Jornal Oficial da União Europeia

L 235

Edição em língua portuguesa

Legislação

58.º ano

9 de setembro de 2015

Índice

[1] Texto relevante para efeitos do EEE

PT

Os atos cujos títulos são impressos em tipo fino são atos de gestão corrente adotados no âmbito da política agrícola e que têm, em geral, um período de validade limitado.

Os atos cujos títulos são impressos em tipo negro e precedidos de um asterisco são todos os restantes.

[1] Texto relevante para efeitos do EEE

II

(Atos não legislativos)

REGULAMENTOS

REGULAMENTO DE EXECUÇÃO (UE) 2015/1501 DA COMISSÃO

de 8 de setembro de 2015

que estabelece o quadro de interoperabilidade, nos termos do artigo 12.º, n.º 8, 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 ([1]), nomeadamente o artigo 12.º, n.º 8,

Considerando o seguinte:

(1) O artigo 12.º, n.º 2, do Regulamento (UE) n.º 910/2014 prevê que deve ser estabelecido um quadro de interoperabilidade para efeitos da interoperabilidade dos sistemas nacionais de identificação eletrónica notificados nos termos do artigo 9.º, n.º 1, do referido regulamento.

(2) Os nós desempenham um papel central na interligação dos sistemas de identificação eletrónica dos Estados-Membros. O seu contributo é explicado na documentação relacionada com o Mecanismo Interligar a Europa criado pelo Regulamento (UE) n.º 1316/2013 do Parlamento Europeu e do Conselho ([2]), incluindo as funções e componentes do «nó eIDAS».

(3) Sempre que um Estado-Membro ou a Comissão forneça *software* para assegurar a autenticação de um nó explorado noutro Estado-Membro, a parte que fornece e atualiza o *software* utilizado no mecanismo de autenticação pode estabelecer por acordo com a parte que acolhe o *software* a forma como o funcionamento do mecanismo de autenticação será gerido. Este acordo não deve impor à parte que acolhe o *software* requisitos técnicos ou custos desproporcionados (incluindo o apoio, responsabilidades, alojamento e outras despesas).

(4) Na medida em que a aplicação do quadro de interoperabilidade o justifique, poderão ser elaboradas pela Comissão, em colaboração com os Estados-Membros, outras especificações técnicas que pormenorizem os requisitos técnicos estabelecidos no presente regulamento, em especial tendo em conta os pareceres da rede de cooperação referida no artigo 14.º, alínea d), da Decisão de Execução (UE) 2015/296 da Comissão ([3]). Estas especificações devem ser elaboradas como parte das infraestruturas de serviços digitais previstas no Regulamento (UE) n.º 1316/2013, que estabelece os meios para a aplicação prática de um elemento de identificação eletrónica.

([1]) JO L 257 de 28.8.2014, p. 73.

([2]) Regulamento (UE) n.º 1316/2013 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2013, que cria o Mecanismo Interligar a Europa, altera o Regulamento (UE) n.º 913/2010 e revoga os Regulamentos (CE) n.º 680/2007 e (CE) n.º 67/2010 (JO L 348 de 20.12.2013, p. 129).

([3]) Decisão de Execução (UE) 2015/296 da Comissão, de 24 de fevereiro de 2015, que estabelece as disposições processuais de cooperação entre Estados-Membros em matéria de identificação eletrónica nos termos do artigo 12.º, n.º 7, 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 (JO L 53 de 25.2.2015, p. 14).

(5) Os requisitos técnicos estabelecidos no presente regulamento devem ser aplicáveis não obstante eventuais alterações nas especificações técnicas que possam vir a ser elaboradas nos termos do artigo 12.º do presente regulamento.

(6) O projeto-piloto de grande escala STORK, incluindo as especificações aí desenvolvidas, e os princípios e conceitos do quadro europeu de interoperabilidade para os serviços públicos europeus foram tidos na máxima conta ao estabelecer as modalidades do quadro de interoperabilidade no presente regulamento.

(7) Os resultados da cooperação entre os Estados-Membros foram tidos na máxima conta.

(8) As medidas previstas no presente regulamento são conformes com o parecer do comité instituído pelo artigo 48.º do Regulamento (UE) n.º 910/2014,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Objeto

O presente regulamento estabelece os requisitos técnicos e operacionais do quadro de interoperabilidade, a fim de garantir a interoperabilidade dos sistemas de identificação eletrónica que os Estados-Membros notificam à Comissão.

Estes requisitos incluem, em especial:

a) Requisitos técnicos mínimos relacionados com os níveis de garantia e a correspondência entre os níveis de garantia nacionais dos meios de identificação eletrónica notificados emitidos no âmbito de sistemas de identificação eletrónica notificados nos termos do artigo 8.º do Regulamento (UE) n.º 910/2014, que são definidos nos artigos 3.º e 4.º;

b) Requisitos técnicos mínimos para a interoperabilidade, que são definidos nos artigos 5.º e 8.º;

c) O conjunto mínimo de dados de identificação que representam de modo único uma pessoa singular ou coletiva, que é definido no artigo 11.º e no anexo;

d) As normas comuns de segurança operacional, que são definidas nos artigos 6.º, 7.º, 9.º e 10.º;

e) As modalidades de resolução de litígios, que são definidas no artigo 13.º.

Artigo 2.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Nó», um ponto de ligação que faz parte da arquitetura da interoperabilidade da identificação eletrónica e que participa na autenticação transfronteiriça de pessoas, tendo capacidade para reconhecer e tratar ou transmitir comunicações de ou para outros nós, permitindo às infraestruturas de identificação eletrónica nacionais de um Estado-Membro interagirem com as infraestruturas de identificação eletrónica de outros Estados-Membros;

2) «Operador do nó», a entidade responsável por assegurar que o nó funciona corretamente e realiza de forma fiável as suas funções de ponto de ligação.

Artigo 3.º

Requisitos técnicos mínimos relacionados com os níveis de garantia

Os requisitos técnicos mínimos relacionados com os níveis de garantia são definidos no Regulamento de Execução (UE) 2015/1502 da Comissão ([1]).

Artigo 4.º

Recenseamento dos níveis de garantia nacionais

O recenseamento dos níveis de garantia nacionais dos sistemas de identificação eletrónica notificados deve satisfazer os requisitos estabelecidos no Regulamento de Execução (UE) 2015/1502 da Comissão. Os resultados do recenseamento devem ser notificados à Comissão, utilizando o modelo de notificação definido na Decisão de Execução (UE) 2015/1505 da Comissão ([2]).

Artigo 5.º

Nós

1. O nó de um Estado-Membro deve poder ligar-se aos nós de outros Estados-Membros.

2. Os nós devem ser capazes de distinguir entre os organismos do setor público e as outras partes utilizadoras através de meios técnicos.

3. A aplicação por um Estado-Membro dos requisitos técnicos estabelecidos no presente regulamento não pode impor requisitos técnicos ou custos desproporcionados a outros Estados-Membros para que estes possam interagir com o sistema adotado pelo primeiro.

Artigo 6.º

Privacidade e confidencialidade dos dados

1. A proteção da vida privada e da confidencialidade dos dados trocados e a conservação da integridade dos dados entre os nós devem ser garantidas mediante a utilização das melhores soluções técnicas e práticas de proteção disponíveis.

2. Os nós não devem armazenar quaisquer dados pessoais, exceto para os fins previstos no artigo 9.º, n.º 3.

Artigo 7.º

Integridade e autenticidade dos dados a comunicar

A comunicação entre os nós deve assegurar a integridade e autenticidade dos dados de forma a garantir que todos os pedidos e respostas são autênticos e não foram manipulados. Para o efeito, devem utilizar as soluções que foram aplicadas com êxito na utilização operacional transfronteiriça.

([1]) Regulamento de Execução (UE) 2015/1502 da Comissão, de 8 de setembro de 2015, que estabelece as especificações técnicas mínimas e os procedimentos para a atribuição dos níveis de garantia dos meios de identificação eletrónica, nos termos do artigo 8.º, n.º 3, 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 (ver página 7 do presente Jornal Oficial).

([2]) 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 (ver página 26 do presente Jornal Oficial).

Artigo 8.º

Formato das mensagens para a comunicação

Os nós devem utilizar uma sintaxe comum de formatos de mensagem baseados em normas que já foram utilizadas mais do que uma vez entre os Estados-Membros e que deram provas de funcionalidade num ambiente operacional. A sintaxe deve permitir:

a) O tratamento adequado do conjunto mínimo de dados de identificação que representam de modo único uma pessoa singular ou coletiva;

b) O tratamento adequado do nível de garantia dos meios de identificação eletrónica;

c) A distinção entre os organismos do setor público e as outras partes utilizadoras;

d) A flexibilidade para responder às necessidades de atributos adicionais de identificação.

