser uma sequência de informação histórica como se define adiante.

Histórico(1) do Serviço(1) do TSP(1)

Service type identifier (cláusula 5.6.1)

Este campo é OBRIGATÓRIO e DEVERÁ especificar o identificador do tipo de serviço, com o formato e o significado utilizados em «TSP Service Information – Service type identifier» (cláusula 5.5.1).

Service name (cláusula 5.6.2)

Este campo é OBRIGATÓRIO e DEVERÁ especificar a denominação sob a qual o PSC prestava o serviço identificado em «TSP Service Information – Service type identifier» (cláusula 5.5.1), com o formato e o significado utilizados em «TSP Service Information – Service name» (cláusula 5.5.2). Esta cláusula não exige que o nome seja o mesmo nome especificado na cláusula 5.5.2. Uma alteração de nome PODE ser uma das circunstâncias que exigem um novo estado.

▼M1

Service digital identity (cláusula 5.6.3)

Este campo é OBRIGATÓRIO e DEVERÁ especificar pelo menos uma representação do identificador digital (ou seja, o certificado X.509v3) utilizado em «TSP Service Information — Service digital identity» (cláusula 5.5.3), com o formato e o significado definidos na ETSI TS 102231, cláusula 5.5.3.

Nota: Para cada valor de um certificado X.509v3 que seja utilizado no campo «Sdi» (cláusula 5.5.3) de um serviço, deve haver apenas uma única entrada de serviço numa lista aprovada por cada valor de «Sti:Sie/additionalServiceInformation». As informações do campo «Sdi» (cláusula 5.6.3) utilizadas no histórico do estado de aprovação do Serviço associadas a uma entrada de serviço e as informações do campo «Sdi» (cláusula 5.5.3) utilizadas nesta entrada de serviço DEVEM referir-se ao mesmo valor do certificado X.509v3. Quando um serviço constante da lista altera o seu «Sdi» (ou seja, renova ou reintroduz um certificado X.509v3, por exemplo respeitante a um AC/PKC ou AC/CQ) ou cria um novo «Sdi» para um desses serviços, mesmo que os valores associados de «Sti», «Sn» e [«Sie»] se mantenham idênticos, o operador do Sistema DEVE criar uma entrada de serviço diferente da anterior.

▼C1

Service previous status (cláusula 5.6.4)

Este campo é OBRIGATÓRIO e DEVERÁ especificar o identificador do estado anterior do serviço, com o formato e o significado utilizados em «TSP Service Information – Service current status» (cláusula 5.5.4).

Previous status starting date and time (cláusula 5.6.5)

Este campo é OBRIGATÓRIO e DEVERÁ especificar a data e a hora em que o anterior estado de aprovação em questão passou a ser efectivo, com o formato e o significado utilizados em «TSP Service Information – Service current status starting date and time» (cláusula 5.5.5).

Service information extensions (cláusula 5.6.6)

Este campo é FACULTATIVO e PODE ser utilizado pelos operadores dos sistemas para fornecer informação específica relacionada com o serviço, com o formato e a acepção utilizados em «TSP Service Information – Service information extensions» (cláusula 5.5.9).

▼C2

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

Idem para TSP(1) Service(1) History(2) (antes do History 1)

…

TSP(1) Service(2)

Idem para TSP(1) Service 2 (se aplicável)

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

…

TSP(2) Information

Idem para TSP 2 (se aplicável)

Idem para TSP 2 Service 1

Idem para TSP 2 Service 1 History 1.

▼M1

Signed TSL

A aplicação TSL da LA em formato legível pelos utilizadores, elaborada de acordo com as presentes especificações e, nomeadamente, com o capítulo IV, DEVE ser assinada pelo «Scheme Operator Name» (cláusula 5.3.4), para garantir a sua autenticidade e integridade ([1]). O formato da assinatura DEVE ser PAdES parte 3 (ETSI TS 102 778-3 ([2])), mas PODE ser PAdES parte 2 (ETSI TS 102 778-2 ([3])) no âmbito do modelo específico de confiança estabelecido pela publicação dos certificados utilizados para assinar as listas aprovadas.

A aplicação TSL da LA em formato que permita o tratamento por computador, elaborada segundo as presentes especificações, DEVERÁ ser assinada pelo «Scheme Operator Name» (cláusula 5.3.4), para garantir a sua autenticidade e integridade. O formato da aplicação TSL da LA para tratamento por computador, elaborada segundo as presentes especificações, DEVERÁ ser XML e DEVERÁ ser conforme com as especificações indicadas nos anexos b e C da ETSI TS 102 231.

O formato da assinatura DEVERÁ ser XAdES BES ou EPES, como definido pelas especificações da ETSI TS 101 903 para aplicações XML. Essa aplicação da assinatura electrónica DEVERÁ cumprir os requisitos definidos no anexo B da ETSI TS 102 231 ([4]). Os requisitos gerais adicionais relativos a esta assinatura são apresentados nas secções seguintes.

