

**DECISÃO DE EXECUÇÃO (UE) 2015/1505 DA COMISSÃO****de 8 de setembro de 2015****que estabelece as especificações técnicas e os formatos relativos às listas de confiança, nos termos do artigo 22.º, n.º 5, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno****(Texto relevante para efeitos do EEE)**

A COMISSÃO EUROPEIA,

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

Tendo em conta o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE <sup>(1)</sup>, nomeadamente o artigo 22.º, n.º 5,

Considerando o seguinte:

- (1) As listas de confiança são essenciais para a criação de confiança entre os operadores do mercado, dado que indicam o estatuto do prestador do serviço quando se efetua o controlo.
- (2) A utilização transfronteiriça de assinaturas eletrónicas foi facilitada pela Decisão 2009/767/CE da Comissão <sup>(2)</sup>, que estabeleceu a obrigação de os Estados-Membros elaborarem, manterem e publicarem listas de confiança com informações relativas aos 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 <sup>(3)</sup> e que são controlados e aprovados pelos Estados-Membros.
- (3) O artigo 22.º do Regulamento n.º 910/2014/UE prevê a obrigação de os Estados-Membros elaborarem, manterem e publicarem listas de confiança, de forma segura, assinadas ou seladas eletronicamente num formato adequado para tratamento automático e a notificar à Comissão os organismos responsáveis pela elaboração das listas de confiança nacionais.
- (4) Um prestador de serviços de confiança e os serviços de confiança que presta devem ser considerados qualificados quando o estatuto de qualificado estiver associado ao prestador na lista aprovada. A fim de assegurar que outras obrigações decorrentes do Regulamento (UE) n.º 910/2014, em especial as fixadas nos artigos 27.º e 37.º, possam ser facilmente respeitadas, à distância e por meios eletrónicos, pelos prestadores de serviços e a fim de responder às expectativas legítimas dos outros prestadores de serviços de certificação que não emitem certificados qualificados mas prestam serviços relacionados com assinaturas eletrónicas nos termos da Diretiva 1999/93/CE e que constarão da lista até 30 de junho de 2016, deve ser possível que os Estados-Membros acrescentem serviços de confiança não qualificados às listas de confiança, numa base voluntária, a nível nacional, desde que seja claramente indicado que essas estruturas não são qualificadas em conformidade com o Regulamento (UE) n.º 910/2014.
- (5) De acordo com o considerando 25 do Regulamento (UE) n.º 910/2014, os Estados-Membros podem acrescentar outros tipos de serviços de confiança definidos a nível nacional, para além dos definidos no artigo 3.º, n.º 16, do Regulamento (UE) n.º 910/2014, desde que seja claramente indicado que não são qualificados em conformidade com o Regulamento (UE) n.º 910/2014.
- (6) As medidas previstas na presente decisão são conformes com o parecer do comité instituído pelo artigo 48.º do Regulamento (UE) n.º 910/2014,

ADOTOU A PRESENTE DECISÃO:

*Artigo 1.º*

Os Estados-Membros devem elaborar, publicar e manter listas de confiança, incluindo informações sobre os prestadores de serviços de confiança qualificados que supervisionam, bem como informações sobre os serviços de confiança qualificados por eles prestados. Estas listas devem ser conformes com as especificações técnicas definidas no anexo I.

<sup>(1)</sup> JO L 257 de 28.8.2014, p. 73.

<sup>(2)</sup> 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 (JO L 274 de 20.10.2009, p. 36).

<sup>(3)</sup> 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 (JO L 13 de 19.1.2000, p. 12).

*Artigo 2.º*

Os Estados-Membros podem incluir nas listas de confiança informações sobre prestadores de serviços de confiança não qualificados, bem como informações relacionadas com os serviços de confiança não qualificados por eles prestados. A lista deve indicar claramente que os prestadores de serviços de confiança e os serviços de confiança por eles prestados não são qualificados.