Artigo 9.º

Gestão da segurança da informação e metadados

1. O operador do nó deve comunicar os metadados de gestão do nó num formato normalizado que permita o tratamento automatizado e de um modo seguro e fiável.

2. No mínimo, os parâmetros relevantes para a segurança devem ser tratados automaticamente.

3. O operador do nó deve armazenar os dados que, em caso de incidente, permitam a reconstrução da sequência da troca de mensagens por forma a determinar o local e a natureza do incidente. Os dados são armazenados durante um período de tempo de acordo com os requisitos nacionais e, no mínimo, devem conter os seguintes elementos:

a) Identificação do nó;

b) Identificação da mensagem;

c) Data e hora da mensagem.

Artigo 10.º

Normas de garantia e segurança da informação

1. Os operadores de nós que prestam serviços de autenticação devem provar que, relativamente aos nós que participam no quadro de interoperabilidade, o seu nó cumpre os requisitos da norma ISO/IEC 27001 através da certificação ou de métodos equivalentes de avaliação ou de acordo com a legislação nacional.

2. Os operadores de nós devem proceder às atualizações críticas de segurança sem demora injustificada.

Artigo 11.º

Dados de identificação pessoal

1. O conjunto mínimo de dados de identificação que representam de modo único uma pessoa singular ou coletiva deve cumprir os requisitos estabelecidos no anexo, quando utilizado num contexto transfronteiriço.

2. O conjunto mínimo de dados para uma pessoa singular que represente uma pessoa coletiva deve incluir a combinação dos atributos enumerados no anexo para as pessoas singulares e para as pessoas coletivas, quando utilizado num contexto transfronteiriço.

3. Os dados devem ser transmitidos com base nos carateres originais e, quando adequado, também com a sua transliteração em carateres latinos.

Artigo 12.º

Especificações técnicas

1. Quando o processo de aplicação do quadro de interoperabilidade o justifique, a rede de cooperação estabelecida pela Decisão de Execução (UE) 2015/296 pode emitir pareceres ao abrigo do artigo 14.º, alínea d), sobre a necessidade de elaborar especificações técnicas. Essas especificações técnicas devem fornecer informações mais pormenorizadas sobre os requisitos técnicos estabelecidos no presente regulamento.

2. Nos termos do parecer referido no n.º 1, a Comissão, em cooperação com os Estados-Membros, deve elaborar as especificações técnicas como parte das infraestruturas de serviços digitais do Regulamento (UE) n.º 1316/2013.

3. A rede de cooperação deve emitir um parecer nos termos do artigo 14.º, alínea d), da Decisão de Execução (UE) 2015/296, em que avalia se, e em que medida, as especificações técnicas elaboradas nos termos do n.º 2 correspondem às necessidades identificadas no parecer referido no n.º 1, ou cumprem os requisitos estabelecidos no presente regulamento. A rede de cooperação pode recomendar que os Estados-Membros tomem em conta as especificações técnicas ao aplicarem o quadro de interoperabilidade.

4. A Comissão deve fornecer uma aplicação de referência como um exemplo de interpretação das especificações técnicas. Os Estados-Membros podem aplicar esta aplicação de referência ou utilizá-la como amostra quando se testam outras aplicações das especificações técnicas.

Artigo 13.º

Resolução de litígios

1. Sempre que possível, quaisquer litígios relativos ao quadro de interoperabilidade devem ser resolvidos pelos Estados-Membros em causa através de negociações.

2. Se não se alcançar a uma solução em conformidade com o disposto no n.º 1, a rede de cooperação estabelecida pela Decisão de Execução (UE) 2015/296 terá competência para resolver o litígio em conformidade com o seu regulamento interno.

Artigo 14.º

Entrada em vigor

O presente regulamento 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

Requisitos relativos ao conjunto mínimo de dados de identificação que representem de modo único uma pessoa singular ou coletiva referido no artigo 11.º

1. **Conjunto mínimo de dados para uma pessoa singular**

O conjunto mínimo de dados para uma pessoa singular deve conter obrigatoriamente todas as seguintes características:

a) Apelido(s) atual(is);

b) Nome(s) próprio(s) atual(is);

c) Data de nascimento;

d) Um identificador único atribuído pelo Estado-Membro de expedição, conforme com as especificações técnicas para efeitos de identificação transfronteiriça e tão persistente quanto possível no tempo.

O conjunto mínimo de dados para uma pessoa singular pode conter uma ou mais das seguintes características:

a) Nome(s) próprio(s) e apelido(s) de nascimento;

b) Local de nascimento;

c) Endereço atual;

d) Sexo.

2. **Conjunto mínimo de dados para uma pessoa coletiva**

O conjunto mínimo de dados para uma pessoa coletiva deve conter obrigatoriamente todas as seguintes características:

a) Denominação oficial atual;

b) Um identificador único atribuído pelo Estado-Membro de expedição, conforme com as especificações técnicas para efeitos de identificação transfronteiriça e tão persistente quanto possível no tempo.

O conjunto mínimo de dados para uma pessoa coletiva pode conter uma ou mais das seguintes características:

a) Endereço atual;

b) Número do IVA;

c) Número de identificação fiscal;

d) O identificador relacionado com o artigo 3.º, n.º 1, da Diretiva 2009/101/CE do Parlamento Europeu e do Conselho ([1]);

e) Identificador de pessoa jurídica a que se refere o Regulamento de Execução (UE) n.º 1247/2012 da Comissão ([2]);

f) Número de registo de operador económico (EORI) a que se refere o Regulamento de Execução (UE) n.º 1352/2013 da Comissão ([3]);

g) Número de imposto especial de consumo previsto no artigo 2.º, n.º 12, do Regulamento (UE) n.º 389/2012 do Conselho ([4]).

([1]) Diretiva 2009/101/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, tendente a coordenar as garantias que, para proteção dos interesses dos sócios e de terceiros, são exigidas nos Estados-Membros às sociedades, na aceção do segundo parágrafo do artigo 48.º do Tratado, a fim de tornar equivalentes essas garantias em toda a Comunidade (JO L 258 de 1.10.2009, p. 11).

([2]) Regulamento de Execução (UE) n.º 1247/2012 da Comissão, de 19 de dezembro de 2012, que estabelece as normas técnicas de execução no que se refere ao formato e à periodicidade dos relatórios de transações a transmitir aos repositórios de transações nos termos do Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações (JO L 352 de 21.12.2012, p. 20).

([3]) Regulamento de Execução (UE) n.º 1352/2013 da Comissão, de 4 de dezembro de 2013, que estabelece os formulários previstos no Regulamento (UE) n.º 608/2013 do Parlamento Europeu e do Conselho relativo à intervenção das autoridades aduaneiras para assegurar o cumprimento da legislação sobre os direitos de propriedade intelectual (JO L 341 de 18.12.2013, p. 10).

([4]) Regulamento (UE) n.º 389/2012 do Conselho, de 2 de maio de 2012, relativo à cooperação administrativa no domínio dos impostos especiais de consumo e que revoga o Regulamento (CE) n.º 2073/2004 (JO L 121 de 8.5.2012, p. 1).

REGULAMENTO DE EXECUÇÃO (UE) 2015/1502 DA COMISSÃO

de 8 de setembro de 2015

que estabelece as especificações técnicas mínimas e os procedimentos para a atribuição dos níveis de garantia dos meios de identificação eletrónica, nos termos do artigo 8.º, n.º 3, 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 ([1]), nomeadamente o artigo 8.º, n.º 3,

Considerando o seguinte:

(1) O artigo 8.º do Regulamento (UE) n.º 910/2014 prevê que os sistemas de identificação eletrónica notificados nos termos do artigo 9.º, n.º 1, especifiquem os níveis de garantia reduzido, substancial e elevado para os meios de identificação eletrónica neles produzidos.

(2) É essencial definir as especificações técnicas mínimas, as normas e os procedimentos aplicáveis, a fim de assegurar um entendimento comum dos elementos dos níveis de garantia, bem como a sua interoperabilidade, ao recensear os níveis de garantia nacionais dos sistemas de identificação eletrónica notificados relativamente aos níveis de garantia previstos no artigo 8.º, tal como previsto no artigo 12.º, n.º 4, alínea b), do Regulamento (UE) n.º 910/2014.

