Jornal Oficial
da União Europeia

PT
Série L

2025/1943

30.9.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/1943 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 às normas de referência para certificados qualificados de assinaturas eletrónicas e certificados qualificados de selos eletrónicos

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 28.º, n.º 6, e o artigo 38.º, n.º 6,

Considerando o seguinte:

(1) Os certificados qualificados de assinaturas eletrónicas e os certificados qualificados de selos eletrónicos desempenham um papel crucial no ambiente empresarial digital ao promoverem a transição dos processos tradicionais em suporte papel para equivalentes eletrónicos. Ao ligar os dados de validação da assinatura eletrónica ou os dados de validação do selo eletrónico a uma pessoa singular ou coletiva, respetivamente, e ao confirmar o nome dessa pessoa, os certificados qualificados reforçam a certeza quanto à identidade do signatário e do criador do selo.

(2) A presunção de conformidade estabelecida no artigo 28.º, n.º 6, e no artigo 38.º, n.º 6, do Regulamento (UE) n.º 910/2014 só deve aplicar-se quando os serviços de confiança qualificados para a emissão de certificados qualificados de assinaturas eletrónicas e os serviços de confiança qualificados para a emissão de certificados qualificados de selos eletrónicos 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 dos serviços de confiança qualificados e do conteúdo dos certificados qualificados.

(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.

(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

Normas de referência e especificações para certificados qualificados de assinaturas eletrónicas e selos eletrónicos

1. As normas de referência e especificações a que se refere o artigo 28.º, n.º 6, do Regulamento (UE) n.º 910/2014 constam do anexo I do presente regulamento.

2. As normas de referência e especificações a que se refere o artigo 38.º, n.º 6, do Regulamento (UE) n.º 910/2014 constam do anexo II 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

([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 I

Lista de normas de referência e especificações para certificados qualificados de assinaturas eletrónicas

Aplicam-se as normas ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2») e ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5»), com as seguintes adaptações:

1) Para a norma ETSI EN 319 411-2

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 EN 319 411-1 V1.5.1 (2025-04) «Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); requisitos de política e de segurança para os prestadores de serviços de confiança que emitem certificados; parte 1: requisitos gerais], com as seguintes adaptações:

A cláusula 2.1, referências normativas, da norma ETSI EN 319 411-1 V1.5.1 é alterada do seguinte modo:

— [9] 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].

— [10] ETSI EN 319 412-2 V2.4.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 2: perfil de certificado para certificados emitidos a pessoas singulares].

— [14] ETSI EN 319 412-1 V1.6.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 1: descrição geral e estruturas de dados comuns].

— [3] ETSI EN 319 412-5 V2.5.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 5: «QCStatements»].

— [5] ETSI EN 319 412-1 V1.6.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 1: descrição geral e estruturas de dados comuns].

— [6] CEN/TS 419261:2015 «Security requirements for trustworthy systems managing certificates and time-stamps» (Requisitos de segurança para sistemas fiáveis de gestão de certificados e selos temporais).

— [7] 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) ([1]).

— [8] Regulamento de Execução (UE) 2024/482 da Comissão ([2]), 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).

— [9] Regulamento de Execução (UE) 2024/3144 da Comissão ([3]), que altera o Regulamento de Execução (UE) 2024/482 no respeitante às normas internacionais aplicáveis e que retifica esse regulamento de execução.

— [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).

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

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

2) 5.2 Requisitos relativos à declaração de práticas de certificação

— OVR-5.2-02 As políticas de certificação (CP) identificadas pela documentação do prestador de serviços de confiança (TSP) devem especificar os requisitos relativos aos perfis de certificados a utilizar.

3) 5.3 Nome e identificação da política de certificação

— OVR-5.3-01 Se forem introduzidas alterações numa CP, tal como descrita na cláusula 4.2.2, que afetem a aplicabilidade, o identificador da política deve ser alterado.

4) 6.1 Responsabilidades em matéria de publicação e criação de repositórios

— OVR-6.1-02 As informações identificadas no DIS-6.1-04 da norma ETSI EN 319 411-1 [2] devem estar disponíveis pública e internacionalmente.

5) 6.2.2 Validação inicial de identidade

— REG-6.2.2-01A A recolha de atributos e elementos de prova sobre a identidade do sujeito, bem como a respetiva validação, deve ser especificada em conformidade com os atos de execução adotados nos termos do artigo 24.º, n.º 1-C, do Regulamento (UE) n.º 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] e [QCP-n-qscd] A identidade da pessoa singular e, se aplicável, quaisquer atributos específicos dessa pessoa devem ser verificados em conformidade com os atos de execução adotados nos termos do artigo 24.º, n.º 1-C, do Regulamento (UE) n.º 910/2014 [i.1].

— NOTA 1 nula e sem efeito.

6) 6.3.3 Emissão do certificado

— GEN-6.3.3-01 São aplicáveis os requisitos GEN-6.3.3-01 a GEN-6.3.3-10 identificados na norma ETSI EN 319 411-1 [2], cláusula 6.3.3.

— GEN-6.3.3-02 [CONDICIONAL] Se for emitido um certificado a uma pessoa singular identificada em associação com a pessoa coletiva, os atributos do sujeito que identificam a organização no certificado representam a pessoa coletiva ou subentidade dessa pessoa coletiva e o identificador do sujeito no certificado é a pessoa singular.