*Artigo 3.º*

1. Nos termos do artigo 22.º, n.º 2, do Regulamento (UE) n.º 910/2014, os Estados-Membros devem assinar ou selar eletronicamente, num formato adequado para tratamento automático, a sua lista aprovada em conformidade com as especificações técnicas definidas no anexo I.
2. Se um Estado-Membro publicar a lista de confiança por via eletrónica num formato legível por pessoas, deve assegurar que este formato da lista aprovada contém os mesmos dados do que o formato adequado para tratamento automático e deve assiná-la ou selá-la por via eletrónica de acordo com as especificações técnicas definidas no anexo I.

*Artigo 4.º*

1. Os Estados-Membros devem comunicar à Comissão as informações a que se refere o artigo 22.º, n.º 3, do Regulamento (UE) n.º 910/2014 utilizando o modelo que figura no anexo II.
2. As informações a que se refere o n.º 1 devem incluir dois ou mais certificados de chave pública do operador do sistema, com prazos de validade alternados em, pelo menos, três meses, que correspondam às chaves privadas que podem ser utilizadas para assinar ou selar eletronicamente a lista aprovada no formato adequado para tratamento automático e no formato legível por pessoas, quando publicado.
3. Nos termos do artigo 22.º, n.º 4, do Regulamento (UE) n.º 910/2014, a Comissão deve disponibilizar ao público, através de um canal seguro para um servidor Web autenticado, as informações referidas nos n.ºs 1 e 2, tal como notificadas pelos Estados-Membros, num formato adequado para tratamento automático, eletronicamente assinado ou selado.
4. A Comissão deve disponibilizar ao público, através de um canal seguro para um servidor Web autenticado, as informações referidas nos n.ºs 1 e 2, tal como notificadas pelos Estados-Membros, num formato legível por pessoas, eletronicamente assinado ou selado.

*Artigo 5.º*

A presente decisão entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 8 de setembro de 2015.

*Pela Comissão*  
*O Presidente*  
Jean-Claude JUNCKER

## ANEXO I

## ESPECIFICAÇÕES TÉCNICAS PARA UM MODELO COMUM DE LISTA DE CONFIANÇA

## CAPÍTULO I

## REQUISITOS GERAIS

As listas de confiança devem incluir todas as informações atuais e históricas relativas ao estatuto dos serviços de confiança constantes das listas, a contar da inclusão de um prestador de serviços de confiança nas listas de confiança.

No quadro das presentes especificações, os termos «aprovado», «acreditado» e/ou «controlado» abrangem igualmente os sistemas nacionais de aprovação, devendo no entanto os Estados-Membros fornecer, na respetiva lista de confiança, informações adicionais sobre a natureza desses sistemas nacionais, incluindo esclarecimentos sobre as eventuais diferenças relativamente aos sistemas de controlo aplicados aos prestadores de serviços de confiança qualificados e aos serviços de confiança qualificados que prestam.

A informação fornecida na lista de confiança destina-se essencialmente a apoiar a validação de «tokens» de serviços de confiança qualificados, ou seja, objetos físicos ou binários (lógicos) gerados ou emitidos em resultado do recurso a um serviço de confiança qualificado, por exemplo, assinaturas/selos eletrónicos qualificados, assinaturas/selos eletrónicos avançados baseados num certificado qualificado, selos temporais qualificados, comprovativos eletrónicos de entrega qualificados, etc.

## CAPÍTULO II

## ESPECIFICAÇÕES TÉCNICAS PORMENORIZADAS PARA O MODELO COMUM DE LISTA DE CONFIANÇA

As presentes especificações baseiam-se nas especificações e requisitos da ETSI TS 119 612 v2.1.1 (a seguir designada ETSI TS 119 612).

Quando as presentes especificações não prevejam qualquer requisito específico, devem aplicar-se na íntegra os requisitos da ETSI TS 119 612, cláusulas 5 e 6. Quando os requisitos específicos constarem das presentes especificações, estes prevalecem sobre os requisitos correspondentes da ETSI TS 119 612. Em caso de discrepâncias entre as presentes especificações e as especificações da ETSI TS 119 612, prevalecem as presentes especificações.