(3) A norma internacional ISO/IEC 29115 foi tida em consideração para as especificações e procedimentos previstos no presente ato de execução, dado que se trata da principal norma internacional existente no domínio dos níveis de segurança dos meios de identificação eletrónica. No entanto, o conteúdo do Regulamento (UE) n.º 910/2014 difere da norma internacional, em especial no que diz respeito aos requisitos de prova e verificação da identidade, bem como quanto à forma como as diferentes modalidades de identidade dos Estados-Membros e os instrumentos existentes na UE para esse efeito são tidos em consideração. Por conseguinte, embora o anexo nela se baseie, não deve fazer referência a qualquer conteúdo concreto da norma internacional ISO/IEC 29115.

(4) O presente regulamento foi concebido numa abordagem devidamente baseada nos resultados, o que também se reflete nas definições utilizadas para especificar os termos e conceitos. Estes têm em conta o objetivo do Regulamento (UE) n.º 910/2014 em relação aos níveis de segurança dos meios de identificação eletrónica. Por conseguinte, o projeto-piloto de grande escala STORK, incluindo as especificações aí desenvolvidas, bem como as definições e conceitos da norma ISO/IEC 29115, devem ser tidos na máxima conta ao estabelecer as especificações e procedimentos previstos no presente ato de execução.

(5) Em função do contexto em que um elemento de prova de identidade tem de ser verificado, as fontes qualificadas podem assumir muitas formas, nomeadamente registos, documentos ou organismos. As fontes qualificadas que podem ser diferentes nos diversos Estados-Membros, mesmo num contexto semelhante.

(6) Os requisitos de prova e verificação da identidade devem ter em conta os diferentes sistemas e práticas, assegurando simultaneamente um grau de garantia suficientemente elevado para estabelecer a confiança necessária. Portanto, a aceitação dos procedimentos utilizados anteriormente para outros fins que não a produção de meios de identificação eletrónica deve estar subordinada à confirmação de que esses procedimentos cumprem os requisitos previstos para o nível de garantia correspondente.

([1]) JO L 257 de 28.8.2014, p. 73.

(7) Em geral são utilizados certos fatores de autenticação, como a partilha de segredos comerciais, dispositivos físicos e atributos físicos. No entanto, a utilização de um maior número de fatores de autenticação, em especial de diferentes categorias, deve ser incentivada para aumentar a segurança do processo de autenticação.

(8) O presente regulamento não deve afetar os direitos de representação das pessoas coletivas. No entanto, o anexo deve prever os requisitos para a ligação entre os meios de identificação eletrónica de pessoas singulares e coletivas.

(9) A importância da segurança da informação e dos sistemas de gestão de serviços deve ser reconhecida, tal como deve ser reconhecida a importância do emprego de metodologias reconhecidas e da aplicação dos princípios consagrados em normas como a ISO/IEC 27000 e a série de normas ISO/IEC 20000.

(10) As boas práticas relativamente aos níveis de garantia nos Estados-Membros também devem ser tidas em conta.

(11) A certificação de segurança informática baseada em normas internacionais é um instrumento importante para verificar a conformidade dos produtos com os requisitos previstos no presente ato de execução.

(12) O Comité referido no artigo 48.º do Regulamento (UE) n.º 910/2014 não emitiu um parecer no prazo estipulado pela respetiva presidência,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

1. Os níveis de garantia reduzido, substancial e elevado dos meios de identificação eletrónica produzidos no âmbito de um sistema de identificação eletrónica notificado são determinados com base nas especificações e procedimentos definidos no anexo.

2. As especificações e procedimentos definidos no anexo devem ser utilizados para especificar o nível de garantia dos meios de identificação eletrónica produzidos no âmbito de um sistema de identificação eletrónica notificado, para determinar a confiança e qualidade dos seguintes elementos:

a) A inscrição, conforme definida no ponto 2.1 do anexo do presente regulamento, em conformidade com o artigo 8.º, n.º 3, alínea a), do Regulamento (UE) n.º 910/2014;

b) A gestão dos meios de identificação eletrónica, conforme definida no ponto 2.2 do anexo do presente regulamento, em conformidade com o artigo 8.º, n.º 3, alíneas b) e f), do Regulamento (UE) n.º 910/2014;

c) A autenticação, conforme definida no ponto 2.3 do anexo do presente regulamento, em conformidade com o artigo 8.º, n.º 3, alínea c), do Regulamento (UE) n.º 910/2014;

d) A gestão e organização, conforme definidas no ponto 2.4 do anexo do presente regulamento, em conformidade com o artigo 8.º, n.º 3, alíneas d) e e), do Regulamento (UE) n.º 910/2014.

3. Quando os meios de identificação eletrónica produzidos no âmbito de um sistema de identificação eletrónica notificado cumprirem os requisitos do nível de garantia mais elevado, presume-se que cumprem os requisitos equivalentes de um nível de garantia inferior.

4. Salvo indicação em contrário na parte relevante do anexo, todos os elementos enumerados no anexo para um determinado nível de garantia do meio de identificação eletrónica produzido no âmbito de um sistema de identificação eletrónica notificado devem ser cumpridos para se atingir o nível de garantia em questão.

Artigo 2.º

O presente regulamento 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

Especificações técnicas e procedimentos para a atribuição dos níveis de garantia reduzido, substancial e elevado dos meios de identificação eletrónica produzidos no âmbito de um sistema de identificação eletrónica notificado

1. Definições aplicáveis

Para efeitos do presente anexo, entende-se por:

1) «Fonte qualificada», qualquer fonte, independentemente da sua forma, que pode ser considerada fiável para fornecer dados exatos, informações e/ou elementos de prova que podem ser utilizados para comprovar a identidade;

2) «Fator de autenticação», um elemento confirmado como ligado a uma pessoa, que se enquadra numa das seguintes categorias:

   a) «Fator de autenticação baseado na posse», um fator de autenticação em que a pessoa em causa tem de provar a sua posse;

   b) «Fator de autenticação baseado no conhecimento», um fator de autenticação em que a pessoa em causa tem de demonstrar o conhecimento do mesmo;

   c) «Fator de autenticação inerente», um fator de autenticação que tem por base um atributo físico de uma pessoa singular, que a pessoa em causa tem de demonstrar possuir;

3) «Autenticação dinâmica», um processo eletrónico que utiliza criptografia ou outras técnicas para fornecer um meio de criar a pedido uma prova eletrónica de que a pessoa em causa controla ou tem na sua posse os dados de identificação e que se altera com cada autenticação entre a pessoa em causa e o sistema que verifica a sua identidade;

4) «Sistema de gestão da segurança das informações», um conjunto de processos e procedimentos destinados a garantir níveis aceitáveis de riscos associados à segurança da informação.

2. Especificações técnicas e procedimentos

Os elementos das especificações técnicas e procedimentos descritos no presente anexo devem ser utilizados para determinar a forma como os requisitos e critérios estabelecidos no artigo 8.º do Regulamento (UE) n.º 910/2014 devem ser aplicados aos meios de identificação eletrónica produzidos por um sistema de identificação eletrónica.

2.1. *Inscrição*

2.1.1. Pedido e registo

Nível de garantia	Elementos necessários
Reduzido	1. Assegurar que o requerente tem conhecimento dos termos e condições relacionados com a utilização dos meios de identificação eletrónica. 2. Assegurar que o requerente tem conhecimento das precauções recomendadas relativamente à utilização dos meios de identificação eletrónica. 3. Recolher os dados de identificação necessários para a prova e verificação da identidade.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.1.2. Prova e verificação da identidade (pessoa singular)

