DECISÃO DE EXECUÇÃO DA COMISSÃO

de 14 de outubro de 2013

que altera a Decisão 2009/767/CE no que diz respeito à elaboração, atualização e publicação de listas aprovadas de prestadores de serviços de certificação controlados/acreditados por Estados-Membros

[notificada com o número C(2013) 6543]

(Texto relevante para efeitos do EEE)

(2013/662/UE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

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

Considerando o seguinte:

(1) A Decisão 2009/767/CE 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 Diretiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno [2], obriga os Estados-Membros a disponibilizar a informação necessária para a validação das assinaturas eletrónicas avançadas suportadas por um certificado qualificado. Esta informação deve ser apresentada uniformemente com base nas denominadas «listas aprovadas», que contêm informações sobre os prestadores de serviços de certificação que emitem certificados qualificados destinados ao público, em conformidade com a Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrónicas [3], e que são controlados/acreditados pelos Estados-Membros.

(2) A experiência prática com a aplicação da Decisão 2009/767/CE pelos Estados-Membros demonstrou a necessidade de certas melhorias para se poder maximizar os benefícios derivados das listas aprovadas. Além disso, o Instituto Europeu de Normalização das Telecomunicações (ETSI) publicou novas especificações técnicas para as listas aprovadas (TS 119 612) que têm por base as especificações que figuram atualmente no anexo da decisão, mas que, ao mesmo tempo, introduzem um certo número de melhorias nas especificações existentes.

(3) A Decisão 2009/767/CE deve, por conseguinte, ser alterada por forma a ter em conta as especificações técnicas 119 612 do ETSI e incluir as alterações consideradas necessárias para melhorar e facilitar a aplicação e utilização das listas aprovadas.

(4) Para que os Estados-Membros possam proceder às necessárias alterações técnicas das suas atuais listas aprovadas, importa que a presente decisão seja aplicável a partir de 1 de fevereiro de 2014.

(5) As medidas previstas na presente decisão são conformes com o parecer do Comité da Diretiva Serviços,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

Alterações da Decisão 2009/767/CE

A Decisão 2009/767/CE é alterada do seguinte modo:

1) O artigo 2.º é alterado do seguinte modo:

a) Os n.os 1, 2 e 2-A passam a ter a seguinte redação:

«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.

2. Os Estados-Membros devem elaborar e publicar as suas listas aprovadas em formato que permita o tratamento por computador, de acordo com as especificações constantes do anexo. Se os Estados-Membros decidirem publicar uma lista aprovada em formato legível pelos utilizadores, esse formato da lista aprovada deve respeitar as especificações apresentadas no anexo.

2-A. Os Estados-Membros devem assinar eletronicamente as suas listas aprovadas em formato que permita o tratamento por computador de modo a garantir a sua autenticidade e integridade. Se os Estados-Membros publicarem as listas aprovadas em formato legível pelos utilizadores, devem assegurar que as listas aprovadas apresentadas com base neste formato contêm os mesmos dados que as listas aprovadas apresentadas com base no formato que permita o tratamento por computador e devem assiná-las eletronicamente com o mesmo certificado utilizado para o formato que permita o tratamento por computador.»;

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

b) É inserido o seguinte n.º 2-B:

«2-B. Os Estados-Membros devem assegurar que as listas aprovadas apresentadas em formato que permita o tratamento por computador sejam acessíveis no seu local de publicação, em qualquer momento e sem interrupção, exceto para efeitos de manutenção.»;

c) O n.º 3 passa a ter a seguinte redação:

«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 que permita o tratamento por computador;

b) O local em que se encontram publicadas as listas aprovadas em formato que permita o tratamento por computador;

c) Dois ou mais certificados de chave pública do operador do sistema, com períodos de validade alterados em, pelo menos, três meses, que correspondam às chaves privadas que podem ser utilizadas para assinar eletronicamente as listas aprovadas em formato que permita o tratamento por computador;

d) Quaisquer alterações das informações referidas nas alíneas a), b) e c).»;

d) É inserido o seguinte n.º 3-A:

«3-A. Se os Estados-Membros publicarem as listas aprovadas em formato legível pelos utilizadores, as informações referidas no n.º 3 devem ser igualmente notificadas para esse formato.».

2) O anexo é substituído pelo anexo da presente decisão.

Artigo 2.º

Aplicação

A presente decisão é aplicável a partir de 1 de fevereiro de 2014.

Artigo 3.º

Destinatários

Os destinatários da presente decisão são os Estados-Membros.

Feito em Bruxelas, em 14 de outubro de 2013.

Pela Comissão

Michel BARNIER

Membro da Comissão

ANEXO

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

PRESCRIÇÕES GERAIS

1. **Introdução**

A finalidade do padrão de referência harmonizado para a «lista aprovada de prestadores de serviços de certificação controlados/acreditados» dos Estados-Membros é estabelecer o modo comum como cada Estado-Membro deve 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 Diretiva 1999/93/CE, o que inclui a prestação de informação sobre o histórico do estado de controlo/acreditação dos serviços de certificação controlados/acreditados.

Esta informação destina-se essencialmente a apoiar a validação de assinaturas eletrónicas qualificadas (AEQ) e assinaturas eletrónicas avançadas (AEA) ([2]) suportadas por um certificado qualificado ([3]) ([4]).

A informação obrigatória a inserir na lista aprovada deve incluir, pelo menos, informação sobre os PSC controlados/ /acreditados que emitem certificados qualificados (CQ) ([5]), em conformidade com o disposto na Diretiva 1999/93/CE (artigo 3.º, n.os 2 e 3, e artigo 7.º, n.º 1, alínea a)), incluindo, se não fizer parte do CQ, informação sobre o CQ que suporta uma assinatura eletrónica e sobre se essa assinatura foi ou não criada por um dispositivo seguro de criação de assinaturas (SSCD) ([6]).

