DECISÃO DE EXECUÇÃO (UE) 2016/650 DA COMISSÃO

de 25 de abril de 2016

que estabelece normas para a avaliação da segurança dos dispositivos qualificados de criação de assinaturas e selos nos termos dos artigos 30.º, n.º 3, e 39.º, n.º 2, 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 30.º, n.º 3, e 39.º, n.º 2,

Considerando o seguinte:

(1) O anexo II do Regulamento (UE) n.º 910/2014 estabelece os requisitos aplicáveis aos dispositivos qualificados de criação de assinaturas eletrónicas ou aos dispositivos qualificados de criação de selos eletrónicos.

(2) A tarefa de elaborar as especificações técnicas necessárias para a produção e a colocação no mercado de produtos adequados ao estado atual da tecnologia está a cargo das organizações competentes no domínio da normalização.

(3) A ISO/IEC (Organização Internacional de Normalização/Comissão Eletrotécnica Internacional) estabelece os conceitos e princípios gerais da segurança informática e especifica o modelo geral de avaliação que servirá de base para a avaliação das propriedades de segurança dos produtos informáticos.

(4) No âmbito do mandato de normalização M/460 conferido pela Comissão, o Comité Europeu de Normalização (CEN) elaborou normas para os dispositivos qualificados de criação de assinaturas e selos eletrónicos, em que os dados para a criação da assinatura eletrónica ou dos selos eletrónicos se encontram num ambiente inteiramente gerido pelo utilizador, mas não necessariamente de forma exclusiva. Estas normas são consideradas adequadas para a avaliação da conformidade dos dispositivos com os requisitos aplicáveis estabelecidos no anexo II do Regulamento (UE) n.º 910/2014.

(5) O anexo II do Regulamento (UE) n.º 910/2014 estabelece que apenas um prestador qualificado de serviços de confiança pode gerir dados para a criação de uma assinatura eletrónica em nome do signatário. Os requisitos de segurança e respetivas especificações de certificação são diferentes quando o signatário possui fisicamente um produto ou quando um prestador qualificado de serviços de confiança age em nome do signatário. Para abranger ambas as situações, bem como para favorecer o desenvolvimento futuro de produtos e normas de avaliação adequadas às necessidades específicas, o anexo da presente decisão contem uma lista de normas que cobrem ambas as situações.

(6) No momento em que a presente Decisão da Comissão foi adotada, vários prestadores de serviços de confiança já oferecem soluções de gestão dos dados para a criação de uma assinatura eletrónica em nome dos seus clientes. A certificação de produtos está atualmente limitada aos módulos de segurança de *hardware* certificados de acordo com diferentes normas, mas ainda não são certificados especificamente quanto aos requisitos para os dispositivos de criação de assinaturas e selos qualificados. No entanto, as normas publicadas, como a EN 419 211 (aplicável à assinatura eletrónica criada num ambiente inteiramente gerido pelo utilizador, mas não necessariamente de forma exclusiva), ainda não existem para o mercado igualmente importante dos produtos à distância certificados. Dado que as normas que podem ser adequadas para esses fins estão atualmente a ser elaboradas, quando estiverem disponíveis e forem avaliadas em função dos requisitos estabelecidos no anexo II do Regulamento (UE) n.º 910/2014, a Comissão irá complementar a presente decisão. Até que a lista dessas normas seja elaborada, pode utilizar-se um processo alternativo para a avaliação da conformidade de tais produtos nas condições previstas na do artigo 30.º, n.º 3, alínea b), do Regulamento (UE) n.º 910/2014.