Nível de garantia	Elementos necessários
Reduzido	1. Pode considerar-se que a pessoa está na posse de elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica e que representam a identidade declarada. 2. Pode considerar-se que os elementos de prova são genuínos, ou que são conformes com uma fonte qualificada e parecem ser válidos. 3. Sabe-se, de acordo com uma fonte qualificada, que a identidade declarada existe e pode presumir-se que a pessoa que declara a identidade é a própria.
Substancial	Idênticos ao nível reduzido, acrescidos de uma das alternativas enumeradas nos pontos 1 a 4: 1. Verificou-se que a pessoa está na posse de elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica e que representam a identidade declarada e Os elementos de prova são controlados para verificar se são genuínos; ou, de acordo com uma fonte qualificada, sabe-se que existem e que se referem a uma pessoa real e Foram tomadas medidas para minimizar o risco de que a identidade da pessoa não seja a identidade declarada, tendo em conta, por exemplo, o risco de apresentação de elementos de prova perdidos, roubados, suspensos, revogados ou caducados; ou 2. Um documento de identidade é apresentado durante um processo de registo no Estado-Membro em que o documento foi emitido e o documento parece dizer respeito à pessoa que o apresenta e Foram tomadas medidas para minimizar o risco de que a identidade da pessoa não seja a identidade declarada, tendo em conta, por exemplo, o risco de apresentação de documentos perdidos, roubados, suspensos, revogados ou caducados; ou 3. Quando os procedimentos anteriormente utilizados no mesmo Estado-Membro por uma entidade pública ou privada, para outros fins que não a produção de meios de identificação eletrónica, assegurarem um nível de garantia equivalente ao estabelecido no ponto 2.1.2 para o nível garantia substancial, a entidade competente para o registo não tem de repetir esses procedimentos anteriores, desde que essa garantia equivalente seja confirmada por um organismo de avaliação da conformidade referido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho ([1]), ou por um organismo equivalente; ou 4. Nos casos em que são produzidos meios de identificação eletrónica com base em meios de identificação eletrónica válidos com um nível de garantia substancial ou elevado, e tendo em conta o risco de uma alteração dos dados de identificação pessoal, não é necessário repetir os processos de prova e verificação da identidade. Se os meios de identificação eletrónica que servem de base não tiverem sido notificados, o nível de garantia substancial ou elevado deve ser confirmado por um organismo de avaliação da conformidade a que se refere o artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, ou por um órgão equivalente.

Nível de garantia	Elementos necessários
Elevado	Têm de ser respeitados os requisitos do ponto 1 ou 2: 1. Idênticos ao nível substancial, acrescidos de uma das alternativas enumeradas nos pontos a) a c): a) Nos casos em que se verifique que a pessoa está na posse de elementos de identificação com fotografia ou dados biométricos reconhecidos pelo Estado-Membro em que se efetua o pedido de identidade eletrónica, e que os elementos de prova representem a identidade declarada, os elementos de prova são controlados para verificar se esta é válida de acordo com uma fonte qualificada; e O requerente é identificado com a identidade declarada através da comparação de uma ou mais características físicas da pessoa com uma fonte qualificada; ou b) Quando os procedimentos anteriormente utilizados no mesmo Estado-Membro por uma entidade pública ou privada, para outros fins que não a produção de meios de identificação eletrónica, assegurarem um nível de garantia equivalente ao estabelecido no ponto 2.1.2 para o nível garantia elevado, a entidade competente para o registo não tem de repetir esses procedimentos anteriores, desde que essa garantia equivalente seja confirmada por um organismo de avaliação da conformidade referido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, ou por um organismo equivalente; e Foram tomadas medidas para demonstrar que os resultados dos procedimentos anteriores continuam a ser válidos; ou c) Nos casos em que são produzidos meios de identificação eletrónica com base em meios de identificação eletrónica válidos com um nível de garantia elevado, e tendo em conta o risco de uma alteração dos dados de identificação pessoal, não é necessário repetir os processos de prova e verificação da identidade. Se os meios de identificação eletrónica que servem de base não tiverem sido notificados, o nível de garantia elevado deve ser confirmado por um organismo de avaliação da conformidade a que se refere o artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, ou por um órgão equivalente. e Foram tomadas medidas para demonstrar que os resultados do anterior procedimento de emissão de um meio de identificação eletrónica notificado continuam válidos. OU 2. Se o requerente não apresentar quaisquer elementos de identificação reconhecidos com fotografia ou dados biométricos, são aplicados os mesmos procedimentos utilizados a nível nacional no Estado-Membro da entidade responsável pelo registo para obter tais elementos de identificação reconhecidos com fotografia ou dados biométricos.

(1) Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30).

2.1.3. Prova e verificação da identidade (pessoa coletiva)

Nível de garantia	Elementos necessários
Reduzido	1. A identidade declarada é demonstrada com base em elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica.

Nível de garantia	Elementos necessários
	2. Os elementos de prova aparentam ser válidos e genuínos, ou presume-se a sua existência de acordo com uma fonte qualificada, quando a inclusão de uma pessoa coletiva na fonte autorizada é voluntária e está regulamentada por um acordo entre a pessoa coletiva e a fonte qualificada. 3. A pessoa coletiva não é reconhecida por uma fonte qualificada com um estatuto que a impeça de atuar como pessoa coletiva.
Substancial	Idênticos ao nível reduzido, acrescidos de uma das alternativas enumeradas nos pontos 1 a 3: 1. A identidade da pessoa coletiva declarada é demonstrada com base em elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica, incluindo a designação da pessoa coletiva, a forma jurídica e (quando aplicável) o número de registo. e Os elementos de prova são analisados a fim de determinar a sua autenticidade, ou se a sua existência é conhecida em conformidade com uma fonte qualificada, quando a inclusão da pessoa coletiva na fonte qualificada é uma condição para a pessoa coletiva exercer a atividade no seu setor e Foram tomadas medidas para minimizar o risco de que a identidade da pessoa coletiva não seja a identidade declarada, tendo em conta, por exemplo, o risco de apresentação de documentos perdidos, roubados, suspensos, revogados ou caducados; ou 2. Quando os procedimentos anteriormente utilizados no mesmo Estado-Membro por uma entidade pública ou privada, para outros fins que não a produção de meios de identificação eletrónica, assegurarem um nível de garantia equivalente ao estabelecido no ponto 2.1.3 para o nível garantia substancial, a entidade competente para o registo não tem de repetir esses procedimentos anteriores, desde que essa garantia equivalente seja confirmada por um organismo de avaliação da conformidade referido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008 ou por um organismo equivalente; ou 3. Nos casos em que são produzidos meios de identificação eletrónica com base em meios de identificação eletrónica válidos com um nível de garantia substancial ou elevado, não é necessário repetir os processos de prova e verificação da identidade. Se os meios de identificação eletrónica que servem de base não tiverem sido notificados, o nível de garantia substancial ou elevado deve ser confirmado por um organismo de avaliação da conformidade a que se refere o artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, ou por um órgão equivalente.
Elevado	Idênticos ao nível substancial, acrescidos de uma das alternativas enumeradas nos pontos 1 a 3: 1. A identidade da pessoa coletiva declarada é demonstrada com base em elementos de prova reconhecidos pelo Estado-Membro em que se efetua o pedido de meios de identidade eletrónica, incluindo a designação da pessoa coletiva, a forma jurídica e, pelo menos, um identificador único que represente a pessoa coletiva, utilizado num contexto nacional. e Os elementos de prova são controlados para verificar a sua validade de acordo com uma fonte qualificada; ou

Nível de garantia	Elementos necessários
	2. Quando os procedimentos anteriormente utilizados no mesmo Estado-Membro por uma entidade pública ou privada, para outros fins que não a produção de meios de identificação eletrónica, assegurarem um nível de garantia equivalente ao estabelecido no ponto 2.1.3 para o nível garantia elevado, a entidade competente para o registo não tem de repetir esses procedimentos anteriores, desde que essa garantia equivalente seja confirmada por um organismo de avaliação da conformidade referido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008 ou por um organismo equivalente; e Foram tomadas medidas para demonstrar que os resultados dos procedimentos anteriores continuam a ser válidos; ou 3. Nos casos em que são produzidos meios de identificação eletrónica com base em meios de identificação eletrónica válidos com um nível de garantia elevado, não é necessário repetir os processos de prova e verificação da identidade. Se os meios de identificação eletrónica que servem de base não tiverem sido notificados, o nível de garantia elevado deve ser confirmado por um organismo de avaliação da conformidade a que se refere o artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, ou por um órgão equivalente. e Foram tomadas medidas para demonstrar que os resultados do anterior procedimento de emissão de um meio de identificação eletrónica notificado continuam válidos.

2.1.4. Ligação entre os meios de identificação eletrónica de pessoas singulares e coletivas

Se for caso disso, são aplicáveis as seguintes condições à ligação entre o meios de identificação eletrónica de uma pessoa singular e os meios de identificação eletrónica de uma pessoa coletiva («ligação»):

1) É possível suspender e/ou revogar uma ligação. O ciclo de vida de uma ligação (por exemplo, ativação, suspensão, renovação, revogação) é gerido de acordo com os procedimentos reconhecidos a nível nacional.

2) A pessoa singular cujos meios de identificação eletrónica estão ligados aos meios de identificação eletrónica da pessoa coletiva pode delegar o exercício da ligação noutra pessoa singular com base em procedimentos reconhecidos a nível nacional. No entanto, a pessoa singular que efetua a delegação permanecerá responsável.