Na lista aprovada pode ser incluída, a nível nacional e a título facultativo, informação adicional sobre outros PSC que não emitem CQ mas que prestam serviços relacionados com assinaturas eletrónicas (por exemplo, PSC que prestam serviços de validação temporal e emitem «Tokens» de validação cronológica, PSC que emitem certificados não qualificados, etc.), desde que sejam controlados/acreditados de modo análogo aos PSC que emitem CQ ou autorizados no âmbito de um sistema nacional diferente de autorização. Os sistemas nacionais de autorização podem, nalguns Estados-Membros, diferir dos sistemas de controlo ou de acreditação facultativa aplicável a PSC que emitem CQ relativamente a requisitos aplicáveis e/ou à organização responsável. Os termos «acreditado» e/ou «controlado» no quadro das presentes especificações cobrem igualmente os sistemas nacionais de autorização, devendo no entanto ser fornecidas pelos Estados-Membros informações adicionais sobre a natureza de quaisquer sistemas nacionais na respetiva lista aprovada, incluindo clarificações sobre as eventuais diferenças com os sistemas de acreditação/controlo aplicados aos PSC que emitem CQ.

O padrão de referência harmonizado assenta na ETSI TS 119612 v1.1.1 ([7]) (a seguir designada por ETSI TS 119612) que visa a elaboração, publicação, localização, acessibilidade, autenticação e integridade dessas listas.

2. **Estrutura do padrão de referência harmonizado para a lista aprovada**

O padrão de referência harmonizado para a lista aprovada de cada Estado-Membro está estruturado, com base na ETSI TS 119612, de acordo com as seguintes categorias de informação:

1. Uma etiqueta (*tag*) de lista aprovada que facilite a identificação da lista aprovada durante as pesquisas eletrónicas;

2. Informação sobre a lista aprovada e respetivo sistema de emissão;

3. 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);

4. Para cada PSC incluído na lista, os pormenores dos seus serviços de confiança específicos e o estado atual em que se encontram registados na lista aprovada são fornecidos na forma de uma sequência de campos de identificação inequívoca dos serviços de certificação controlados/acreditados prestados pelo PSC e do seu estado atual (esta sequência deve ter no mínimo uma entrada);

([1]) Ver definição no artigo 2.º, ponto 11, da Diretiva 1999/93/CE.
([2]) Ver definição no artigo 2.º, ponto 2, da Diretiva 1999/93/CE.
([3]) Neste documento, a sigla «AEA_{CQ}» é utilizada para referir uma AEA suportada por um CQ.
([4]) Refira-se que existem diversos serviços eletrónicos baseados em AEA simples, cuja utilização transfronteiras também seria facilitada se os serviços de certificação correspondentes (por exemplo, a emissão de certificados não qualificados) fossem incluídos nos serviços controlados/acreditados abrangidos por um Estado-Membro na parte sobre informação facultativa da sua lista aprovada.
([5]) Ver definição no artigo 2.º, ponto 10, da Diretiva 1999/93/CE.
([6]) Ver definição no artigo 2.º, ponto 6, da Diretiva 1999/93/CE.
([7]) ETSI TS 119612 v1.1.1 (2013-06) – *Electronic Signatures and Infrastructures* (ESI); Listas aprovadas.

5. Para cada serviço de certificação controlado/acreditado incluído na lista, a informação sobre o historial desse estado, se for caso disso;

6. A assinatura aplicada na lista aprovada.

Nos casos de PSC que emitem CQ, a estrutura da lista aprovada e, em especial, da componente de informação sobre o serviço (de acordo com o ponto 4), permite a prestação de informação complementar no quadro de extensões da informação sobre serviços a fim de compensar as situações em que se encontra disponível informação insuficiente (processável por computador) no certificado qualificado sobre o seu estado de «qualificado», o seu eventual suporte por um SSCD e, em especial, para fazer face ao facto adicional de a maioria dos PSC (comerciais) recorrer a uma única autoridade de certificação (AC) para a emissão de vários tipos de certificados de entidade final, qualificados e não qualificados.

No contexto dos serviços (AC) de geração de certificados, o número de entradas de serviços na lista relativamente a um PSC pode ser reduzido se um ou vários serviços das AC de nível superior existirem no PKI do PSC [por exemplo, no contexto de uma hierarquia de AC que vai desde uma AC de raiz (*Root CA*) até várias AC emitentes], por inclusão na lista desses serviços das AC de nível superior e não dos serviços das AC emitentes de certificados de entidade final (por exemplo, inclusão na lista apenas da AC de raiz do PSC). No entanto, nesses casos, a informação relativa ao estado é aplicável a toda a hierarquia dos serviços da AC abaixo do serviço incluído na lista e deve ser mantido e assegurado o princípio de garantir uma ligação inequívoca entre o serviço de certificação dos PSC_{CQ} e o conjunto de certificados que se destinam a ser identificados como CQ.

2.1. *Descrição da informação em cada categoria*

1. Etiqueta da lista aprovada

2. Informação sobre a lista aprovada e respetivo sistema de emissão

Faz parte desta categoria a seguinte informação:

— Um **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 Diretiva 1999/93/CE);

— **Informação sobre o operador do sistema (proprietário)** da lista aprovada (por exemplo, nome, endereço, contactos, etc. do organismo do Estado-Membro encarregado de elaborar, publicar com segurança e atualizar 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 caráter 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 advertência legal, obrigações, responsabilidades** da lista aprovada;

— **Data e hora da emissão** da lista aprovada;

— **Próxima atualização prevista** da lista aprovada.

3. Informação de identificação inequívoca sobre todos os PCS controlados/acreditados pelo sistema

Este conjunto de informação inclui, pelo menos, o seguinte:

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

— O endereço e contactos do PSC;

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

4. Por cada PSC incluído na lista, uma sequência de campos contendo a identificação inequívoca do serviço de certificação prestado por esse PSC e controlado/acreditado no âmbito da Diretiva 1999/93/CE

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

— Identificador do tipo de serviço: 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) do serviço: Denominação (comercial) deste serviço de certificação;

— Identidade digital do serviço: Um identificador único e inequívoco desse serviço de certificação;

— Estado atual do serviço: Um identificador do estado atual do serviço;

— Data e hora do início do estado atual;

— Extensão da informação sobre o serviço, quando aplicável: Informação complementar sobre o serviço (por exemplo, apresentada diretamente ou através da referência de um endereço de onde essa informação possa ser descarregada): Informação sobre a definição do serviço prestado pelo operador do sistema, informação sobre o acesso no que diz respeito ao serviço, informação sobre a definição do serviço prestado pelo PSC e extensões da informação sobre o serviço. Por exemplo, para os serviços AC/CQ (*CA/QC*), uma sequência facultativa de conjuntos de informação, cada um dos quais indicando:

  — Os critérios a utilizar para uma identificação de nível superior (filtro), no âmbito do serviço de confiança identificado, do conjunto exato de serviços prestados [ou seja, um conjunto de certificados (qualificados)], em relação ao qual é requerida/fornecida informação complementar no que se refere ao seu estado, à indicação do suporte de SSCD e/ou emissão a favor de uma pessoa coletiva, e ainda

  — Os «qualificadores» associados que fornecem informação sobre se o conjunto dos serviços prestados identifica certificados que devem ser considerados qualificados e/ou se os certificados qualificados identificados emitidos deste serviço são suportados por um SSCD e/ou informação sobre se esses CQ são emitidos a favor de pessoas coletivas (por defeito, devem ser considerados como tendo sido emitidos a favor de pessoas singulares).

