2025/1946

30.9.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/1946 DA COMISSÃO

de 29 de setembro de 2025

que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante aos serviços qualificados de preservação de assinaturas eletrónicas qualificadas e de selos eletrónicos qualificados

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 34.º, n.º 2, e o artigo 40.º,

Considerando o seguinte:

(1) Os serviços qualificados de preservação de assinaturas eletrónicas qualificadas e de selos eletrónicos qualificados asseguram a integridade, a autenticidade, a prova de existência e a acessibilidade a longo prazo das provas de preservação dessas assinaturas e selos eletrónicos. Tal permite demonstrar a sua validade jurídica durante períodos alargados e garante que podem ser validados independentemente da evolução tecnológica futura. Estes serviços são prestados de forma independente ou como parte de outro serviço de confiança qualificado, como os serviços qualificados de arquivo eletrónico.

(2) A presunção de conformidade estabelecida no artigo 34.º, n.º 1-A, e no artigo 40.º do Regulamento (UE) n.º 910/2014 só deve aplicar-se quando os serviços qualificados de preservação de assinaturas eletrónicas qualificadas e de selos eletrónicos qualificados cumprirem as normas estabelecidas no presente regulamento. Estas normas devem refletir as práticas estabelecidas e ser amplamente reconhecidas nos setores pertinentes. Devem ser adaptadas de modo a incluir controlos adicionais que garantam a segurança e a fiabilidade do serviço de confiança qualificado, bem como a capacidade de verificar o estatuto de qualificado e a validade técnica das assinaturas e selos ao longo do tempo.

(3) Se um prestador de serviços de confiança cumprir os requisitos estabelecidos no anexo do presente regulamento, as entidades supervisoras devem presumir a conformidade com os requisitos pertinentes do Regulamento (UE) n.º 910/2014 e ter devidamente em conta essa presunção para conceder ou confirmar o estatuto de qualificado do serviço de confiança. No entanto, um prestador qualificado de serviços de confiança pode continuar a invocar outras práticas para demonstrar o cumprimento dos requisitos do Regulamento (UE) n.º 910/2014.

(4) A Comissão avalia periodicamente as novas tecnologias, práticas, normas ou especificações técnicas. Em conformidade com o considerando 75 do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho ([2]), a Comissão deve rever e atualizar o presente regulamento, se necessário, a fim de assegurar que o mesmo acompanha a evolução mundial, novas tecnologias, normas ou especificações técnicas e de seguir as boas práticas no mercado interno.

([1]) JO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho, de 11 de abril de 2024, que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação do Regime Europeu para a Identidade Digital (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(5) O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([3]) e, se for caso disso, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([4]) aplicam-se às atividades de tratamento de dados pessoais ao abrigo do presente regulamento.

(6) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([5]) e emitiu parecer em 6 de junho de 2025.

(7) As medidas previstas no presente regulamento estão em conformidade com o parecer do comité instituído pelo artigo 48.º do Regulamento (UE) n.º 910/2014,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Normas de referência e especificações

As normas de referência e especificações a que se referem o artigo 34.º, n.º 2, e o artigo 40.º do Regulamento (UE) n.º 910/2014 constam do anexo do presente regulamento.

Artigo 2.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 29 de setembro de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

([3]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANEXO

Lista das normas de referência e especificações a que se refere o artigo 2.º

Aplicam-se as normas ETSI TS 119 511 V1.1.1 (2019-06) («ETSI TS 119 511») e ETSI TS 119 172-4 V1.1.1 (2021-05) («ETSI TS 119 172-4»), com as seguintes adaptações:

1. Para a norma ETSI TS 119 511

(1) 2.1 Referências normativas

— [1] ETSI EN 319 401 V3.1.1 (2024-06) «Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); requisitos de política geral para os prestadores de serviços de confiança].

— [2] ETSI TS 119 612 (V2.3.1) «Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); listas de confiança].

— [5] FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules» (Requisitos de segurança para módulos criptográficos).

— [6] Regulamento de Execução (UE) 2024/482 da Comissão ([1]) que estabelece regras de execução do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho no respeitante à adoção do sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC).

— [7] Regulamento de Execução (UE) 2024/3144 da Comissão ([2]) que altera o Regulamento de Execução (UE) 2024/482 no respeitante às normas internacionais aplicáveis e que retifica esse regulamento de execução.