3) A ligação efetua-se do seguinte modo:

Nível de garantia	Elementos necessários
Reduzido	1. A prova de identidade da pessoa singular que age em nome da pessoa coletiva é verificada como tendo sido realizada com um nível de garantia reduzido ou superior. 2. A ligação foi estabelecida com base nos procedimentos reconhecidos a nível nacional. 3. A pessoa singular não é reconhecida por uma fonte qualificada com um estatuto que a impeça de agir em nome da pessoa coletiva.
Substancial	Ponto 3 do nível reduzido, acrescido de: 1. A prova de identidade da pessoa singular que age em nome da pessoa coletiva é verificada como tendo sido realizada com um nível de garantia substancial ou elevado.

Nível de garantia	Elementos necessários
	2. A ligação foi estabelecida com base nos procedimentos reconhecidos a nível nacional, o que resultou na inscrição da ligação numa fonte qualificada. 3. A ligação foi verificada com base nas informações provenientes de uma fonte qualificada.
Elevado	Ponto 3 do nível reduzido e ponto 2 do nível substancial, acrescido de: 1. A prova de identidade da pessoa singular que age em nome da pessoa coletiva é verificada como tendo sido realizada com um nível de garantia elevado. 2. A ligação foi verificada com base num identificador único que representa a pessoa coletiva, utilizado no contexto nacional; e, com base nas informações de uma fonte qualificada que representam de modo único uma pessoa singular.

2.2. *Gestão dos meios de identificação eletrónica*

2.2.1. Características e configuração dos meios de identificação eletrónica

Nível de garantia	Elementos necessários
Reduzido	1. Os meios de identificação eletrónica utilizam, pelo menos, um fator de autenticação. 2. Os meios de identificação eletrónica são concebidos de modo a assegurar que o emitente toma as medidas razoáveis para verificar que só são utilizados sob o controlo ou na posse da pessoa a que pertencem.
Substancial	1. Os meios de identificação eletrónica utilizam, pelo menos, dois fatores de autenticação de diferentes categorias. 2. Os meios de identificação eletrónica são concebidos de modo a permitir presumir que só são utilizados sob o controlo ou na posse da pessoa a que pertencem.
Elevado	Nível substancial, acrescido de: 1. O meio de identificação eletrónica protege contra a duplicação e a manipulação, bem como contra ataques de elevado potencial 2. O meio de identificação eletrónica é concebido de forma a poder ser eficazmente protegido pela pessoa a que pertence contra a utilização por terceiros.

2.2.2. Emissão, entrega e ativação

Nível de garantia	Elementos necessários
Reduzido	Após a emissão, os meios de identificação eletrónica são entregues através de um mecanismo que permite presumir que só chegam à pessoa a que se destinam.
Substancial	Após a emissão, os meios de identificação eletrónica são entregues através de um mecanismo que permite presumir que só ficam na posse da pessoa a que pertencem.
Elevado	O processo de ativação verifica se os meios de identificação eletrónica foram entregues e ficaram na posse da pessoa a que pertencem.

2.2.3. Suspensão, revogação e reativação

Nível de garantia	Elementos necessários
Reduzido	1. É possível suspender e/ou revogar um meio de identificação eletrónica de uma forma atempada e eficaz. 2. Foram tomadas medidas para impedir a sua revogação, suspensão e/ou reativação não autorizadas. 3. A reativação só terá lugar se os mesmos requisitos de garantia estabelecidos antes da suspensão ou revogação continuarem a verificar-se.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.2.4. Renovação e substituição

Nível de garantia	Elementos necessários
Reduzido	Tendo em conta o risco de alteração dos dados de identificação pessoal, a renovação ou substituição devem cumprir os mesmos requisitos de garantia do processo inicial de prova e verificação da identidade, ou basear-se num meio de identificação eletrónica válido do mesmo nível de garantia ou superior.
Substancial	Idênticos ao nível reduzido.
Elevado	Nível reduzido, acrescido de: Em caso de renovação ou substituição com base num meio de identificação eletrónica válido, os dados de identificação são verificados junto de uma fonte qualificada.

2.3. *Autenticação*

Esta secção debruça-se sobre os perigos associados à utilização do mecanismo de autenticação e enumera os requisitos para cada nível de garantia. As verificações previstas nesta secção devem ser entendidas como proporcionais aos riscos de determinado nível de garantia.

2.3.1. Mecanismo de autenticação

O quadro seguinte apresenta os requisitos por nível de garantia relativos ao mecanismo de autenticação, através do qual a pessoa singular ou coletiva utiliza o meio de identificação eletrónica para confirmar a sua identidade perante um utilizador.

Nível de garantia	Elementos necessários
Reduzido	1. A introdução dos dados de identificação pessoal é precedida por uma verificação fiável dos meios de identificação eletrónica e da sua validade. 2. Nos casos em que os dados de identificação pessoal são armazenados no quadro do mecanismo de autenticação, essas informações devem ser securizadas de modo a assegurar a sua proteção contra as perdas e fuga, incluindo a análise fora de linha. 3. O mecanismo de autenticação executa controlos de segurança para a verificação dos meios de identificação eletrónica, de forma a que seja altamente improvável que atividades como a adivinhação, escutas não autorizadas, reprodução ou manipulação de comunicações por um intruso com capacidade de ataque básica-reforçada possa subverter os mecanismos de autenticação.

Nível de garantia	Elementos necessários
Substancial	Nível reduzido, acrescido de: 1. A introdução dos dados de identificação pessoal é precedida por uma verificação fiável dos meios de identificação eletrónica e da sua validade através de uma autenticação dinâmica. 2. O mecanismo de autenticação executa controlos de segurança para a verificação dos meios de identificação eletrónica, de forma a que seja altamente improvável que atividades como a adivinhação, escutas não autorizadas, reprodução ou manipulação de comunicações por um intruso com capacidade de ataque moderada possa subverter os mecanismos de autenticação.
Elevado	Nível substancial, acrescido de: O mecanismo de autenticação executa controlos de segurança para a verificação dos meios de identificação eletrónica, de forma a que seja altamente improvável que atividades como a adivinhação, escutas não autorizadas, reprodução ou manipulação de comunicações por um intruso com capacidade de ataque elevada possa subverter os mecanismos de autenticação.

2.4. *Gestão e organização*

Todos os participantes que prestam um serviço relacionado com a identificação eletrónica num contexto transfronteiriço (a seguir designados «prestadores») devem dispor de práticas documentadas de gestão da segurança da informação, políticas e abordagens em matéria de gestão do risco e outros controlos reconhecidos que ofereçam garantias aos órgãos de gestão responsáveis pelos sistemas de identificação eletrónica dos respetivos Estados-Membros de que estão em vigor práticas eficazes. Ao longo de toda a secção 2.4, todos os requisitos/ /elementos devem ser entendidos como proporcionais aos riscos de determinado nível.

2.4.1. Disposições gerais

Nível de garantia	Elementos necessários
Reduzido	1. Os prestadores de serviços operacionais abrangidos pelo presente regulamento são uma autoridade pública ou uma entidade jurídica reconhecida como tal pelo direito nacional de um Estado-Membro, com uma organização estabelecida e plenamente operacional em todas as partes relevantes para a prestação dos serviços. 2. Os prestadores têm de cumprir todos os requisitos legais que lhes incumbem no âmbito da operação e prestação dos serviços, incluindo os tipos de informações que podem ser solicitadas, a forma como a verificação da identidade é realizada, o tipo de informações que podem ser conservadas e durante quanto tempo. 3. Os prestadores devem poder demonstrar a sua capacidade para assumirem os riscos decorrentes da responsabilidade por danos, bem como dispor dos recursos financeiros suficientes para garantir a continuidade das operações e da prestação dos serviços. 4. Os prestadores são responsáveis pelo cumprimento de qualquer dos compromissos subcontratados a outra entidade e pela conformidade com o regime, como se eles próprios prestassem os serviços. 5. Os sistemas de identificação eletrónica não instituídos pela legislação nacional devem prever um plano de cessação efetiva. Esse plano deve prever interrupções ordenadas do serviço ou a continuação por outro prestador, a forma como as autoridades competentes e os utilizadores finais são informados, bem como os pormenores sobre a forma como os registos devem ser protegidos, mantidos e destruídos em conformidade com a política do sistema.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.4.2. Publicação de notificações e informações para os utilizadores

Nível de garantia	Elementos necessários
Reduzido	1. Existe uma definição de serviços publicada que inclui todos os termos, condições e taxas, incluindo eventuais restrições à sua utilização. A definição de serviços deve incluir uma política de proteção da privacidade. 2. Devem ser postos em prática políticas e procedimentos adequados para assegurar que os utilizadores do serviço são informados atempadamente e de forma fiável de quaisquer alterações da definição ou das condições de quaisquer serviços ou da política de proteção da privacidade dos serviços em causa. 3. Devem ser postas em vigor políticas e procedimentos adequados para que os pedidos de informações recebam respostas exaustivas e exatas.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.4.3. Gestão da segurança da informação

Nível de garantia	Elementos necessários
Reduzido	Existe um sistema de gestão da segurança da informação eficaz para a gestão e controlo dos riscos da segurança da informação.
Substancial	Nível reduzido, acrescido de: O sistema de gestão da segurança das informações respeita normas ou princípios comprovados de gestão e controlo dos riscos de segurança da informação.
Elevado	Idênticos ao nível substancial.