**Designação do sistema** (cláusula 5.3.6)

Este campo deve estar presente e estar conforme com as especificações da TS 119 612, cláusula 5.3.6, devendo ser utilizada a seguinte designação para efeitos do sistema:

«EN\_name\_value» = «Lista de confiança que inclui informações relativas aos prestadores de serviços de confiança qualificados sujeitos ao controlo do Estado-Membro de emissão, bem como informações relacionadas com os serviços de confiança qualificados por eles prestados, em conformidade com as disposições aplicáveis do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga Diretiva 1999/93/CE.»

**Informação URI do sistema** (cláusula 5.3.7)

Este campo deve estar presente e estar conforme com as especificações da TS 119 612, cláusula 5.3.7, devendo a informação adequada sobre o sistema incluir, no mínimo:

- a) Informações introdutórias comuns a todos os Estados-Membros, relativas ao âmbito e aos antecedentes da lista de confiança e ao(s) sistema(s) subjacente(s) de aprovação (por exemplo, de acreditação). O texto comum a utilizar é o texto a seguir apresentado, em que a cadeia de caracteres «[nome do Estado-Membro em causa]» deve ser substituída pelo nome do Estado-Membro em causa:

«A presente lista é a lista de confiança que inclui informações relativas aos prestadores de serviços de confiança qualificados sujeitos ao controlo de [nome do Estado-Membro em causa], bem como informações relacionadas com os serviços de confiança qualificados por eles prestados, em conformidade com as disposições aplicáveis do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga Diretiva 1999/93/CE.»

A utilização transfronteiriça de assinaturas eletrónicas foi facilitada pela Decisão 2009/767/CE da Comissão, de 16 de outubro de 2009, que estabeleceu a obrigação de os Estados-Membros elaborarem, manterem e publicarem listas de confiança com informações relativas aos 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, e que são controlados/acreditados pelos Estados-Membros. A presente lista de confiança é a continuação da lista aprovada estabelecida na Decisão 2009/767/CE.»

As listas de confiança são elementos essenciais para a criação de confiança entre os operadores do mercado eletrónico, permitindo aos utilizadores determinar o estatuto qualificado e o historial do estatuto dos prestadores de serviços de confiança e os seus serviços.

As listas de confiança dos Estados-Membros incluem, no mínimo, as informações especificadas nos artigos 1.º e 2.º da Decisão de Execução (UE) 2015/1505.

Os Estados-Membros podem incluir nas listas de confiança informações sobre prestadores de serviços de confiança não qualificados, bem como informações relacionadas com os serviços de confiança não qualificados por eles prestados. Deve ser claramente indicado que não são qualificados em conformidade com o Regulamento (UE) n.º 910/2014.

Os Estados-Membros podem incluir nas listas de confiança informações sobre outros tipos de serviços de confiança definidos a nível nacional, para além dos definidos no artigo 3.º, n.º 16, do Regulamento (UE) n.º 910/2014. Deve ser claramente indicado que não são qualificados em conformidade com o Regulamento (UE) n.º 910/2014.

b) Informações específicas sobre o regime de controlo subjacente e, se aplicável, o(s) regime(s) de aprovação nacional (por exemplo, a acreditação), em especial <sup>(1)</sup>:

- (1) Informações sobre o sistema de controlo nacional aplicável aos prestadores de serviços de confiança qualificados e não qualificados e aos serviços de confiança qualificados e não qualificados que estes prestam, tal como previsto no Regulamento (UE) n.º 910/2014;
- (2) Se aplicável, informações sobre os regimes nacionais facultativos de acreditação aplicáveis aos prestadores de serviços de certificação que emitem certificados qualificados em conformidade com a Diretiva 1999/93/CE.