▼C1

Scheme identification (cláusula 5.7.2)

Este campo é OBRIGATÓRIO e DEVERÁ especificar uma referência atribuída pelo operador do sistema, que identifique de forma inequívoca o sistema descrito nas presentes especificações e a TSL elaborada, que DEVE ser incluída no cálculo da assinatura. Essa referência deverá ser uma cadeia de caracteres ou uma cadeia de bits.

([1]) Caso a aplicação TSL da LA em formato legível pelos utilizadores não seja assinada, a sua autenticidade e integridade DEVEM ser garantidas através de um meio de comunicação apropriado, com um nível de segurança equivalente. A utilização de TSL (*IETF RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2*) é recomendada para este efeito, e a impressão digital do certificado do canal TLS DEVE ser disponibilizada pelo Estado-Membro aos utilizadores TSL fora da banda.

([2]) ETSI TS 102 778-3 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced — PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic — Profile based on ISO 32000-1.

([4]) É obrigatório proteger o certificado de assinatura do «Scheme Operator» através de assinatura numa das formas especificada na ETSI TS 101 903, devendo o ds:keyInfo incluir a cadeia relevante de certificados, quando aplicável.

▼M1

No âmbito das presentes especificações, a referência atribuída DEVERÁ incluir o «TSL type» (cláusula 5.3.3), o «Scheme name» (cláusula 5.3.6) e o valor da extensão «SubjectKeyIdentifier» do certificado utilizado pelo operador do Sistema para assinar electronicamente a TSL.

▼C1

Signature algorithm identifier (cláusula 5.7.3)

Este campo é OBRIGATÓRIO e DEVERÁ especificar o algoritmo de encriptação que foi utilizado para criar a assinatura. Consoante o algoritmo utilizado, este campo PODE exigir parâmetros adicionais. Este campo DEVE ser incluído no cálculo da assinatura.

Signature value (cláusula 5.7.4)

Este campo é OBRIGATÓRIO e DEVERÁ conter o valor real da assinatura digital. Todos os campos da TSL (excepto o próprio valor da assinatura) DEVEM ser incluídos no cálculo da assinatura.

TSL extensions (cláusula 5.8)

Extensão **expiredCertsRevocationInfo** (cláusula 5.8.1)

Esta extensão é FACULTATIVA. Quando utilizada, DEVE ser conforme com as especificações da ETSI TS 102 231, cláusula 5.8.1.

Extensão **additionalServiceInformation** (cláusula 5.8.2)

Quando utilizada, esta extensão FACULTATIVA DEVE ser utilizada apenas ao nível do Serviço e apenas no campo definido na cláusula 5.5.9 («Service information extension»). É utilizada para fornecer informação complementar sobre um serviço e DEVERÁ ser uma sequência de um ou mais tuplos, cada um dos quais indicando:

a) um URI que identifique a informação complementar, por exemplo:

   — um URI que indique qualquer qualificação específica definida a nível nacional para um fornecedor de «Tokens» de Serviço de Confiança controlado/acreditado, por exemplo:

      — um nível específico de granularidade segurança/qualidade referente ao sistema nacional de controlo/acreditação para PSC que não emitem DC(s) (por exemplo, RGS */**/*** em FR, estado de «supervisão» específico estabelecido pela legislação nacional para PSC(s) específicos que emitem CQ(s) em DE), ver Nota (4) do «Service current status» – cláusula 5.5.4;

      — ou um estatuto jurídico específico para um fornecedor de «Tokens» de Serviço de Confiança controlado/acreditado (por exemplo, «TST qualificado» definido a nível nacional, como na DE ou HU);

      — ou o significado de um identificador de Política específico presente num certificado X.509v3 indicado no campo «Sdi».

   — ou um URI registado, conforme especificado em «Service type identifier», cláusula 5.5.1, a fim de especificar melhor a participação do serviço identificado pelo «Sti» como sendo um serviço integrado num prestador de serviços de certificação que emite CQ (por exemplo, Protocolo OCSP-CQ, CRL-CQ e RootAC-CQ);

b) uma cadeia facultativa contendo o valor da serviceInformation, com o significado especificado no sistema (por exemplo, *, ** ou ***);

c) qualquer informação adicional facultativa fornecida num formato específico do sistema.

▼**M1**

A desreferenciação do URI DEVERÁ gerar informação legível pelos utilizadores (pelo menos em inglês e eventualmente noutra ou outras línguas nacionais) que seja considerada apropriada e suficiente para que os interessados possam compreender a extensão, em particular explicitando o significado dos URI fornecidos e especificando os valores possíveis do campo «serviceInformation» e o significado de cada um desses valores.

Qualifications Extension (cláusula L.3.1)

Descrição:: Este campo é FACULTATIVO mas DEVERÁ estar presente quando a sua utilização for REQUERIDA, por exemplo, para serviços de RootAC/CQ ou AC/CQ, e quando

— a informação fornecida em «Service digital identity» não for suficiente para identificar inequivocamente os certificados qualificados emitidos por este serviço,

— a informação presente nos certificados qualificados em questão não permitir uma identificação processável por computador dos factos sobre se o CQ é ou não suportado por um SSCD.