5. Para cada serviço de certificação incluído na lista, a informação histórica sobre o seu estado

6. Uma assinatura eletrónica para efeitos de autenticação para todos os campos da LA, exceto o próprio valor da assinatura

3. **Orientações para a edição de entradas na lista aprovada**

3.1. *Informação sobre o estado dos serviços de certificação controlados/acreditados e respetivos prestadores apresentada numa lista única*

A lista aprovada de um Estado-Membro significa «a 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 Diretiva 1999/93/CE».

A lista aprovada é o único instrumento a ser utilizado pelo Estado-Membro em causa para prestar informação sobre o estado de controlo/acreditação dos serviços de certificação e respetivos prestadores:

— **Todos os prestadores de serviços de certificação**, tal como definidos no artigo 2.º, ponto 11, da Diretiva 1999/93/CE, ou seja, «uma entidade ou uma pessoa singular ou coletiva que emite certificados ou presta outros serviços relacionados com assinaturas eletrónicas»;

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

Ao ter em conta as definições e disposições estabelecidas na Diretiva 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 (PSC_{CQ}) e os PSC que não emitem CQ destinados ao público mas que prestam «outros serviços (acessórios) relacionados com assinaturas eletrónicas»:

— **PCS que emitem CQ:**

  — 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 Diretiva 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 e que são acreditados num Estado-Membro devem, ainda, ser sujeitos a um sistema adequado de controlo do 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 Diretiva 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 (respetivamente, no artigo 2.º, ponto 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, 11, 12 e 13).

— **PCS que não emitem CQ**:

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

— Alguns dos objetos 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.

Cada Estado-Membro deve elaborar e atualizar uma lista aprovada única, que indique o estado de controlo e/ou acreditação dos serviços de certificação dos PSC que são controlados/acreditados por esse Estado-Membro. A lista aprovada deve incluir, pelo menos, os PSC que emitem CQ. A lista aprovada pode também indicar o estado de outros serviços de certificação controlados ou acreditados sob um sistema de aprovação definido a nível nacional.

3.2. *Um conjunto único de valores para o estado de controlo/acreditação*

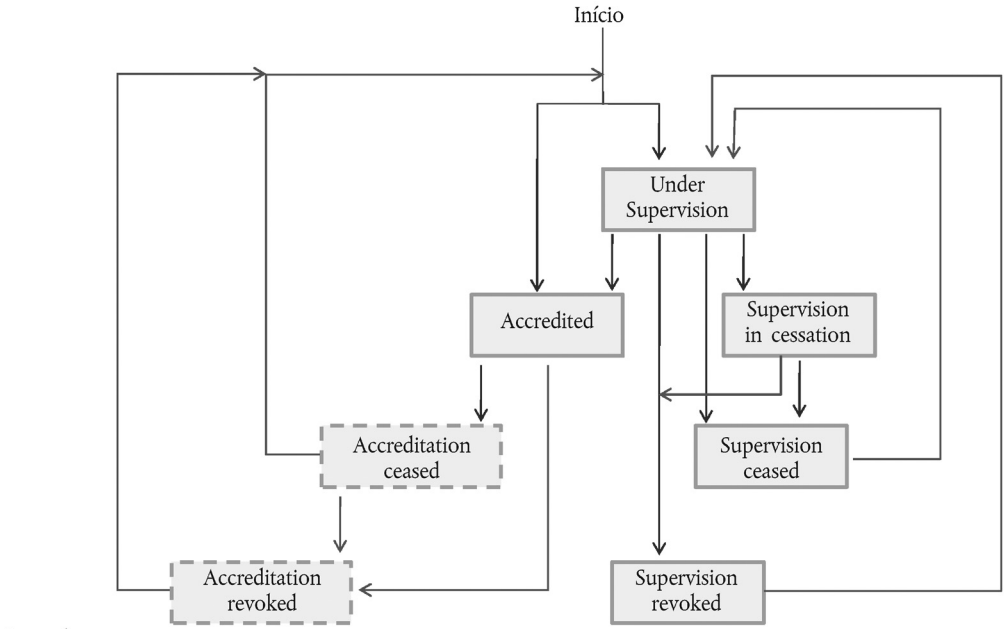
Na lista aprovada, o facto de um serviço estar a ser atualmente «controlado» ou «acreditado» é expresso pelo valor do seu estado atual. Além disso, o estado de controlo ou acreditação pode ser positivo («under supervision», «accredited», «supervision in cessation»), cessado («supervision ceased», «accreditation ceased») ou mesmo revogado («supervision revoked», «accreditation revoked») e ser fixado ao valor correspondente. 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 o possível estado de controlo e o 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 controlo) pode, após algum tempo, decidir conceder a acreditação facultativa ao serviço de certificação atualmente objeto de controlo. Por outro lado, um prestador de serviços de certificação estabelecido noutro Estado-Membro pode decidir não suspender um serviço de certificação acreditado e passá-lo do estado de acreditação para o estado de supervisão, nomeadamente por motivos de ordem comercial e/ou económica.