Estas informações específicas devem incluir, relativamente a cada um dos sistemas subjacentes atrás enumerados, pelo menos o seguinte:

- (1) Descrição geral;
- (2) Informação sobre o processo utilizado pelo sistema de controlo nacional e, quando aplicável, para a aprovação no âmbito de um regime nacional;
- (3) Informação sobre os critérios segundo os quais os prestadores de serviços de confiança são controlados ou, quando aplicável, aprovados;
- (4) Informação sobre os critérios e as regras utilizados para selecionar os supervisores/auditores e para definir a forma como os prestadores de serviços de confiança e os serviços de confiança que estes prestam são avaliados;
- (5) Quando aplicável, outros contactos e informações gerais referentes ao funcionamento do sistema.

#### **Tipo/comunidade/regras do sistema** (cláusula 5.3.9)

Este campo deve estar presente e estar conforme com as especificações da TS 119 612, cláusula 5.3.9.

Deve incluir apenas URI em língua inglesa (Reino Unido).

<sup>(1)</sup> Estes conjuntos de informação têm uma importância fundamental para que os utilizadores possam avaliar o nível de qualidade e segurança destes sistemas. Estes conjuntos de informação devem ser fornecidos ao nível da lista de confiança enquanto estiver a ser utilizado a atual «Informação URI do sistema» (cláusula 5.3.7 — informação fornecida pelo Estado-Membro), o «Tipo/comunidade/regras do sistema» (cláusula 5.3.9 — através da utilização de um texto comum a todos os Estados-Membros) e a «Lista de serviços de confiança — política/advertência jurídica» (cláusula 5.3.11 — um texto comum a todos os Estados-Membros, conjugado com a possibilidade de os Estados-Membros acrescentarem texto/referências específicas). Se aplicável e requerido, pode ser prestada informação complementar sobre os sistemas nacionais aplicáveis aos prestadores de serviços de confiança não qualificados e definidos (qualificados) a nível nacional (por exemplo, para distinguir vários níveis de qualidade/segurança), através do recurso à informação URI do sistema (cláusula 5.5.6).

O relatório deve incluir, pelo menos, dois URI:

- (1) Um URI comum às listas de confiança de todos os Estados-Membros, que reenvia para um texto descritivo que deve ser aplicável a todas as listas de confiança, 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 including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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

*Policy/rules for the assessment of the listed services*

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

*Interpretation of the Trusted List*

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

The "qualified" status of a trust service is indicated by the combination of the "Service type identifier" ("Sti") value in a service entry and the status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time". Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

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

— indicates that any end-entity certificate issued by or under the CA represented by the "Service digital identifier" ("Sdi") CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

- the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),
- the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. “undersupervision”, “supervisionincessation”, “accredited” or “granted”) for that entry.

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

— to indicate the qualified certificate nature:

— “QCStatement” meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;

— “QCForESig” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) n.º 910/2014;

— “QCForESeal” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) n.º 910/2014;

— “QCForWSA” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) n.º 910/2014.

— to indicate that the certificate is not to be considered as qualified:

— “NotQualified” meaning the identified certificate(s) is(are) not to be considered as qualified; and/or

— to indicate the nature of the SSCD support:

— “QCWithSSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

— “QCNoSSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

— “QCSSCDStatusAsInCert” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

— to indicate the nature of the QSCD support:

— “QCWithQSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

— “QCNoQSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

— “QCQSCDStatusAsInCert” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

— “QCQSCDManagedOnBehalf” indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or

- to indicate issuance to Legal Person:
  - “QCForLegalPerson” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

- if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, and
- if no “Sie” “Qualifications Extension” information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a “QCStatement” qualifier, or
- an “Sie” “Qualifications Extension” information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a “NotQualified” qualifier,

then the certificate is not to be considered as qualified.

“Service digital identifiers” are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer’s or seal creator’s certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other “Sti” type entry is that, for that “Sti” identified service type, the listed service named according to the “Service name” field value and uniquely identified by the “Service digital identity” field value has the current qualified or approval status according to the “Service current status” field value as from the date indicated in the “Current status starting date and time”.