(7) O anexo inclui a norma EN 419 211, que é constituída por várias partes (1 a 6) que abrangem diferentes situações. A EN 419 211, parte 5, e a EN 419 211, parte 6, concedem extensões relacionadas com o ambiente

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

do dispositivo qualificado de criação de assinaturas, como a comunicação com as aplicações de criação de assinaturas de confiança. Os fabricantes são livres de aplicar essas extensões. De acordo com o considerando 56 do Regulamento (UE) n.º 910/2014, o âmbito de aplicação da certificação ao abrigo dos artigos 30.º e 39.º do referido regulamento limita-se a proteger os dados de criação da assinatura e as aplicações de criação de assinaturas estão excluídas do âmbito da certificação.

(8) A fim de garantir que as assinaturas ou selos eletrónicos gerados por um dispositivo de criação qualificado são eficazmente protegidos contra a falsificação, em conformidade com o anexo II do Regulamento (UE) n.º 910/2014, os algoritmos criptográficos adequados, as dimensões da chave e as funções *hash* são um pré-requisito para a segurança do produto certificado. Dado que esta questão não foi harmonizada a nível europeu, os Estados-Membros devem cooperar entre si para chegar a acordo sobre os algoritmos criptográficos, as dimensões da chave e as funções *hash* a utilizar no domínio das assinaturas e selos eletrónicos.

(9) A adoção da presente decisão torna a Decisão 2003/511/CE da Comissão [1] obsoleta. Consequentemente, deve ser revogada.

(10) As medidas previstas na presente decisão estão em conformidade com o parecer do comité referido no artigo 48.º do Regulamento (UE) n.º 910/2014,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

1. O anexo da presente decisão enumera as normas de avaliação da segurança dos produtos informáticos aplicáveis à certificação dos dispositivos qualificados de criação de assinaturas ou selos eletrónicos, em conformidade com o artigo 30.º, n.º 3, alínea a), ou com o artigo 39.º, n.º 2, do Regulamento (UE) n.º 910/2014, quando os dados de criação da assinatura eletrónica ou dos selos eletrónicos se encontram num ambiente inteiramente gerido pelo utilizador, mas não necessariamente de forma exclusiva.

2. Na pendência da elaboração pela Comissão de uma lista de normas de avaliação da segurança dos produtos informáticos aplicáveis à certificação dos dispositivos qualificados de criação de assinaturas ou selos eletrónicos, quando um prestador qualificado de serviços de confiança gere os dados de criação da assinatura eletrónica ou dos selos eletrónicos em nome de um signatário ou de um criador de um selo, a certificação de tais produtos deve basear-se num processo que, nos termos do artigo 30.º, n.º 3, alínea b), assegure níveis de segurança comparáveis aos exigidos pelo artigo 30.º, n.º 3, alínea a), e que são notificados à Comissão pela entidade pública ou privada referida no artigo 30.º, n.º 1, do Regulamento (UE) n.º 910/2014.

Artigo 2.º

É revogada a Decisão 2003/511/CE.

Artigo 3.º

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

Feito em Bruxelas, em 25 de abril de 2016.

Pela Comissão

O Presidente

Jean-Claude JUNCKER

[1] Decisão 2003/511/CE da Comissão, de 14 de julho de 2003, sobre a publicação dos números de referência das normas geralmente reconhecidas para produtos de assinatura eletrónica, nos termos da Diretiva 1999/93/CE do Parlamento Europeu e do Conselho (JO L 175 de 15.7.2003, p. 45).

ANEXO

LISTA DAS NORMAS REFERIDA NO ARTIGO 1.º, N.º 1

— ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, parts 1 to 3 as listed below:

  — ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1. ISO, 2009

  — ISO/IEC 15408-2:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 2. ISO, 2008

  — ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3. ISO, 2008

  e

— ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation

  e

— EN 419 211 — Protection profiles for secure signature creation device, parts 1 to 6 — as appropriate — as listed below:

  — EN 419211-1:2014 — Protection profiles for secure signature creation device — Part 1: Overview

  — EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation

  — EN 419211-3:2013 — Protection profiles for secure signature creation device — Part 3: Device with key generation

  — EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application

  — EN 419211-5:2013 — Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application

  — EN 419211-6:2014 — Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application