— [8] Grupo Europeu para a Certificação da Cibersegurança, subgrupo para a criptografia: «Agreed Cryptographic Mechanisms» (Mecanismos criptográficos acordados), publicado pela Agência da União Europeia para a Cibersegurança (ENISA) ([3]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) «Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists» [Assinaturas eletrónicas e infraestruturas (ESI); políticas de assinatura; parte 4: regras de aplicabilidade das assinaturas (política de validação) para assinaturas/ /selos eletrónicos qualificados europeus que utilizam listas de confiança].

— [10] ISO/IEC 15408:2022 (partes 1 a 5) «Information security, cybersecurity and privacy protection — Evaluation criteria for IT security» (Segurança da informação, cibersegurança e proteção da privacidade — Critérios de avaliação da segurança informática).

(2) 3.1 Termos

— Dispositivo criptográfico seguro: dispositivo que detém a chave privada do utente, a protege contra o risco de comprometimento e executa funções de assinatura ou decifragem em nome do utente.

(3) 6.4 Perfis de preservação

— OVR-6.4-08A [WTS][WOS] A duração prevista das provas deve estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [8].

— NOTA 3 nula e sem efeito.

(4) 6.5 Política de preservação de provas

— OVR-6.5-04 A Os algoritmos criptográficos utilizados devem estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [8].

— NOTA 1 nula e sem efeito.

([1]) JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

(5) 7.2 Recursos humanos

— OVR-7.2-02 O pessoal do prestador de serviços de preservação (PSP) com funções de confiança e, se aplicável, os seus subcontratantes com funções de confiança devem ser capazes de cumprir o requisito de dispor de conhecimentos especializados, experiência e qualificações adquiridos por meio de formação formal e credenciais, de experiência ou de uma combinação de ambas.

— OVR-7.2-03 A conformidade com o OVR-7.2-02 deve incluir atualizações regulares (pelo menos a cada 12 meses) sobre as novas ameaças e as atuais práticas de segurança.

(6) 7.5 Controlos criptográficos

— OVR-7.5-05 [CONDICIONAL] Quando o PSP assina (parte de) uma prova de preservação, a chave de assinatura privada desse PSP deve ser conservada e utilizada num dispositivo criptográfico seguro que seja um sistema fiável certificado em conformidade com:

(a) Os Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, estabelecidos na norma ISO/IEC 15408 [10] ou nos Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, versão CC:2022, partes 1 a 5, publicados pelos participantes no Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI, e certificado com o nível EAL 4 ou superior; ou

(b) O EUCC [6] [7] e certificado com o nível EAL 4 ou superior; ou

(c) Até 31.12.2030, FIPS PUB 140-3 [5] nível 3.

Esta certificação refere-se a uma meta de segurança ou a um perfil de proteção, ou a uma documentação de segurança e conceção de módulos, que cumpra os requisitos do presente documento, com base numa análise de risco e tendo em conta as medidas de segurança físicas e outras medidas de segurança não técnicas.

Se o dispositivo criptográfico seguro possuir uma certificação EUCC [6] [7], esse dispositivo deve ser configurado e utilizado em conformidade com essa certificação.

— OVR-7.5-06 [CONDICIONAL] nulo e sem efeito.

— OVR-7.5-07 [CONDICIONAL] Quando o PSP assina (parte de) uma prova de preservação, quaisquer cópias de segurança das chaves de assinatura privadas do PSP devem ser protegidas pelo dispositivo criptográfico seguro, de modo que a sua integridade e confidencialidade sejam garantidas antes de serem armazenadas fora desse dispositivo.

— OVR-7.5-08 A chave de assinatura privada de um PSP só deve ser exportada e importada para um dispositivo criptográfico seguro diferente se essa exportação e importação forem implementadas de forma segura e em conformidade com a certificação desses dispositivos.

(7) 7.8 Segurança da rede

— OVR-7.8-03 A análise das vulnerabilidades solicitada pelo REQ-7.8-13 da norma ETSI EN 319 401 [1] deve ser efetuada pelo menos uma vez por trimestre.

— OVR-7.8-04 O teste de penetração solicitado pelo REQ-7.8-17X da norma ETSI EN 319 401 [1] deve ser efetuado pelo menos uma vez por ano.

— OVR-7.8-05 As barreiras de segurança devem ser configuradas de modo a impedir todos os protocolos e acessos não necessários para a operação do PSP.

(8) 7.14 Monitorização criptográfica

— OVR-7.14-03A A avaliação dos algoritmos criptográficos previstos no OVR-7.14.01 e no OVR-7.14.02 deve estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [8].

— NOTA nula e sem efeito.