Quando usada, esta extensão DEVE ser utilizada apenas no campo definido em «Service Information Extension» (cláusula 5.5.9) e DEVE ser conforme com as especificações estabelecidas no anexo L.3.1 da ETSI TS 102 231.

TakenOverBy Extension (cláusula L.3.2)

Descrição.: Esta extensão é FACULTATIVA mas DEVERÁ estar presente quando um serviço que se encontrava sob a responsabilidade legal de um PSC for tomado a cargo por outro PSC, declarando formalmente a responsabilidade legal por um serviço e permitindo que o *software* de verificação possa mostrar ao utilizador certos elementos de carácter legal. As informações fornecidas nesta extensão DEVEM ser coerentes com a correspondente utilização da cláusula 5.5.6 e DEVEM cumprir as especificações constantes do anexo L.3.2 da ETSI TS 102 231.

▼M1

CAPÍTULO II

Ao estabelecer as suas listas aprovadas, os Estados-Membros utilizarão:

Códigos de língua em minúsculas e códigos de país em maiúsculas.

Os códigos de língua e país que constam do quadro a seguir apresentado.

Quando for usado o alfabeto latino (com o código de língua apropriado), é acrescentada uma transliteração para o alfabeto latino com os respectivos códigos de língua, especificados no quadro a seguir apresentado.

Nome abreviado (língua de origem)	Nome abreviado (inglês)	Código de país	Código de língua	Notas	Transliteração para alfabeto latino
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	Código de país recomendado pela UE	el-Latn
España	Spain	ES	es	também Catalão (ca), Basco (eu), Galego (gl)	
France	France	FR	fr		
▼M2 Hrvatska	Croácia	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**

Nome abreviado (língua de origem)	Nome abreviado (inglês)	Código de país	Código de língua	Notas	Transliteração para alfabeto latino
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Código de país recomendado pela UE	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Transliteração para o alfabeto latino: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

CAPÍTULO IV

ESPECIFICAÇÕES PARA O FORMULÁRIO LEGÍVEL POR PESSOAS DA APLICAÇÃO TSL DA LISTA APROVADA

DEVE ser disponibilizada ao público e tornada acessível por meios electrónicos uma forma legível por pessoas (HR) da aplicação TSL da Lista Aprovada. Esta DEVERÁ ser apresentada sob a forma de um documento «Portable Document Format» (PDF), em conformidade com a ISO 32000, que DEVE ser formatado de acordo com o perfil PDF/A (ISO 19005).

O conteúdo do formulário HR de tipo PDF/A da aplicação TSL da Lista Aprovada DEVERÁ satisfazer os seguintes requisitos:

▼M1

— O título das Listas Aprovadas em formato legível pelos utilizadores será construído com base na concatenação dos seguintes elementos:

  — Imagem da bandeira nacional do Estado-Membro (facultativo);

  — Espaço em branco;

  — Nome abreviado do país na(s) língua(s) de origem (tal como figura na primeira coluna do quadro do capítulo II);

  — Espaço em branco;

  — «(»;

  — Nome abreviado do país em inglês (tal como figura na segunda coluna do quadro do capítulo II), entre os parêntesis;

  — «):» para fechar o parêntesis e funcionar como separador;

  — Espaço em branco;

  — «Lista Aprovada»;

  — Logótipo do operador do sistema do Estado-Membro (facultativo);

▼C1

— A estrutura do formulário HR DEVERÁ reflectir o modelo lógico descrito na secção 5.1.2 da ETSI TS 102 231;

— Todos os campos presentes DEVERÃO ser visíveis e indicar:

  — O título do campo (por exemplo, «Service type identifier»);

  — O valor do campo (por exemplo, «AC/CQ»);

  — O significado (descrição) do valor do campo, quando aplicável e em especial nos termos do anexo D da ETSI TS 102 231 ou das presentes especificações para URI(s) registadas (por exemplo, «Uma Autoridade de Certificação que emite certificados de chave pública»);

  — Versões múltiplas em linguagens naturais, como estipulado na aplicação TSL da Lista Aprovada, quando aplicável.

— DEVERÃO, no mínimo, ser visíveis no formulário HR os seguintes campos e valores correspondentes dos certificados digitais presentes no campo «Service digital identity»:

  — Versão

  — Número de série

  — Algoritmo de assinatura

  — Emissor

  — Válido a partir de

  — Válido até

  — Utilizador

▼C1

— Chave pública

— Políticas de Certificados

— Identificador da Chave do Utilizador

— Pontos de Distribuição CRL

— Identificador da Chave da Autoridade

— Utilização de chaves

— Restrições de base

— Algoritmo de impressão digital

— Impressão digital

— O formulário HR DEVERÁ ser fácil de imprimir

— O formulário HR PODE ser assinado electronicamente. Quando assinado, o formulário HR DEVE ser assinado pelo Operador do Sistema de acordo com as especificações de assinatura idênticas às da aplicação TSL da Lista Aprovada.