Figura 1

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



Legenda

Estado de trânsito quando existir um modelo de controlo associado (por exemplo, para um PSC que emite CQ acreditados e controlados no Estado-Membro em que está estabelecido),
Eventual estado atual quando não existir qualquer modelo de controlo associado (por exemplo, para PSC acreditado num Estado-Membro em que não esteja estabelecido)

Eventual estado atual

Quando estabelecido num Estado-Membro, um serviço de certificação que emite CQ deve ser controlado (pelo Estado-Membro em que se encontra estabelecido) e pode ser acreditado facultativamente. O valor do estado desse serviço, se incluído numa lista aprovada, deve dispor de um dos valores de estado acima indicados como «valor atual do estado» em conformidade com o seu estado real e deve mudar, se for caso disso, de acordo com o fluxo acima apresentado. No entanto, a «acreditação cessada» e a «acreditação revogada» devem ser valores de «estado transitório» quando os correspondentes serviços dos PSC_{CQ} estão incluídos na lista aprovada do Estado-Membro em que está estabelecido, uma vez que esses serviços devem ser controlados por defeito (mesmo quando não estão ou deixaram de estar acreditados); quando o serviço correspondente estiver incluído (acreditado) num Estado-Membro diferente daquele em que está estabelecido, estes valores podem ser valores finais.

Os Estados-Membros que estão a elaborar ou já elaboraram um(ns) «sistema(s) de aprovação reconhecido(s)», definido(s) e aplicado(s) a nível nacional para o controlo do cumprimento por parte de serviços de PCS que **não** emitem CQ das disposições estabelecidas na Diretiva 1999/93/CE e das eventuais disposições nacionais referentes à prestação de serviços de certificação (na aceção do artigo 2.º, ponto 11, da Diretiva 1999/93/CE), devem incluir esse(s) sistema(s) de aprovação numa das duas categorias seguintes:

— «Acreditação facultativa», tal como definida e regulamentada pela Diretiva 1999/93/CE (artigo 2.º, ponto 13, artigo 3.º, n.º 2, artigo 7.º, n.º 1, alínea a), artigo 8.º, n.º 1, artigo 11.º, considerandos 4, 11, 12 e 13);

— «Controlo», conforme estipulado na Diretiva 1999/93/CE e aplicado através de disposições e requisitos nacionais, em conformidade com a legislação nacional.

Por conseguinte, um serviço de certificação que não emite CQ pode ser controlado ou acreditado facultativamente. O valor do estado desse serviço, se incluído numa lista aprovada, deve dispor de um dos valores de estado acima indicados como «valor atual do estado» (ver figura 1) em conformidade com o seu estado real e deve mudar, se for caso disso, de acordo com o fluxo acima apresentado.

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_{CQ};

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

— 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.

Os dois últimos conjuntos de informação têm uma importância fundamental para que os terceiros que se apoiam no certificado avaliem a qualidade e o grau de segurança dos sistemas de controlo/acreditação aplicados a nível nacional aos PSC que não emitem CQ. Quando a informação sobre o estado de controlo/acreditação respeitante aos serviços de PSC que não emitem CQ é fornecida na lista aprovada, os atrás referidos conjuntos de informação devem ser fornecidos ao nível dessa lista, 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 Diretiva 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, 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 5.5.9.4) como parte das «Service information extensions» (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 e que o seu estado de controlo/acreditação seja atualizado em consequência.

3.3. *Entradas na lista aprovada destinadas a facilitar a validação de AEQ e* AEA_{CQ}

A parte mais difícil da criação da lista aprovada é a organização da parte obrigatória dessa lista, designadamente a «lista de serviços» por PSC que emitem CQ, de modo a refletir corretamente a situação exata de cada serviço de certificação emitente de CQ 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).

A informação exigida pode incluir informação que não a «Service digital identity» de uma única AC de raiz, em especial a informação que identifica o estado do CQ dos certificados emitidos por esse serviço da AC e se as assinaturas foram criadas por um SSCD. O organismo que, num Estado-Membro, tenha sido indicado para elaborar, editar e manter a lista aprovada deve, por conseguinte, ter em conta o perfil atual e o conteúdo do certificado em cada CQ emitido, para cada serviço de PSC_{QC} incluído nessa lista.

Sempre que possível, cada CQ emitido deve incluir a declaração de QcCompliance definida pelo ETSI ([1]), 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 eletrónicas, e/ou que cada CQ emitido inclui um dos QCP/QCP + Identificadores de Objecto (OID) da política de certificados definidos pela ETSI EN 319 411-2 ([2]). A utilização pelos PSC que emitem CQ 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 a nível do conteúdo real dos CQ atualmente 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 eletrónica é um CQ e se este está ou não associado a um SSCD, através do qual a assinatura foi criada.

([1]) Veja-se ETSI EN 319 412-5 - Assinaturas e Infraestruturas Eletrónicas [*Electronic Signatures and Infrastructures* (ESI)]; perfis dos prestadores de serviços aprovados que emitem certificados; parte 5: extensão do perfil do certificado qualificado para a definição dessa declaração.

([2]) ETSI EN 319 411-2 - Assinaturas e Infraestruturas Eletrónicas [*Electronic Signatures and Infrastructures* (ESI)]; requisitos políticos e de segurança para os prestadores de serviços aprovados que emitem certificados; parte 2: requisitos para as autoridades de certificação emitentes de certificados qualificados.

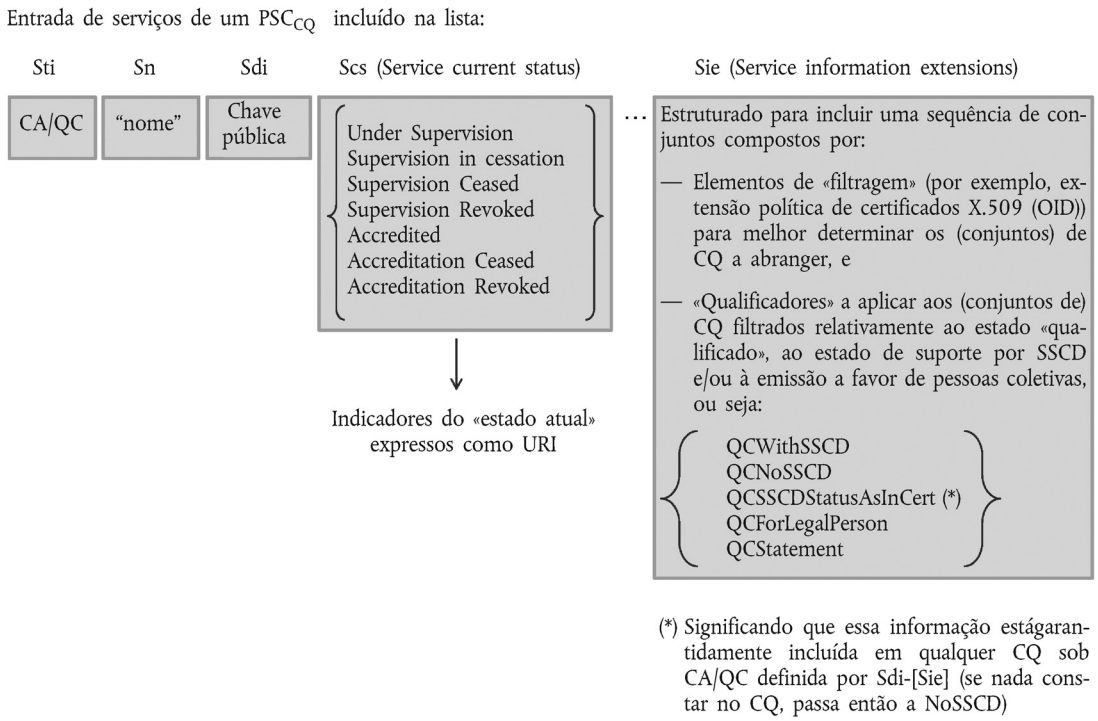
Preencher os campos «Service type identifier» («Sti»), «Service name» («Sn») e «Service digital identity» («Sdi») da entrada de serviço na lista aprovada com informação fornecida no campo «Service information extensions» («Sie») permite a determinação integral do tipo específico de certificado qualificado emitido por um PSC incluído na lista de serviços de certificação que emitem CQ e fornece 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 associada a esta entrada. Este processo está apresentado na figura 2.