2.4.4. Manutenção de registos

Nível de garantia	Elementos necessários
Reduzido	1. Registar e conservar as informações relevantes utilizando um sistema de gestão de arquivos eficaz, tendo em conta a legislação aplicável e as boas práticas em matéria de proteção e conservação de dados. 2. Manter, na medida em que tal seja permitido pela legislação nacional ou outras disposições administrativas nacionais, e proteger os registos enquanto forem necessários para fins de auditoria e investigação de violações da segurança, e de manutenção, após o que os registos devem ser destruídos de forma segura.
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.4.5. Instalações e pessoal

O quadro seguinte apresenta os requisitos relativos a instalações e pessoal e, quando aplicável, a subcontratantes que desempenham funções abrangidas pelo presente regulamento. A conformidade com todos os requisitos deve ser proporcional ao nível de risco associado ao nível de garantia em questão.

Nível de garantia	Elementos necessários
Reduzido	1. Existem procedimentos que asseguram que o pessoal e os subcontratantes são devidamente formados, qualificados e experientes nas competências necessárias para executar as funções que desempenham. 2. Existe pessoal e subcontratantes em número suficiente para prestar de forma adequada os serviços com os recursos conformes com as suas políticas e procedimentos. 3. As instalações utilizadas para prestar o serviço são permanentemente monitorizadas para detetar e proteger contra os danos causados por fenómenos ambientais, o acesso não autorizado e outros fatores que possam afetar a segurança do serviço. 4. As instalações utilizadas para prestar o serviço garantem que o acesso às zonas de conservação ou tratamento de informações pessoais, criptográficas ou outras informações sensíveis é limitado ao pessoal ou aos subcontratantes autorizados
Substancial	Idênticos ao nível reduzido.
Elevado	Idênticos ao nível reduzido.

2.4.6. Controlos técnicos

Nível de garantia	Elementos necessários
Reduzido	1. Existem controlos técnicos proporcionados para gerir os riscos que se colocam à segurança dos serviços e proteger a confidencialidade, a integridade e a disponibilidade das informações tratadas. 2. Os canais de comunicação eletrónicos utilizados para intercâmbio de informações sensíveis ou pessoais estão protegidos contra a interceção, a manipulação e a reprodução. 3. O acesso a material criptográfico sensível, se utilizado para a emissão de meios de identificação eletrónica e para a autenticação, está estritamente limitado às funções e aplicações que exijam esse acesso. Deve garantir-se que este material nunca é armazenado de forma persistente em forma de texto. 4. Existem procedimentos para garantir que a segurança se mantém ao longo do tempo e tem capacidade de resposta às alterações dos níveis de risco, aos incidentes e às falhas de segurança. 5. Todos os suportes que contenham dados criptográficas ou pessoais ou outros dados sensíveis, são armazenados, transportados e eliminados de forma segura.
Substancial	Idênticos ao nível reduzido, acrescido de: O material criptográfico sensível, se utilizado para a emissão de meios de identificação eletrónica e a autenticação, é protegido contra a manipulação abusiva
Elevado	Idênticos ao nível substancial.

2.4.7. Conformidade e auditoria

Nível de garantia	Elementos necessários
Reduzido	São realizadas auditorias internas periódicas, planeadas para incluir todas as partes relevantes da prestação dos serviços, a fim de garantir a sua conformidade com as políticas relevantes.

Nível de garantia	Elementos necessários
Substancial	São realizadas auditorias independentes internas ou externas periódicas, planeadas para incluir todas as partes relevantes da prestação dos serviços, a fim de garantir a sua conformidade com as políticas relevantes.
Elevado	1. São realizadas auditorias independentes externas periódicas, planeadas para incluir todas as partes relevantes da prestação dos serviços, a fim de garantir a sua conformidade com as políticas relevantes. 2. Quando o regime é gerido diretamente por um organismo governamental, é objeto de uma auditoria realizada de acordo com o direito nacional.

REGULAMENTO DE EXECUÇÃO (UE) 2015/1503 DA COMISSÃO

de 8 de setembro de 2015

que estabelece os valores forfetários de importação para a determinação do preço de entrada de certos frutos e produtos hortícolas

A COMISSÃO EUROPEIA,

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

Tendo em conta o Regulamento (UE) n.º 1308/2013 do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, que estabelece uma organização comum dos mercados dos produtos agrícolas e que revoga os Regulamentos (CEE) n.º 922/72, (CEE) n.º 234/79, (CE) n.º 1037/2001, (CE) n.º 1234/2007 do Conselho ([1]),

Tendo em conta o Regulamento de Execução (UE) n.º 543/2011 da Comissão, de 7 de junho de 2011, que estabelece regras de execução do Regulamento (CE) n.º 1234/2007 do Conselho nos sectores das frutas e produtos hortícolas e das frutas e produtos hortícolas transformados ([2]), nomeadamente o artigo 136.º, n.º 1,

Considerando o seguinte:

(1) O Regulamento de Execução (UE) n.º 543/2011 estabelece, em aplicação dos resultados das negociações comerciais multilaterais do «Uruguay Round», os critérios para a fixação pela Comissão dos valores forfetários de importação dos países terceiros relativamente aos produtos e aos períodos indicados no Anexo XVI, parte A.

(2) O valor forfetário de importação é calculado, todos os dias úteis, em conformidade com o artigo 136.º, n.º 1, do Regulamento de Execução (UE) n.º 543/2011, tendo em conta os dados diários variáveis. O presente regulamento deve, por conseguinte, entrar em vigor no dia da sua publicação no *Jornal Oficial da União Europeia*,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Os valores forfetários de importação referidos no artigo 136.º do Regulamento de Execução (UE) n.º 543/2011 são fixados no anexo do presente regulamento.

Artigo 2.º

O presente regulamento entra em vigor na data 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

Em nome do Presidente,

Jerzy PLEWA

Diretor-Geral da Agricultura e do Desenvolvimento Rural

([1]) JO L 347 de 20.12.2013, p. 671.
([2]) JO L 157 de 15.6.2011, p. 1.

ANEXO

Valores forfetários de importação para a determinação do preço de entrada de certos frutos e produtos hortícolas

(EUR/100 kg)

Código NC	Código países terceiros (1)	Valor forfetário de importação
0702 00 00	MA	173,3
	MK	48,7
	XS	41,5
	ZZ	87,8
0707 00 05	MK	76,3
	TR	116,3
	XS	42,0
	ZZ	78,2
0709 93 10	TR	133,1
	ZZ	133,1
0805 50 10	AR	135,9
	BO	135,7
	CL	125,5
	UY	142,2
	ZA	136,9
	ZZ	135,2
0806 10 10	EG	239,8
	MK	63,9
	TR	129,5
	ZZ	144,4
0808 10 80	AR	188,7
	BR	93,9
	CL	134,4
	NZ	143,4
	US	112,5
	UY	110,5
	ZA	117,6
	ZZ	128,7
0808 30 90	AR	131,9
	CL	100,0
	TR	122,9
	ZA	113,5
	ZZ	117,1
0809 30 10, 0809 30 90	MK	80,1
	TR	141,7
	ZZ	110,9

(EUR/100 kg)

Código NC	Código países terceiros (1)	Valor forfetário de importação
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Nomenclatura dos países fixada pelo Regulamento (UE) n.º 1106/2012 da Comissão, de 27 de novembro de 2012, que executa o Regulamento (CE) n.º 471/2009 do Parlamento Europeu e do Conselho relativo às estatísticas comunitárias do comércio externo com países terceiros, no que respeita à atualização da nomenclatura dos países e territórios (JO L 328 de 28.11.2012, p. 7). O código «ZZ» representa «outras origens».