(9) 7.12 Cessação e planos de cessação do prestador de serviços de confiança (TSP)

— OVR-7.12-01A O plano de cessação do TSP deve cumprir os requisitos estabelecidos nos atos de execução adotados nos termos do artigo 24.º, n.º 5, do Regulamento (UE) n.º 910/2014 [i.2].

(10) 7.17 Cadeia de abastecimento

— OVR-7.17-01 Aplicam-se os requisitos especificados na norma ETSI EN 319 401 [1], cláusula 7.14.

(11) Anexo A (normativo): serviço qualificado de preservação de assinaturas eletrónicas qualificadas (QES) na aceção do artigo 34.º do Regulamento (UE) n.º 910/2014

— OVR-A-02 [PDS][PDS+PGD]

(a) O serviço de preservação deve conservar todas as informações necessárias para verificar o estatuto de qualificado do selo ou da assinatura eletrónica que não estejam disponíveis ao público até ao final do período de preservação;

(b) O serviço de preservação deve assegurar que, em qualquer momento do período de preservação, a informação conservada seja suficiente para que, quando fornecida como entrada para o processo especificado na cláusula 4.4 da norma ETSI TS 119 172-4 [9], o resultado desse processo determine claramente se o selo ou assinatura digital era, no momento da sua preservação, tecnicamente adequado para executar uma assinatura eletrónica ou um selo eletrónico qualificado da UE.

— OVR-A-03 [PDS][PDS+PGD] Os selos temporais utilizados nas provas de preservação devem ser selos temporais qualificados nos termos do Regulamento (UE) n.º 910/2014 [i.2].

2. Para a norma ETSI TS 119 172-4

(1) 2.1 Referências normativas

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) «Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); procedimentos para a criação e validação de assinaturas digitais AdES; parte 1: criação e validação].

— Qualquer referência à «ETSI TS 119 102-1 [1]» deve ser entendida como uma referência à «ETSI EN 319 102-1 [1]».

— [2] ETSI TS 119 612 (V2.3.1) «Electronic Signatures and Trust Infrastructures (ESI); Trusted Lists» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); listas de confiança].

— [13] ETSI TS 119 101 V1.1.1 (2016-03) «Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation» [Assinaturas eletrónicas e infraestruturas (ESI); requisitos de política e de segurança para aplicações de criação e validação de assinaturas].

(2) 4.2 Restrições e procedimentos de validação, requisito REQ-4.2-03, secção X.509, relativa às restrições de validação, alínea c)

— i) Se um certificado de entidade final representar uma âncora de confiança, não se pode utilizar «RevocationCheckingConstraints».

— ii) Se um certificado de entidade final não representar uma âncora de confiança, deve definir-se «RevocationCheckingConstraints» como «eitherCheck», conforme especificado na norma ETSI TS 119 172-1 [3], cláusula A.4.2.1, quadro A.2, linhas m)2.1.

— iii) Se um certificado de entidade final representar uma âncora de confiança, as restrições «Revocation-FreshnessConstraints» definidas na norma ETSI TS 119 172-1 [3], cláusula A.4.2.1, quadro A.2, linhas m)2.2., não podem ser utilizadas.

— iv) Se um certificado de entidade final não representar uma âncora de confiança, as restrições «RevocationFreshnessConstraints» definidas na norma ETSI TS 119 172-1 [3], cláusula A.4.2.1, quadro A.2, linhas m)2.2, devem ser utilizadas com um valor máximo de 0 para o certificado de assinatura, assegurando que a informação de revogação só é aceite se tiver sido emitida após a melhor hora de assinatura («best signature time»). Não é fixado qualquer valor para «RevocationFreshnessConstraints» para certificados que não o certificado de assinatura, incluindo os certificados comprovativos dos selos temporais.

(3) 4.3 Requisitos relativos às práticas de validação de assinaturas e de verificação das regras de aplicabilidade

— REQ-4.3-02 As aplicações de validação de assinaturas devem estar em conformidade com a norma ETSI TS 119 101 [13].

(4) 4.4 Processo de verificação (das regras) de aplicabilidade técnica

— REQ-4.4.2-03 Se alguma das verificações especificada no REQ-4.4.2-01 falhar:

— o processo é interrompido,

— a assinatura deve ser tecnicamente considerada indeterminada, ou seja, não é uma assinatura eletrónica qualificada da UE nem um selo eletrónico qualificado da UE,

— o resultado acima referido e os resultados dos processos de todos os processos intermédios devem ser tidos em conta no relatório de verificação das regras de aplicabilidade da assinatura.