Incluir um serviço na lista indicando apenas o «Sdi» de uma AC de raiz significaria que é garantido (pelo PCS emitente de CQ e, também, pelo organismo de controlo/acreditação encarregado do controlo/acreditação desse PCS) que qualquer certificado de entidade final emitido pela (hierarquia) dessa AC de raiz contém suficiente informação definida pelo ETSI e suscetível 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 AC de raiz leva apenas a concluir que os CQ emitidos pela hierarquia desta AC de raiz não são suportados por nenhum SSCD. Para se poder indicar que esses CQ devem ser considerados como suportados por um SSCD, um campo «Sie» deve ser utilizado para indicar este facto (o que também indica que esta informação é garantida pelo PSC emitente de CQ e controlado/acreditado, respetivamente, pelo organismo de controlo ou de acreditação).

Figura 2

Entrada de um serviço de PSC que emite CQ incluído na lista aprovada

Princípios gerais – Regras de edição – Entradas de PSC_{CQ} (serviços incluídos na lista)



As presentes especificações técnicas do padrão de referência harmonizado para a presente lista aprovada 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 («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 a chave pública (no mínimo) de uma AC que emite CQ;

— Para os serviços AC/CQ, a informação facultativa «Service information extension» («Sie») permite a inclusão de um determinado número de elementos de informação específica relacionada com os serviços no que diz respeito ao estado de revogação de certificados anulados, às características adicionais de CQ, à assunção do controlo de um PSC por outro PSC e a outra informação adicional sobre os serviços. Por exemplo, as características adicionais dos CQ são representadas por uma sequência de um ou mais conjuntos, indicando cada um o seguinte:

  — Os critérios a utilizar para identificar a um nível superior (filtro), no âmbito do serviço de certificação identificado pelo «Sdi», o conjunto específico de certificados qualificados para o qual é requerida/fornecida informação complementar no que se refere à indicação do estado de «qualificado», ao suporte por um SSCD e/ou à emissão a favor de uma pessoa coletiva; e ainda

  — A informação associada («qualificadores») sobre se o conjunto de certificados qualificados que devem ser considerados como «qualificados» 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 a informação referente ao facto de esses CQ serem emitidos para pessoas coletivas (por defeito, estes devem ser considerados como tendo sido emitidos apenas para pessoas singulares).

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

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

  — O estado de controlo/acreditação em si.

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

As **orientações gerais de edição** são as seguintes:

1. Quando é garantido [garantia prestada por um PSC_{QC} 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 pela ETSI, e contém de facto a declaração QcSSCD e/ou QCP + Identificador de Objeto (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 não contém a 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 devem ser suportados por SSCD e outros não (por exemplo, essa distinção pode ser feita por OID específicas de políticas de certificados dos PSC ou através de outra informação específica do PSC contida no CQ, direta ou indiretamente, processável por computador ou não), mas um certificado suportado por um SSCD não contém NEM a declaração QcSSCD NEM o QCP(+) OID da 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_{QC} ou através de outra informação específica do PSC_{QC} contida no CQ, direta ou indiretamente, 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 qualificação. 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».

Como princípio geral por defeito, um PSC incluído na lista aprovada deve ter uma entrada de serviço por cada chave pública para um tipo de serviço de certificação AC/CQ, ou seja, por autoridade de certificação que emite (diretamente) CQ. Em algumas circunstâncias excecionais e em condições cuidadosamente geridas, o organismo de controlo/organismo de acreditação

do Estado-Membro pode decidir utilizar, como «Sdi» de uma única entrada na lista de serviços deste PSC listado, a chave pública de uma AC de raiz ou de uma AC de nível superior no PKI do PSC (por exemplo, no contexto de uma hierarquia de AC dos PSC que vai desde uma AC de raiz até várias AC emitentes) em vez de incluir na lista todos os serviços das AC subordinados e emitentes (ou seja, incluir na lista uma autoridade de certificação que não emite diretamente CQ de entidade final mas que certifica uma hierarquia de AC que vai até às AC que emitem CQ a entidades finais). As consequências (vantagens e desvantagens) de usar essa chave pública de AC de raiz ou de AC de nível superior como valor do «Sdi» das entradas de serviços de uma lista aprovada devem ser cuidadosamente analisadas quando aplicado pelos Estados-Membros. Além disso, sempre que utilizar esta exceção autorizada ao princípio por defeito, o Estado-Membro deve fornecer a documentação necessária para facilitar a construção e verificação do caminho de certificação. A título de exemplo, no caso de um PSC_{QC} que utiliza uma AC de raiz sob a qual várias AC emitem CQ e certificados não qualificados, mas para a qual os CQ incluem apenas a declaração de QcCompliance mas não qualquer indicação de serem ou não suportados por um SSCD, listar o «Sdi» da AC de raiz significará, nos termos das regras anteriormente explicadas, que nenhum CQ emitido sob essa AC de raiz é suportado por um SSCD. Se houver CQ que sejam realmente suportados por um SSCD, mas sem declaração processável por computador indicando esse suporte incluída nos certificados, será altamente recomendável recorrer à declaração QcSSCD nos CQ emitidos no futuro. Entretanto (até ao último CQ que não contém esta informação ter expirado), a lista aprovada deve utilizar o campo «Sie» e a extensão «Qualifications» que lhe está associada, por exemplo, prestar informação filtrante destinada a identificar certificados através da utilização de OID definidos para PSC_{CQ} específicos eventualmente utilizados pelo PSC_{QC} para fazer a distinção entre tipos diferentes de CQ (alguns suportados por um SSCD e outros não) e associando «informação sobre suporte por um SSCD» explícita no que se refere aos conjuntos de certificados (filtrados) identificados através do uso de «qualificadores».

