2025/1929

30.9.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/1929 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 à vinculação da data e da hora aos dados e à determinação da exatidão das fontes horárias para o fornecimento de selos temporais 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 42.º, n.º 2,

Considerando o seguinte:

(1) Os selos temporais qualificados desempenham um papel crucial no ambiente digital ao promoverem a transição dos processos tradicionais em suporte papel para equivalentes eletrónicos. Ao vincularem a informação sobre data e hora a dados eletrónicos, os selos temporais qualificados ajudam a assegurar a exatidão da data e da hora que indicam e a integridade dos documentos digitais aos quais a data e a hora estão vinculadas.

(2) A presunção de conformidade estabelecida no artigo 42.º, n.º 1-A, do Regulamento (UE) n.º 910/2014 só deve aplicar-se quando os serviços de confiança qualificados para a emissão de selos temporais 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, da vinculação da data e da hora aos dados e da exatidão da fonte horária.

(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 de execução, 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.

(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.

([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).

([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).

(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

As normas de referência e especificações a que se refere o artigo 42.º, n.º 2, do Regulamento (UE) n.º 910/2014 constam do anexo do presente regulamento.

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 29 de setembro de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

([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 de normas de referência e especificações para serviços de selos temporais qualificados

Aplicam-se as normas ETSI EN 319 421 V1.3.1 ([1]) («ETSI EN 319 421») e ETSI EN 319 422 V1.1.1 ([2]) («ETSI EN 319 422»), com as seguintes adaptações:

1) Para a norma ETSI EN 319 421

1) 2.1 Referências normativas

— [3] 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).

— [4] 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].

— [5] ETSI EN 319 422 V1.1.1 (2016-03) «Electronic Signatures Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles» [Assinaturas eletrónicas e infraestruturas (ESI); perfis de protocolo de validação cronológica e de fichas de selos temporais].

— [6] Nulo e sem efeito.

— [9] 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]).

— [10] Regulamento de Execução (UE) 2024/482 da Comissão ([4]), de 31 de janeiro de 2024, 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).

— [11] Regulamento de Execução (UE) 2024/3144 da Comissão ([5]), de 18 de dezembro de 2024, que altera o Regulamento de Execução (UE) 2024/482 no respeitante às normas internacionais aplicáveis e que retifica esse regulamento de execução.

2) 3.1 Termos

— Período de validade do certificado: intervalo de tempo entre «notBefore» (não antes) e «notAfter» (não depois), inclusive, durante o qual a autoridade de certificação (CA) garante que conserva informações sobre o estado de validade do certificado.

3) 3.3 Abreviaturas

— EUCC: Sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns.

4) 6.2 Declaração de práticas dos serviços de confiança

— OVR-6.2-03 A autoridade de validação cronológica (TSA) deve incluir declarações sobre a disponibilidade do seu serviço de validação cronológica na respetiva declaração de divulgação da TSA.

5) 7.3 Segurança do pessoal

— OVR-7.3-02 O pessoal da TSA 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-7.3-03 A conformidade com o OVR-7.3-02 deve incluir atualizações regulares (pelo menos a cada 12 meses) sobre as novas ameaças e as atuais práticas de segurança.

([1]) EN 319 421 — «Electronic Signatures and Trust Infrastructures (ESI) — Policy and Security Requirements for Trust Service Providers issuing Time Stamps», V1.3.1. [Assinaturas eletrónicas e infraestruturas de confiança (ESI) — Requisitos de política e de segurança para os prestadores de serviços de confiança que emitem selos temporais].

([2]) EN 319 422 — «Electronic Signatures and Infrastructures (ESI) — Time-stamping protocol and time-stamp token profiles», V1.1.1 (2016-03), [Assinaturas eletrónicas e infraestruturas (ESI) — Perfis de protocolo de validação cronológica e de fichas de selos temporais] https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.

([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

([4]) JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

([5]) JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Geração de chaves da unidade de validação cronológica (TSU)

— TIS-7.6.2-03 A geração da(s) chave(s) da TSU deve ser realizada 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 [3] 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 [10] [11] e certificado com o nível EAL 4 ou superior; ou

c) Até 31.12.2030, FIPS PUB 140-3 [7] 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 [10] [11], esse dispositivo deve ser configurado e utilizado em conformidade com essa certificação.

— TIS-7.6.2-04 nulo e sem efeito.

— NOTA 3 nula e sem efeito.

— TIS-7.6.2-05A O algoritmo de geração de chaves da TSU, o tamanho da chave de assinatura resultante e o algoritmo de assinatura utilizado para assinar selos temporais e certificados de chave pública da TSU, respetivamente, devem estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança [9] e publicados pela ENISA.