DECISÕES

DECISÃO DE EXECUÇÃO (UE) 2015/1504 DA COMISSÃO

de 7 de setembro de 2015

que concede derrogações a certos Estados-Membros no que diz respeito à transmissão de estatísticas nos termos do Regulamento (CE) n.º 1099/2008 do Parlamento Europeu e do Conselho relativo às estatísticas da energia

[notificada com o número C(2015) 6105]

(Apenas fazem fé os textos nas línguas eslovaca, estónia, francesa, grega e neerlandesa)

(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 (CE) n.º 1099/2008 do Parlamento Europeu e do Conselho, de 22 de outubro de 2008, relativo às estatísticas da energia [1], nomeadamente o artigo 5.º, n.º 4, e o artigo 10.º, n.º 2,

Considerando o seguinte:

(1) Em conformidade com o artigo 5.º, n.º 4, do Regulamento (CE) n.º 1099/2008, a pedido devidamente justificado de um Estado-Membro, podem ser concedidas derrogações relativamente às parcelas das estatísticas nacionais cuja recolha possa implicar uma carga excessiva para os respondentes.

(2) Foram apresentados pedidos da Bélgica, da Estónia, de Chipre e da Eslováquia no sentido de obterem derrogações para a transmissão de estatísticas pormenorizadas sobre o consumo de energia das famílias, por tipo de utilização final, para certos anos de referência.

(3) As informações fornecidas por esses Estados-Membros justificam a concessão das derrogações.

(4) As medidas previstas na presente decisão estão em conformidade com o parecer do Comité do Sistema Estatístico Europeu,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

São concedidas as seguintes derrogações às disposições do Regulamento (CE) n.º 1099/2008:

1) É concedida uma derrogação à Bélgica, no que diz respeito à transmissão de resultados sobre o ano de referência 2015, para o ponto 1.2.3, números 4.2.1 a 4.2.5, ponto 2.2.3, números 4.2.1 a 4.2.5, ponto 3.2.3, números 3.1 a 3.6, ponto 4.2.3, números 7.2.1 a 7.2.5, e ponto 5.2.4, números 4.2.1 a 4.2.5, do anexo B, relativamente às estatísticas sobre o consumo de energia pormenorizado das famílias, por tipo de utilização final (como definido no ponto 2.3, número 26, «Outros setores — Residencial» do anexo A).

[1] JO L 304 de 14.11.2008, p. 1.

2) É concedida uma derrogação à Estónia, no que diz respeito à transmissão de resultados sobre os anos de referência 2015, 2016 e 2017, para o ponto 1.2.3, números 4.2.1 a 4.2.5, ponto 2.2.3, números 4.2.1 a 4.2.5, ponto 3.2.3, números 3.1 a 3.6, ponto 4.2.3, números 7.2.1 a 7.2.5, e ponto 5.2.4, números 4.2.1 a 4.2.5, do anexo B, relativamente às estatísticas sobre o consumo de energia pormenorizado das famílias, por tipo de utilização final (como definido no ponto 2.3, número 26, «Outros setores — Residencial» do anexo A).

3) É concedida uma derrogação a Chipre, no que diz respeito à transmissão de resultados sobre os anos de referência 2015, 2016 e 2017, para o ponto 1.2.3, números 4.2.1 a 4.2.5, ponto 2.2.3, números 4.2.1 a 4.2.5, ponto 3.2.3, números 3.1 a 3.6, e ponto 5.2.4, números 4.2.1 a 4.2.5, do anexo B, relativamente às estatísticas sobre o consumo de energia pormenorizado das famílias, por tipo de utilização final (como definido no ponto 2.3, número 26, «Outros setores — Residencial» do anexo A).

4) É concedida uma derrogação à Eslováquia, no que diz respeito à transmissão de resultados sobre os anos de referência 2015 e 2016, para o ponto 1.2.3, números 4.2.1 a 4.2.5, ponto 2.2.3, números 4.2.1 a 4.2.5, ponto 3.2.3, números 3.1 a 3.6, ponto 4.2.3, números 7.2.1 a 7.2.5, e ponto 5.2.4, números 4.2.1 a 4.2.5, do anexo B, relativamente às estatísticas sobre o consumo de energia pormenorizado das famílias, por tipo de utilização final (como definido no ponto 2.3, número 26, «Outros setores — Residencial» do anexo A).

Artigo 2.º

Os destinatários da presente decisão são o Reino da Bélgica, a República da Estónia, a República de Chipre e a República Eslovaca.

Feito em Bruxelas, em 7 de setembro de 2015.

Pela Comissão

Marianne THYSSEN

Membro da Comissão

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 ([1]), 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 ([2]), 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 ([3]) 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.

([1]) JO L 257 de 28.8.2014, p. 73.

([2]) 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).

([3]) 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 carateres «[*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 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 ([1]):

(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).

([1]) 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 ([1]) 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

([1]) 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 carateres 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 ([1]), que deve ser formatado de acordo com o perfil PDF/A (norma ISO 19005) ([2]).

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 ([3]), 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

([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)
([3]) 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 ([1])

— acesso à informação da autoridade

— acesso à informação da pessoa em causa

— declarações dos certificados qualificados ([2])

— 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.

([1]) RFC 5280: Certificado Internet X.509 de infraestrutura de chave pública (PKI) e perfil CRL

([2]) 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 ([1]) 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.

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

DECISÃO DE EXECUÇÃO (UE) 2015/1506 DA COMISSÃO

de 8 de setembro de 2015

que estabelece especificações relativas aos formatos das assinaturas eletrónicas avançadas e dos selos eletrónicos avançados para reconhecimento pelos organismos públicos nos termos dos artigos 27.º, n.º 5, e 37.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 ([1]), nomeadamente os artigos 27.º, n.º 5, e 37.º, n.º 5,

Considerando o seguinte:

(1) Os Estados-Membros devem dispor dos meios técnicos necessários que lhes permitam processar os documentos assinados eletronicamente que são exigidos para a utilização de serviços em linha oferecidos por organismos públicos ou em nome destes.

(2) O Regulamento (UE) n.º 910/2014 obriga os Estados-Membros que exigem uma assinatura eletrónica avançada ou um selo eletrónico avançado para a utilização de serviços em linha oferecidos por organismos públicos ou em nome destes, a reconhecerem assinaturas eletrónicas avançadas e selos eletrónicos avançados, assinaturas eletrónicas avançadas e selos eletrónicos avançados baseados em certificados qualificados e assinaturas eletrónicas avançadas e selos eletrónicos avançados qualificados em formatos específicos ou formatos alternativos validados em conformidade com métodos de referência específicos.

(3) Para definir os formatos e métodos de referência específicos, devem ser tidas em contas as práticas, normas e atos jurídicos da União.

(4) A Decisão de Execução 2014/148/UE da Comissão ([2]) definiu um certo número de formatos de assinaturas eletrónicas avançadas mais comuns para serem tecnicamente suportadas pelos Estados-Membros onde são necessárias assinaturas eletrónicas avançadas para realizar um procedimento administrativo em linha. O estabelecimento de formatos de referência visa facilitar a validação transfronteiriça das assinaturas eletrónicas e melhorar a interoperabilidade transfronteiriça dos procedimentos eletrónicos.

(5) As normas enumeradas no anexo da presente decisão são as normas existentes para os formatos de assinaturas eletrónicas avançadas. Dado que os organismos de normalização estão a proceder a uma análise das formas de arquivamento a longo prazo dos formatos de referência, as normas pormenorizadas sobre o arquivamento a longo prazo são excluídas do âmbito de aplicação da presente decisão. Quando a nova versão das normas de referência estiverem disponíveis, as normas e cláusulas relativas ao arquivamento a longo prazo serão revistas.

(6) As assinaturas eletrónicas avançadas e os selos eletrónicos avançados são semelhantes do ponto de vista técnico. Por conseguinte, as normas em matéria de formatos de assinaturas eletrónicas avançadas devem aplicar-se *mutatis mutandis* aos formatos de selos eletrónicos avançados.

(7) Quando são utilizadas assinaturas ou selos eletrónicos em formatos diferentes das técnicas mais comuns, devem ser fornecidos meios de validação que permitam que as assinaturas ou selos eletrónicos sejam verificados além-fronteiras. A fim de permitir que os Estados-Membros destinatários possam confiar nesses instrumentos de validação de outro Estado-Membro, é necessário fornecer informações facilmente acessíveis sobre esses instrumentos de validação, incluindo as informações nos documentos eletrónicos, nas assinaturas eletrónicas ou nos contentores de documentos eletrónicos.

([1]) JO L 257 de 28.8.2014, p. 73.