As **orientações gerais de utilização** para aplicações, serviços ou produtos associados às assinaturas eletrónicas e dependentes de uma lista aprovada 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 «AC de raiz/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 AC de raiz identificada pelo «Sdi»), todos os certificados de entidade final emitidos são CQ, **desde que** isso seja afirmado no certificado através do uso de uma QcStatement adequada processável por computador (ou seja, QcCompliance) e/ou de OID QCP(+) definidos pela ETSI (e que isto seja garantido pelo organismo de controlo/acreditação, ver atrás as «orientações gerais de edição»)

Nota: se não for apresentada informação «Sie» «Qualifications Extension» ou se um certificado de entidade final que afirma ser um CQ não for identificado a um nível superior através de uma «Sie» «Qualifications Extension» 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, QcCompliance, QcSSCD) e/ou de OID QCP(+) definidos pela ETSI será garantidamente conforme com aquilo que é afirmado pelo PSC_{QC}.

— **e SE** a informação «Sie» «Qualifications Extension» estiver presente, então, além do recurso à atrás referida regra de interpretação por defeito, os certificados que forem identificados através da utilização desta informação «Sie» «Qualifications Extension», construída com base no princípio de uma sequência de filtros que identificam a um nível superior um conjunto de certificados, devem ser considerados em função dos qualificadores associados que fornecem alguma informação complementar sobre o estado «qualificado», o «suporte SSCD» e/ou a «pessoa coletiva como sujeito» (por exemplo, os certificados que contêm um OID específico na extensão política de certificados, e/ou que têm um padrão «utilização de chave» específico, e/ou filtrados através do uso de um valor específico que figura num campo ou numa extensão de um certificado específico, etc.). Esses qualificadores fazem parte do conjunto seguinte de «qualificadores», usado para compensar a falta de informação no conteúdo correspondente do CQ, e que são utilizados, respetivamente:

  — para indicar o estado «qualificado»: «QCStatement» significa o(s) certificado(s) identificado(s) é(são) qualificado(s);

    E/OU

  — para indicar a natureza do suporte por SSCD

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

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

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

    E/OU

— para indicar emissão em favor de uma pessoa coletiva:

— o valor do qualificador «QCForLegalPerson» significa «Certificado emitido em favor de uma pessoa coletiva»

3.5. *Serviços que suportam os serviços «AC/CQ» mas que não fazem parte do «Sdi» «AC/CQ»*

Os serviços relativos ao estado de validade do certificado relacionados com CQ e para os quais a informação sobre o estado de validade do certificado (por exemplo, respostas dos CRL e dos OCSP) deve ser assinada por uma entidade cuja chave privada não seja certificada de acordo com um caminho de certificação que conduza a CQ listadas emitentes de AC («AC/CQ»), devem ser incluídos na lista aprovada (ou seja, com um tipo de serviço «OCSP/CQ» ou «CRL/CQ», respetivamente), uma vez que estes serviços podem ser considerados parte dos serviços «qualificados» controlados/acreditados relacionados com a prestação de serviços de certificação de CQ. Como é evidente, os respondedores OCSP ou os emissores de CRL cujos certificados sejam assinados por AC hierarquicamente dependentes de um serviço AC/CQ listado devem ser considerados «válidos» e conformes com o valor do estado do serviço AC/CQ listado.

Pode aplicar-se uma disposição semelhante aos serviços de certificação que emitem certificados não qualificados (do tipo de serviço «AC/PKC»).

A lista aprovada deve incluir serviços relativos ao estado de validade dos certificados quando não existir informação sobre a localização desses serviços nos certificados de entidade final aos quais se aplicam os serviços relativos ao estado de validade dos certificados.

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, ponto 11, da Diretiva 1999/93/CE.
Autoridade de certificação	AC	1) Um prestador de serviços de certificação que cria e atribui os certificados de chave pública; ou 2) Um serviço técnico de geração de certificados que é utilizado por um prestador de serviços de certificação que cria e atribui os certificados de chave pública. *NOTA*: Ver cláusula 4 da EN 319 411-2 [1] para mais explicações sobre o conceito de autoridade de certificação.
Autoridade de certificação que emite certificados qualificados	AC/CQ	Uma AC que cumpre os requisitos previstos no anexo II da Diretiva 1999/93/CE e emite certificados qualificados que cumprem os requisitos previstos no anexo I da Diretiva 1999/93/CE.
Certificado	Certificado	Como definido no artigo 2.º, ponto 9, da Diretiva 1999/93/CE.
Certificado qualificado	CQ	Como definido no artigo 2.º, ponto 10, da Diretiva 1999/93/CE.
Signatário	Signatário	Como definido no artigo 2.º, ponto 3, da Diretiva 1999/93/CE.
Controlo	Controlo	Refere-se ao controlo previsto no artigo 3.º, n.º 3, da Diretiva 1999/93/CE. A Diretiva 1999/93/CE 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 referida diretiva.
Acreditação facultativa	Acreditação	Como definido no artigo 2.º, ponto 13, da Diretiva 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 Diretiva 1999/93/CE.