— NOTA 4 nula e sem efeito.

— TIS-7.6.2-06 A chave de assinatura de uma TSU 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) 7.6.3 Proteção de chaves privadas da TSU

— TIS-7.6.3-02 A chave privada da TSU 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 [3] ou nos Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, versão CC:2002, 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 sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC) [10] [11] e certificado de acordo com o nível EAL 4 ou superior; ou

c) Até 31.12.2030, FIPS PUB 140-3 [7] 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 [10] [11], esse dispositivo deve ser configurado e utilizado em conformidade com essa certificação.

— TIS-7.6.3-03 nulo e sem efeito.

— NOTA 2 nula e sem efeito.

8) 7.6.7 Final do ciclo de vida da chave da TSU

— TIS-7.6.7-03A A data de expiração das chaves privadas da TSU deve estar em conformidade com os mecanismos criptográficos acordados [9].

— NOTA 1 nula e sem efeito.

9) 7.10 Segurança da rede

— OVR-7.10-05 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-7.10-06 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-7.10-07 As barreiras de segurança devem ser configuradas de modo a impedir todos os protocolos e acessos não necessários para a operação da TSA.

10) 7.14 Cessação e planos de cessação da TSA

— OVR-7.14-01A O plano de cessação do prestador de serviços de confiança (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.4].

2) Para a norma ETSI EN 319 422

1) 2.1 Referências normativas

— [5] Nulo e sem efeito.

— [6] Nulo e sem efeito.

— [8] Grupo Europeu para a Certificação da Cibersegurança, subgrupo para a criptografia: «Agreed Cryptographic Mechanisms» (Mecanismos criptográficos acordados).

— [9] RFC 9110 «HTTP Semantics» (Semântica do HTTP).

2) 4.1.3 Algoritmos de dispersão a utilizar

— Aplica-se a seguinte cláusula:

Os algoritmos de dispersão utilizados para efetuar a dispersão das informações a assinar com a data/ /hora, a duração prevista do selo temporal e as funções de dispersão selecionadas em relação ao tempo devem 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.

3) 4.2.3 Algoritmos a suportar

— Aplica-se a seguinte cláusula:

Os algoritmos de assinatura das fichas de selos temporais a suportar devem 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.

4) 4.2.4 Tamanhos de chave a suportar

— Aplica-se a seguinte cláusula:

Os tamanhos de chave do algoritmo de assinatura para o algoritmo de assinatura selecionado devem estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA.

— NOTA nula e sem efeito.

5) 5.1.3 Algoritmos a suportar

— Aplica-se a seguinte cláusula:

Os algoritmos de dispersão para os dados do selo temporal a suportar, a duração prevista do selo temporal e as funções de dispersão selecionadas em relação ao tempo devem 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.

6) 5.2.3 Algoritmos a utilizar

— Aplica-se a seguinte cláusula:

Os algoritmos de dispersão utilizados para efetuar a dispersão das informações a assinar com a data/ /hora e os algoritmos de assinatura das fichas de selos temporais devem 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.

7) 6.3 Requisitos de tamanho de chave

— Aplica-se a seguinte cláusula:

O tamanho de chave para o algoritmo de assinatura selecionado para o certificado da TSU 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.

8) 6.5 Requisitos de algoritmo

— Aplica-se a seguinte cláusula:

A chave pública da TSU e a assinatura do certificado da TSU devem utilizar os algoritmos conformes 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 Perfis dos protocolos de transporte a suportar

— O cliente e o servidor da validação cronológica devem suportar o protocolo de validação cronológica via HTTPS [9], tal como definido na cláusula 3.4 do RFC 3161 do IETF [1].

10) 8 Identificadores de objeto dos algoritmos criptográficos

— Aplica-se a seguinte cláusula:

A chave pública da TSU e a assinatura do certificado da TSU devem utilizar algoritmos em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [8].

11) 9.1 Declaração de conformidade do regulamento

— Se uma ficha de selo temporal for classificada pela TSA como um selo temporal qualificado em conformidade com o Regulamento (UE) n.º 910/2014 [i.2], deve incluir uma instância da extensão «qcStatements» no campo da extensão da ficha de selo temporal com a sintaxe definida na cláusula 3.2.6 do RFC 3739 do IETF [i.3].

— A extensão «qcStatements» deve incluir uma instância da declaração «esi4-qtstStatement-1», tal como definido no anexo B.

— A extensão «qcStatements» não deve ser assinalada como crítica.