Despacho 155/2017

Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário

O anexo II 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 a Diretiva 1999/93/CE (Regulamento eIDAS), 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.

Considerando que se encontra em curso o desenvolvimento, por parte do Comité Europeu de Normalização (CEN), no âmbito do mandato de normalização M/460 conferido pela Comissão Europeia, de 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.

Considerando que nos vários Estados-membros existem vários prestadores de serviços de confiança, que já oferecem soluções de gestão dos dados para a criação de assinaturas eletrónicas em nome dos seus clientes.

Considerando que a certificação de produtos está atualmente limitada aos módulos de segurança de *hardware* certificados de acordo com diferentes normas, mas que ainda não são certificados especificamente quanto aos requisitos para os dispositivos de criação de assinaturas e selos qualificados.

Considerando o disposto na 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 eIDAS.

Nestes termos, o Gabinete Nacional de Segurança (GNS), no âmbito das suas atribuições de Entidade Supervisora, e de acordo com o consignado no artigo 17.º do Regulamento eIDAS, vem por este meio definir o seguinte:

1. Na pendência da elaboração pela Comissão de uma lista de normas adequadas para o efeito, fica estabelecido que a avaliação da conformidade dos mecanismos e procedimentos adequados para garantir que o signatário tem o controlo exclusivo da utilização dos dados necessários para a criação da sua assinatura eletrónica, implica o cumprimento cumulativo dos requisitos definidos no Anexo A.

2. O presente despacho tem dois anexos (A e B), que dele fazem parte integrante.

3. O presente despacho entra em vigor no dia seguinte ao da sua assinatura.

Lisboa, 5 de dezembro de 2017

O Diretor-Geral

António Gameiro Marques

CALM

Anexo A

Requisitos para a utilização de sistemas e produtos de confiança para criação de assinaturas eletrónicas à distância

1. Os prestadores qualificados de serviços de confiança estabelecidos em Portugal aplicam procedimentos de segurança, de gestão e de administração adequados, utilizando sistemas e produtos de confiança, com recurso a canais de comunicação eletrónica seguros, de modo a garantir a fiabilidade do ambiente de criação de assinaturas eletrónicas e que esse mesmo ambiente é utilizado sob a supervisão exclusiva do signatário, através:

a. Da garantia da conformidade com os requisitos estabelecidos para o nível 2 da norma CEN/TS 419241 - *Security Requirements for Trustworthy Systems Supporting Server Signing*, de março de 2014; e
b. Da utilização de Dispositivos Seguros de Criação de Assinaturas que beneficiem da medida transitória prevista no n.º 1 do artigo 51.º do regulamento eIDAS.

2. Os certificados qualificados destinados à criação de assinaturas eletrónicas ou selos eletrónicos, cuja gestão é feita pelo prestador qualificado de serviços de confiança em nome do signatário, devem ser construídos com as seguintes regras:

a. No campo "subject", o atributo "organizationUnit" (OU) deve conter o valor "RemoteQSCDManagement";
b. O OU referido na alínea anterior deve ser inscrito no atributo imediatamente anterior ao "commonName".

Anexo B

Avaliação da conformidade dos sistemas e produtos de confiança utilizados para a criação de assinaturas eletrónicas à distância

1. O prestador de qualificado de serviços de confiança, que pretenda disponibilizar um ambiente de criação de assinaturas eletrónicas à distância, em que efetua a gestão em nome do signatário deve apresentar à entidade supervisora um relatório de avaliação da conformidade emitido por um organismo de avaliação da conformidade, que ateste o cumprimento dos requisitos previstos no Anexo A deste despacho.

2. O organismo de avaliação da conformidade deve avaliar, em ambiente operacional/produção, todos os requisitos definidos na norma CEN/TS 419241:2014, nomeadamente:

    a. Os *General Security Requirements* (SRG);
    b. Os *Core Components Security Requirements* (SRC)
    c. Os *Additional Security Requirements for Level 2* (SRA)

3. O relatório de avaliação da conformidade deve incorporar uma tabela de conformidade com a seguinte estrutura:

ID Requisito	**Descrição do requisito**	**Cumprimento do requisito**	**Detalhe da avaliação**
SRG_M.1.1	TW4S SHALL support roles with different privileges	S/N	…
…	…	S/N	…
SRG_IA.1.1	TW4S SHALL require each user to identify him/herself and be successfully authenticated before allowing any action on behalf of that user or role assumed by the user	S/N	…
…	…	…	…