Termo	Sigla	Definição
Lista sobre o estado dos serviços de confiança	TSL	Modelo de lista assinada utilizado como base para a apresentação de informação sobre o estado dos serviços de confiança, em conformidade com as especificações estabelecidas na ETSI TS 119612.
Serviço de confiança		Serviço que reforça a confiança e a segurança relativamente às transações eletrónicas (que habitualmente, mas não necessariamente, utiliza técnicas criptográficas ou envolve material confidencial) (ETSI TS 119612). *NOTA*: Esta designação é utilizada numa aceção mais vasta do que serviço de certificação que emite certificados ou presta outros serviços relacionados com assinaturas eletrónicas.
Prestador de serviços de confiança	TSP	Organismo de que depende um ou mais serviços de confiança (eletrónicos) (esta designação é utilizada numa aceção mais vasta do que PSC).
«Token» de serviço de confiança	TrST	Objeto físico ou binário (lógico) gerado ou emitido em resultado do recurso a um serviço de confiança. São exemplos de TrST binários os certificados, as listas de revogação de certificados (LRC), os «Tokens» de validação cronológica (TST) e as respostas do protocolo sobre o estado do certificado em linha (OCSP).
Assinatura eletrónica qualificada	AEQ	Uma AEA suportada por um CQ e criada por um dispositivo seguro de criação de assinaturas, definido no artigo 2.º da Diretiva 1999/93/CE.
Assinatura eletrónica avançada	AEA	Definida no artigo 2.º, ponto 2, da Diretiva 1999/93/CE.
Assinatura eletrónica avançada suportada por um certificado qualificado	AEA_{CQ}	Significa uma assinatura eletrónica que satisfaz os requisitos de uma AEA e é suportada por um CQ, definido no artigo 2.º da Diretiva 1999/93/CE.
Dispositivo seguro de criação de assinaturas	SSCD	Definido no artigo 2.º, ponto 6, da Diretiva 1999/93/CE.

([1]) EN 319 411-2 - Assinaturas eletrónicas e infraestruturas (ESI); Requisitos políticos e de segurança para os prestadores de serviços de confiança que emitem certificados; Parte 2: Requisitos para as autoridades de certificação emitentes de certificados qualificados.

Nos capítulos seguintes, as palavras-chave «DEVE», «NÃO DEVE», «OBRIGATÓRIO», «RECOMENDADO», «PODE» e «FACULTATIVO» devem ser interpretadas tal como descritas no RFC 2119 ([1]).

CAPÍTULO I

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

As presentes especificações baseiam-se nas especificações e nos requisitos constantes da ETSI TS 119612 v1.1.1 (a seguir designado por ETSI TS 119612).

Nos casos em que as presentes especificações não apresentem nenhum requisito específico, DEVEM aplicar-se na íntegra os requisitos da ETSI TS 119612 cláusulas 5 e 6. Quando os requisitos específicos constarem das presentes especificações, DEVEM prevalecer sobre os requisitos correspondentes da ETSI TS 119612. Em caso de discrepâncias entre as presentes especificações e as especificações da ETSI TS 119612, as presentes especificações SÃO as especificações normativas.

Scheme operator name (cláusula 5.3.4)

Este campo DEVE estar presente e DEVE estar em conformidade com as especificações da TS 119612 cláusula 5.3.4.

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

Os países PODEM ter organismos de controlo e de acreditação distintos e até outros organismos além destes para realizar quaisquer outras atividades operacionais relacionadas. Cabe a cada Estado-Membro designar o operador do sistema da lista aprovada do Estado-Membro. Considera-se que (no caso de serem 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 DEVEM ser sempre indicados e identificados como tal na informação sobre o sistema, como parte da lista aprovada, incluindo na informação específica sobre o sistema indicada pelo «Scheme information URI» (cláusula 5.3.7).

Scheme name (cláusula 5.3.6)

Este campo DEVE estar presente e DEVE estar em conformidade com as especificações da TS 119612 cláusula 5.3.6 em que a seguinte designação DEVE ser utilizada para efeitos do sistema:

«EN_name_value» = «Lista do estado de controlo/acreditação dos serviços de certificação de prestadores de serviços de certificação que são controlados/acreditados pelo Estado-Membro do operador do sistema referenciado quanto ao cumprimento das disposições aplicáveis fixadas pela Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrónicas.»

Scheme information URI (cláusula 5.3.7)

Este campo DEVE estar presente e DEVE estar em conformidade com as especificações da TS 119612 cláusula 5.3.7 em que a informação adequada sobre o sistema DEVE incluir, no mínimo:

— Informações introdutórias comuns a todos os Estados-Membros, no que se refere ao âmbito e aos antecedentes da lista aprovada e ao(s) sistema(s) subjacente(s) de controlo/acreditação. O texto comum a utilizar é o texto a seguir apresentado, em que a cadeia de carateres «[*nome do Estado-Membro em causa*]» DEVE ser substituída pelo nome do Estado-Membro em causa:

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

The Trusted List aims at:

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

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

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

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

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

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

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

  — 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 DEVE incluir, relativamente a cada um dos sistemas subjacentes atrás enumerados, pelo menos o seguinte:

  — Descrição geral;

  — Informação sobre o processo adotado 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 objetos 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 específica complementar do Estado-Membro sobre o sistema PODE ser prestada facultativamente, por exemplo:

— Informação sobre os critérios e as regras utilizados para selecionar 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.

Scheme type/community/rules (cláusula 5.3.9)

Este campo DEVE estar presente, DEVE estar em conformidade com as especificações da TS 119612 cláusula 5.3.9 e DEVE incluir, pelo menos, duas URI:

— Uma URI comum às listas aprovadas de todos os Estados-Membros, apontando para um texto descritivo que DEVE ser aplicável a todas as listas aprovadas, do seguinte modo:

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

  Texto descritivo:

  «*Participation in a scheme*

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

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

  Policy/rules for the assessment of the listed services

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

([1]) 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 aplicáveis aos PSC que não emitem CQ. Estes conjuntos de informação devem ser fornecidos ao nível da lista aprovada 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 Diretiva 1999/93/CE, conjugado com a capacidade dos Estados-Membros para acrescentarem texto/referências específicas de cada um). Se necessário e requerido, pode 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)

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including compliance with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Article 3(3), Article 8)(1), Article 11 (respectively, Article2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11).

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

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

Interpretation of the Trusted List

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

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

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

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

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

— to indicate the qualified status: «QCStatement» meaning the identified certificate(s) is(are) qualified;

AND/OR

— to indicate the nature of the SSCD support:

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

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

— «QCSSCDStatusAsInCert» qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the «Sdi»-«Sie» provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

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

The general interpretation rule for any other «Sti» type entry is that the listed service named according to the «Sn» field value and uniquely identified by the «Sdi» field value has a current supervision/accreditation status according to the «Scs» field value as from the date indicated in the «Current status starting date and time». Specific interpretation rules for any additional information with regard to a listed service (e.g. «Service information extensions» field) may be found, when applicable, in the Member State specific URI as part of the present «Scheme type/community/rules» field.