As regras específicas de interpretação de toda a informação complementar referente a um serviço listado (por exemplo, campo “Service information extensions”) podem ser encontradas, quando aplicável, no URI específico do Estado-Membro como parte do campo “Scheme type/community/rules”.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States’ trusted lists.»

- (2) Um URI específico da lista de confiança por cada Estado-Membro, apontando para um texto descritivo que deve ser aplicável à lista de confiança desse Estado-Membro:

<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC>, sendo «CC» o código ISO 3166-1 <sup>(1)</sup> alpha-2 do país utilizado no campo «Território do sistema» (cláusula 5.3.10)

- Onde os utilizadores podem obter a política/regras específicas do Estado-Membro referenciado que regem a avaliação dos serviços incluídos na lista, em conformidade com o sistema de controlo e, quando aplicável, de aprovação do Estado-Membro.
- Onde os utilizadores podem obter uma descrição específica do Estado-Membro referenciado sobre o modo de utilizar e interpretar o conteúdo da lista de confiança, no que se refere aos serviços de confiança não qualificados e/ou definidos a nível nacional constantes da lista. Este texto pode ser utilizado para indicar uma hipotética granularidade nos sistemas nacionais de aprovação em relação aos prestadores de serviços de confiança que não emitem certificados qualificados e o modo como os campos «URI da definição de serviço do sistema» (cláusula 5.5.6) e «Informação do serviço alargada» (cláusula 5.5.9) são utilizados para o efeito.

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

#### **Lista de serviços de confiança — política/advertência jurídica** (cláusula 5.3.11)

Este campo deve estar presente e estar conforme com as especificações da TS 119 612, cláusula 5.3.11, sendo a política/advertência jurídica sobre o estatuto jurídico do sistema ou os requisitos legais preenchidos pelo sistema na jurisdição em que está estabelecido e/ou eventuais restrições e condições sob as quais a lista de confiança é mantida e publicada

<sup>(1)</sup> ISO 3166-1:2006: «Códigos para a representação dos nomes dos países e suas subdivisões — Parte 1: Códigos dos países».

apresentada numa sequência de cadeias de caracteres multilingues (ver cláusula 5.1.4), com o inglês (Reino Unido) como língua obrigatória e eventualmente uma ou mais línguas nacionais, devendo o texto dessa política ou advertência incluir os seguintes elementos:

- (1) Uma primeira parte obrigatória, comum às listas de confiança de todos os Estados-Membros, indicando o quadro jurídico aplicável, e cuja versão inglesa é a seguinte:

«The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.»

Texto na(s) língua(s) nacional(is) dos Estados-Membros:

O quadro jurídico aplicável à presente lista de confiança é o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

- (2) Uma segunda parte, facultativa, específica de cada lista de confiança, indicando as referências aos quadros jurídicos nacionais específicos aplicáveis.

#### **Estatuto atual do serviço** (cláusula 5.5.4)

Este campo deve estar presente e estar conforme com as especificações da TS 119 612, cláusula 5.5.4.

A migração do «Estatuto atual do serviço» dos serviços enumerados na lista de confiança do Estados-Membros da UE no dia anterior à data em que o Regulamento (UE) n.º 910/2014 se aplica (isto é, 30 de junho de 2016) deve ser executado no dia em que o regulamento é aplicável (ou seja, 1 de julho de 2016), tal como especificados no anexo J da ETSI TS 119 612.

### CAPÍTULO III

#### **CONTINUIDADE DAS LISTAS DE CONFIANÇA**

Os certificados a notificar à Comissão, nos termos do artigo 4.º, n.º 2, da presente decisão devem satisfazer os requisitos da secção 5.7.1 da ETSI TS 119 612 e devem ser emitidos por forma a:

- apresentar, pelo menos, uma diferença de três meses no prazo de validade («Not After»);
- serem criados com base em novos pares de chaves. Os pares de chaves anteriormente utilizados não devem ser objeto de uma nova certificação.