([2]) Decisão de Execução 2014/148/UE da Comissão, de 17 de março de 2014, que altera a Decisão 2011/130/UE que estabelece requisitos mínimos para o processamento transfronteiras de documentos assinados eletronicamente pelas autoridades competentes nos termos da Diretiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno (JO L 80 de 19.3.2014, p. 7).

(8) Nos casos em que as possibilidades de validação da assinatura eletrónica ou do selo eletrónico adequado para tratamento automático estão disponíveis nos serviços públicos de um Estado-Membro, tais possibilidades de validação devem ser disponibilizadas e fornecidas ao Estado-Membro de receção. No entanto, a presente decisão não deverá impedir a aplicação do artigo 27.º, n.ºs 1 e 2, e do artigo 37.º, n.ºs 1 e 2, do Regulamento (UE) n.º 910/2014 quando o tratamento automatizado das possibilidades de validação de métodos alternativos não for possível.

(9) A fim de prever requisitos comparáveis para a validação e para aumentar a confiança nas possibilidades de validação disponibilizadas pelos Estados-Membros para assinaturas ou selos eletrónicos em formatos diferentes dos mais comuns, os requisitos estabelecidos na presente decisão para os instrumentos de validação baseiam-se nos requisitos para a validação de assinaturas e selos eletrónicos qualificados previstos nos artigos 32.º e 40.º do Regulamento (UE) n.º 910/2014.

(10) 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 que exijam uma assinatura eletrónica avançada ou uma assinatura eletrónica avançada baseada num certificado qualificado, conforme previsto no artigo 27.º, n.ºs 1 e 2, do Regulamento (UE) n.º 910/2014, devem reconhecer as assinaturas eletrónicas avançadas em formato XML, CMS ou PDF conformes com o nível B, T ou LT ou utilizando um contentor de assinatura associada, quando essas assinaturas forem conformes com as especificações técnicas constantes do anexo.

Artigo 2.º

1. Os Estados-Membros que exijam uma assinatura eletrónica avançada ou uma assinatura eletrónica avançada baseada num certificado qualificado, conforme previsto no artigo 27.º, n.ºs 1 e 2, do Regulamento (UE) n.º 910/2014, devem reconhecer outros formatos de assinaturas eletrónicas além dos referidos no artigo 1.º da presente decisão, desde que o Estado-Membro em que o prestador de serviços de confiança utilizados pelo signatário está estabelecido ofereça outras possibilidades de validação da assinatura, se possível adequadas para tratamento automático.

2. As possibilidades de validação da assinatura devem:

a) Permitir a outros Estados-Membros validar as assinaturas eletrónicas recebidas em linha, a título gratuito e de uma forma compreensível para os falantes não nativos;

b) Ser indicadas no documento, na assinatura eletrónica ou no contentor de documentos eletrónicos; e

c) Confirmar a validade de uma assinatura eletrónica avançada, desde que:

1) O certificado em que a assinatura eletrónica avançada se baseia seja válido no momento da assinatura e, quando a assinatura eletrónica avançada se baseie num certificado qualificado, o certificado qualificado que comprova a assinatura eletrónica avançada seja, no momento da assinatura, um certificado qualificado de assinatura eletrónica conforme com o disposto no anexo I do Regulamento (UE) n.º 910/2014, tendo sido emitido por um prestador de serviços de confiança qualificado;

2) Os dados para a validação da assinatura correspondam aos dados fornecidos ao utilizador;

3) O conjunto único de dados que representam o signatário seja corretamente fornecido ao utilizador;

4) A eventual utilização de um pseudónimo no momento da assinatura seja claramente indicada ao utilizador;

5) Quando a assinatura eletrónica avançada for criada por um dispositivo qualificado de criação de assinaturas eletrónicas, a utilização desses dispositivos seja claramente indicada à parte utilizadora;

6) A integridade dos dados assinados não tenha sido afetada;

7) Os requisitos previstos no artigo 26.º do Regulamento (UE) n.º 910/2014 estejam preenchidos no momento da assinatura;

8) O sistema utilizado para validar a assinatura eletrónica avançada forneça à parte utilizadora o resultado correto do processo de validação e lhe permita detetar eventuais problemas de segurança relevantes.

Artigo 3.º

Os Estados-Membros que exijam um selo eletrónico avançado ou um selo eletrónico avançado baseado num certificado qualificado, conforme previsto no artigo 37.º, n.ºs 1 e 2, do Regulamento (UE) n.º 910/2014, devem reconhecer selos eletrónicos avançados em formato XML, CMS ou PDF conformes com o nível B, T ou LT ou utilizando um contentor de selo associado, quando estes forem conformes com as especificações técnicas constantes do anexo.

Artigo 4.º

1. Os Estados-Membros que exijam um selo eletrónico avançado ou um selo eletrónico avançado baseado num certificado qualificado, conforme previsto no artigo 37.º, n.ºs 1 e 2, do Regulamento (UE) n.º 910/2014, devem reconhecer outros formatos de selos eletrónicos além dos referidos no artigo 3.º da presente decisão, desde que o Estado-Membro em que o prestador de serviços de confiança utilizados pelo signatário esteja estabelecido ofereça outras possibilidades de validação do selo, se possível adequadas para tratamento automático.

2. As possibilidades de validação do selo devem:

a) Permitir a outros Estados-Membros validar os selos eletrónicos recebidos em linha, a título gratuito e de uma forma compreensível para os falantes não nativos;

b) Ser indicadas no documento selado, no selo eletrónico ou no contentor de documentos eletrónicos;

c) Confirmar a validade de um selo eletrónico avançado, desde que:

1) O certificado em que o selo eletrónico avançado se baseia seja válido no momento da assinatura e, quando o selo eletrónico avançado se baseie num certificado qualificado, o certificado qualificado que comprova o selo eletrónico avançado seja, no momento da selagem, um certificado qualificado de selo eletrónico conforme com o disposto no anexo I do Regulamento (UE) n.º 910/2014, tendo sido emitido por um prestador de serviços de confiança qualificado;

2) Os dados para a validação do selo correspondam aos dados fornecidos ao utilizador;

3) O conjunto único de dados que representam o criador do selo seja corretamente fornecido ao utilizador;

4) A eventual utilização de um pseudónimo no momento da selagem seja claramente indicada ao utilizador;

5) Quando o selo eletrónico avançado for criado por um dispositivo qualificado de criação de selos eletrónicos, a utilização desse dispositivo seja claramente indicada à parte utilizadora;

6) A integridade dos dados selados não tenha sido afetada;

7) Os requisitos previstos no artigo 36.º do Regulamento (UE) n.º 910/2014 estejam preenchidos no momento da assinatura;

8) O sistema utilizado para validar o selo eletrónico avançado forneça à parte utilizadora o resultado correto do processo de validação e lhe permita detetar eventuais problemas de segurança relevantes.

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

Lista de especificações técnicas para as assinaturas eletrónicas avançadas em formato XML, CMS ou PDF e o contentor de assinatura associada

As assinaturas eletrónicas avançadas mencionadas no artigo 1.º da decisão devem respeitar uma das seguintes especificações técnicas do ETSI, com exceção da respetiva cláusula 9:

Perfil de base XAdES	ETSI TS 103171 v.2.1.1. ([1])
Perfil de base CAdES	ETSI TS 103173 v.2.2.1. ([2])
Perfil de base PAdES	ETSI TS 103172 v.2.2.2. ([3])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf.
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf.
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf.

O contentor de assinatura associada mencionado no artigo 1.º da decisão deve respeitar as seguintes especificações técnicas do ETSI:

Perfil de base do contentor de assinatura associada	ETSI TS 103174 v.2.2.1. ([1])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf.

Lista de especificações técnicas para os selos eletrónicos avançados em formato XML, CMS ou PDF e o contentor de selo associado

Os selos eletrónicos avançados mencionados no artigo 3.º da decisão devem respeitar uma das seguintes especificações técnicas do ETSI, com exceção da respetiva cláusula 9:

Perfil de base XAdES	ETSI TS 103171 v.2.1.1.
Perfil de base CAdES	ETSI TS 103173 v.2.2.1.
Perfil de base PAdES	ETSI TS 103172 v.2.2.2.

O contentor de selo associado mencionado no artigo 3.º da decisão deve respeitar as seguintes especificações técnicas do ETSI:

Perfil de base do contentor de selo associado	ETSI TS 103174 v.2.2.1.

ISSN 1977-0774 (edição eletrónica)
ISSN 1725-2601 (edição em papel)

Serviço das Publicações da União Europeia
2985 Luxemburgo
LUXEMBURGO

PT