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

— Um URI específico da lista aprovada de cada Estado-Membro, apontando para um texto descritivo que DEVE ser aplicável à LA desse Estado-Membro:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC em que CC = o código de país ISO 3166-1 ([1]) alfa-2 utilizado no campo «Scheme territory» (cláusula 5.3.10)

— No qual os utilizadores possam obter a política/regras específicas do Estado-Membro referenciado, segundo as quais os serviços incluídos na lista DEVEM ser avaliados, em conformidade com o sistema adequado de controlo e de acreditação facultativa do Estado-Membro.

— No qual os utilizadores possam obter uma descrição específica do Estado-Membro referenciado sobre o modo de utilizar e interpretar o conteúdo da lista aprovada, no que se refere aos serviços de certificação não relacionados com a emissão de CQ. Esse URI pode ser utilizado 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 utilizados o «Scheme service definition URI» (cláusula 5.5.6) e o campo «Service information extension» (cláusula 5.5.9).

Os Estados-Membros PODEM definir e utilizar URI adicionais a partir do atrás referido URI específico de cada Estado-Membro (ou seja, URI definidos a partir desse URI hierárquico específico).

TSL policy/legal notice (cláusula 5.3.11)

Este campo DEVE estar presente e DEVE estar em conformidade com as especificações da TS 119612 cláusula 5.3.11 em que a política/advertência jurídica sobre o estatuto jurídico do sistema ou os requisitos legais preenchidos pelo regime na jurisdição em que está estabelecido e/ou eventuais restrições e condições sob as quais a lista aprovada é mantida e publicada constituam uma cadeia de carateres multilingue (texto não encriptado) composta por duas partes:

1. A primeira parte, obrigatória, comum às listas aprovadas de todos os Estados-Membros (com o inglês britânico como língua obrigatória e, eventualmente, com uma ou mais línguas nacionais), indicando que o quadro jurídico aplicável é a Diretiva 1999/93/CE e a sua correspondente transposição 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 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.».

([1]) ISO 3166-1:2006: «Códigos para a representação dos nomes dos países e suas subdivisões – Parte 1: Códigos dos países».

Texto na(s) língua(s) nacional(is) dos Estados-Membros: [tradução(ões) oficial(is) do texto inglês atrás apresentado].

2. A segunda parte, facultativa, exclusiva de cada lista aprovada (com o inglês britânico como língua obrigatória e, eventualmente, com uma ou mais línguas nacionais), indicando as referências aos quadros jurídicos nacionais aplicáveis (em especial no que se refere aos sistemas nacionais de controlo/acreditação de PSC que não emitem CQ).

CAPÍTULO II

CONTINUIDADE DAS LISTAS APROVADAS

Os certificados a notificar à Comissão, nos termos do artigo 3.º, alínea c), da presente decisão, DEVEM ser emitidos por forma a:

— Disporem, no mínimo, de três meses entre os respetivos prazos de validade,

— Serem criados com base em novos pares de chaves, dado nenhum par de chaves anteriormente utilizado dever ser objeto de nova certificação.

No caso de afetação ou anulação de UMA das chaves privadas correspondente à chave pública que poderia ser utilizada para validar a assinatura da lista aprovada e que foi notificada à Comissão e publicada nas listas centrais de apontadores da Comissão, os Estados-Membros DEVEM:

— Reemitir imediatamente uma nova lista aprovada assinada com uma chave privada não afetada no caso de a lista aprovada publicada ter sido assinada com uma chave privada afetada ou anulada;

— Notificar imediatamente à Comissão a nova lista de certificados de chave pública correspondentes às chaves privadas que poderiam ser utilizadas para assinar a lista aprovada.

No caso de afetação ou anulação de TODAS as chaves privadas correspondentes às chaves públicas que poderiam ser utilizadas para validar a assinatura da lista aprovada e que foram notificadas à Comissão e publicadas nas listas centrais de apontadores da Comissão, os Estados-Membros DEVEM:

— Gerar novos pares de chaves que poderão ser utilizados para assinar a lista aprovada e os correspondentes certificados de chave pública;

— Reemitir imediatamente uma nova lista aprovada assinada com uma dessas novas chaves privadas e cujo certificado correspondente de chave pública deve ser notificado;

— Notificar imediatamente à Comissão a nova lista de certificados de chave pública correspondentes às chaves privadas que poderiam ser utilizadas para assinar a lista aprovada.

CAPÍTULO III

ESPECIFICAÇÕES PARA O FORMULÁRIO LEGÍVEL POR PESSOAS DA LISTA APROVADA

Se um formulário legível por pessoas da lista aprovada for criado e publicado, DEVE ser apresentado sob a forma de um documento «Portable Document Format» (PDF), em conformidade com a ISO 32000 ([1]), que DEVE ser formatado de acordo com o perfil PDF/A (ISO 19005 ([2])).

O conteúdo do formulário legível por pessoas da lista aprovada de tipo PDF/A DEVE satisfazer os seguintes requisitos:

— A estrutura do formulário HR DEVE refletir o modelo lógico descrito na TS 119612;

— Todos os campos presentes DEVEM 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 (por exemplo, «Uma autoridade de certificação que emite certificados de chave pública»);

  — Versões múltiplas em linguagens naturais, como estipulado na lista aprovada, quando aplicável.

([1]) ISO 32000-1:2008: Gestão de documentos – «Portable Document Format» – Parte 1: PDF 1.7
([2]) ISO 19005-2:2011: Gestão de documentos – Formato de ficheiro de documentos eletrónico para a preservação a longo prazo – Parte 2: Utilização da norma ISO 32000-1 (PDF/A-2)

— DEVEM, 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

  — Emitente

  — Data de emissão

  — Data de validade

  — Assunto

  — 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 DEVE ser fácil de imprimir

— O formulário HR DEVE ser assinado pelo operador do sistema de acordo com o perfil de base de assinaturas PAdES ([1]).

([1]) ETSI TS 103172 (março de 2012) - Assinaturas e infraestruturas eletrónicas [*Electronic Signatures and Infrastructures* (ESI)]; Perfil de base PAdES.