Em caso de caducidade de uma das chaves públicas que poderiam ser utilizadas para validar a assinatura ou selo da lista de confiança que foi notificada à Comissão e está publicada nas listas centrais de apontadores da Comissão, os Estados-Membros devem:

- no caso de a lista de confiança publicada ter sido assinada ou selada com uma chave privada cujo certificado de chave pública tenha caducado, reemitir imediatamente uma nova lista de confiança assinada ou selada com uma chave privada cujo certificado de chave pública notificado não tenha caducado;
- se necessário, gerar novos pares de chaves que possam ser utilizados para assinar ou selar a lista de confiança e gerar os correspondentes certificados de chave pública;
- notificar imediatamente à Comissão a nova lista de certificados de chave pública correspondentes às chaves privadas que possam ser utilizadas para assinar ou selar a lista de confiança.

No caso de afetação ou anulação de uma das chaves privadas correspondentes a um dos certificados de chave pública que poderiam ser utilizados para validar a assinatura ou o selo da lista de confiança que foi notificada à Comissão e publicada nas listas centrais de apontadores da Comissão, os Estados-Membros devem:

- reemitir imediatamente uma nova lista de confiança assinada ou selada com uma chave privada não afetada nos casos em que a lista de confiança publicada tenha sido assinada com uma chave privada afetada ou anulada;



- se necessário, gerar novos pares de chaves que poderão ser utilizados para assinar ou selar a lista de confiança e gerar os correspondentes certificados de chave pública;
- notificar imediatamente à Comissão a nova lista de certificados de chave pública correspondentes às chaves privadas que poderiam ser utilizadas para assinar ou selar a lista de confiança.

No caso de afetação ou anulação de todas as chaves privadas correspondentes aos certificados de chave pública que possam ser utilizados para validar a assinatura da lista de confiança e que foi notificada à Comissão e publicada nas listas centrais de apontadores da Comissão, os Estados-Membros devem:

- gerar novos pares de chaves que possam ser utilizados para assinar ou selar a lista de confiança e gerar os correspondentes certificados de chave pública;
- reemitir imediatamente uma nova lista de confiança assinada ou selada 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 ou selar a lista de confiança.

#### CAPÍTULO IV

##### ESPECIFICAÇÕES DO FORMATO LEGÍVEL POR PESSOAS DA LISTA DE CONFIANÇA

Se for criado e publicado um formato legível por pessoas da lista aprovada, este deve ser apresentado sob a forma de um documento «*Portable Document Format*» (PDF), em conformidade com a norma ISO 32000 <sup>(1)</sup>, que deve ser formatado de acordo com o perfil PDF/A (norma ISO 19005) <sup>(2)</sup>.

O conteúdo do documento PDF/A com a lista de confiança em formato legível por pessoas deve satisfazer os seguintes requisitos:

- a estrutura do formato legível por pessoas deve refletir o modelo lógico descrito na TS 119612;
- todos os campos presentes devem ser visíveis e indicar:
  - o título do campo (por exemplo, «*Identificador do tipo de serviço*»),
  - o valor do campo (por exemplo, «<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>»),
  - o significado (descrição) do valor do campo, quando aplicável (por exemplo, «*Um serviço de geração de certificados que cria e assina certificados qualificados baseados na identidade e outros atributos verificados pelos serviços de registo competentes.*»),
- versões múltiplas em linguagens naturais, como previsto na lista de confiança, quando aplicável;
- devem ser visíveis no formulário em formato legível por pessoas, no mínimo, os seguintes campos e valores correspondentes dos certificados digitais <sup>(3)</sup>, se estiverem presentes no campo «*Identidade digital do serviço*»:
  - versão
  - número de série do certificado
  - algoritmo de assinatura
  - emitente — todos os campos do nome distinto
  - prazo de validade
  - pessoa em causa — todos os campos relevantes do nome distinto

<sup>(1)</sup> ISO 32000-1:2008: Gestão de documentos — «*Portable Document Format*» — Parte 1: PDF 1.7.

<sup>(2)</sup> 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)

<sup>(3)</sup> Recomendação ITU-T X.509 | ISO/IEC 9594-8: Tecnologia da informação — Interligação de Sistemas Abertos — Diretório: quadros do certificado de chave pública e atributos (ver <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>)

- chave pública
- identificador da chave da autoridade
- identificador da chave da pessoa em causa
- utilização da chave
- utilização alargada da chave
- políticas em matéria de certificado — todos os identificadores e qualificadores da política
- mapeamento da política
- nome alternativo da pessoa em causa
- atributos do diretório da pessoa em causa
- restrições da política
- condicionalismos da política
- pontos de distribuição CRL <sup>(1)</sup>
- acesso à informação da autoridade
- acesso à informação da pessoa em causa
- declarações dos certificados qualificados <sup>(2)</sup>
- algoritmo hash
- valor hash do certificado;
- o formato legível por pessoas deve ser fácil de imprimir;
- o formato legível por pessoas será assinado ou selado pelo operador do sistema de acordo com a assinatura avançada PDF especificada nos artigos 1.º e 3.º da Decisão de Execução (UE) 2015/1505 da Comissão.

---

---

<sup>(1)</sup> RFC 5280: Certificado Internet X.509 de infraestrutura de chave pública (PKI) e perfil CRL

<sup>(2)</sup> RFC 3739: Internet X.509 de infraestrutura de chave pública (PKI): características dos certificados qualificados.

## ANEXO II

**MODELO PARA AS NOTIFICAÇÕES DOS ESTADOS-MEMBROS**

As informações a notificar pelos Estados-Membros nos termos do artigo 4.º, n.º 1, da presente decisão, devem conter as seguintes informações, bem como as suas eventuais alterações:

- (1) Estado-Membro, utilizando os códigos da norma ISO 3166-1 <sup>(1)</sup> Alpha 2, com as seguintes exceções:
  - a) o código do Reino Unido será «UK»;
  - b) o código da Grécia será «EL».
- (2) O organismo ou organismos responsáveis por elaborar, manter e publicar a lista de confiança no formato adequado para tratamento automático e no formato legível por pessoas:
  - a) designação do operador do sistema: a informação fornecida deve ser idêntica — respeitar as maiúsculas e minúsculas — ao valor do parâmetro «Designação do operador do sistema» constante da lista de confiança, nas línguas aí utilizadas;
  - b) informação facultativa para utilização interna da Comissão apenas nos casos em que a entidade em questão deva ser contactada (esta informação não será publicada na lista compilada pela CE das listas de confiança):
    - endereço do operador do sistema,
    - contactos da(s) pessoa(s) responsável(eis) (nome, telefone, endereço de correio eletrónico).
- (3) Local onde a lista de confiança se encontra publicada em formato adequado para tratamento automático (*local onde se encontra publicada a lista de confiança em vigor*).
- (4) Local onde, quando aplicável, a lista de confiança se encontra publicada em formato legível por pessoas (*local onde se encontra publicada a lista de confiança em vigor*). Caso a lista de confiança já não seja publicada num formato legível por pessoas, indicar esse facto.
- (5) Os certificados de chave pública correspondentes às chaves privadas que podem ser utilizadas para assinar ou selar eletronicamente a lista de confiança no formato adequado para tratamento automático e no formato legível por pessoas: devem ser fornecidos como certificados *Privacy Enhanced Mail Base 64 encoded DER*. Em caso de alteração da notificação, de prestação de informações adicionais no caso de um novo certificado que substitui um certificado específico na lista da Comissão e no caso de o certificado notificado dever ser acrescentado ao(s) existente(s), sem qualquer substituição.
- (6) Data de apresentação dos dados notificados nos pontos (1) a (5).

Os dados notificados de acordo com os pontos (1), (2) (a), (3), (4) e (5) devem ser incluídos na lista compilada pela CE das listas de confiança, em substituição das informações anteriormente comunicadas incluídas nessa lista.

---

<sup>(1)</sup> ISO 3166-1: «Códigos para a representação dos nomes dos países e suas subdivisões — Parte 1: Códigos dos países».