— GEN-6.3.3-03 O identificador da CP é [OPÇÃO]:

a) [QCP-n]

— conforme especificado na cláusula 5.3, alínea a), e/ou

— um identificador de objeto (OID), atribuído pelo TSP, por outras partes interessadas pertinentes ou por uma normalização posterior para uma política de certificação que reforce os requisitos de política aplicáveis correspondentes definidos no presente documento.

b) [QCP-n-qscd]

— conforme especificado na cláusula 5.3, alínea c), e/ou

— um OID, atribuído pelo TSP, por outras partes interessadas pertinentes ou por uma normalização posterior para uma política de certificação que reforce os requisitos de política aplicáveis correspondentes definidos no presente documento.

7) 6.3.5 Utilização de certificados e de pares de chaves

— SDP-6.3.5-02A [CONDICIONAL] Se gerir o dispositivo de criação de assinaturas qualificadas (QSCD) para o sujeito, o TSP deve ser um prestador qualificado de serviços de confiança que fornece um serviço de confiança qualificado para a gestão de um dispositivo qualificado de criação de assinaturas eletrónicas à distância, em conformidade com o Regulamento (UE) n.º 910/2014 [i.1].

— SDP-6.3.5-11A As obrigações do assinante (ver cláusula 6.3.4) incluem, se o assinante ou o sujeito gerar as chaves do sujeito:

a) A obrigação de gerar as chaves do sujeito através de um algoritmo conforme com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança [7] e publicados pela ENISA para as utilizações da chave certificada, tal como identificado na CP;

b) A obrigação de utilizar o tamanho de chave e um algoritmo conforme com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança [7] e publicados pela ENISA para as utilizações da chave certificada, tal como identificado na CP, durante o período de validade do certificado.

8) 6.3.10 Serviços relativos ao estado do certificado

— CSS-6.3.10-08 [CONDICIONAL] Se forem fornecidas listas de revogação de certificados (CRL), o TSP deve preservar a integridade e a disponibilidade da última lista pelo menos durante o período especificado na declaração de práticas de certificação (CPS), conforme exigido em CSS-6.3.10-12.

9) 6.4.4 Controlos do pessoal

— OVR-6.4.4-02 O pessoal do TSP 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-6.4.4-03 A conformidade com o OVR-6.4.4-02 deve incluir atualizações regulares (pelo menos a cada 12 meses) sobre as novas ameaças e as atuais práticas de segurança.

— OVR-6.4.4-04 Para além das funções de confiança identificadas na norma ETSI EN 319 401 [1] (cláusula 7.2-15), devem ser suportadas as funções de confiança dos agentes de registo e de revogação com responsabilidades definidas na norma TS 419261 [6]. Nos casos em que o prestador qualificado de serviços de confiança (QTSP) é gerido diretamente ou operado em nome de um Estado-Membro ou de um organismo do setor público, essas funções de confiança adicionais podem ser desempenhadas por um ou mais representantes formais que atuem em nome e por conta dos agentes de registo e revogação que exerçam funções nas administrações locais ou regionais.

10) 6.4.9 Cessação pela autoridade de certificação (CA) ou pela autoridade de registo (RA)

— OVR-6.4.9-02 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.1].

11) 6.5.1 Instalação e geração de pares de chaves

— OVR-6.5.1-01A A geração de pares de chaves pela CA deve ser realizada utilizando um algoritmo conforme com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [7] para efeitos de assinatura da CA.

— OVR-6.5.1-01B O tamanho da chave e o algoritmo selecionados para a chave de assinatura da CA devem estar em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [7] para efeitos de assinatura da CA.

— OVR-6.5.1-01C [CONDICIONAL] Se a CA gerar as chaves do sujeito, estas devem estar em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [7] para os fins indicados na CP durante o período de validade do certificado.

12) 6.5.2 Proteção de chaves privadas e controlos da engenharia de módulos criptográficos

— GEN-6.5.2-01 São aplicáveis todos os requisitos identificados na norma ETSI EN 319 411-1 [2], cláusula 6.5.2, exceto os requisitos OVR-6.5.2-01, OVR-6.5.2-03 e OVR-6.5.2-04.

— GEN-6.5.2-02 A geração de pares de chaves do TSP, incluindo as chaves utilizadas por serviços de revogação e registo, deve ser realizada num dispositivo criptográfico seguro que seja um sistema fiável certificado em conformidade com:

— 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: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

— o sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC) [8] [9] e certificado com o nível EAL 4 ou superior, ou

— até 31.12.2030, FIPS PUB 140-3 [11] 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 beneficiar de uma certificação EUCC [8] [9], esse dispositivo deve ser configurado e utilizado em conformidade com essa certificação.

— GEN-6.5.2-03 A chave de assinatura privada da CA deve ser mantida e utilizada num dispositivo criptográfico seguro que cumpra os requisitos GEN-6.5.2-01 e GEN-6.5.2-02.

13) 6.5.7 Controlos de segurança da rede

— OVR-6.5.7-02 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-6.5.7-03 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-6.5.7-04 As barreiras de segurança devem ser configuradas de modo a impedir todos os protocolos e acessos não necessários para a operação do TSP.

14) 6.6.1 Perfil do certificado

— GEN-6.6.1-05 O certificado deve incluir um dos identificadores de política identificados em GEN-6.3.3-03 [OPÇÃO]. O certificado pode incluir outros OID atribuídos pelo TSP.

2) Para a norma ETSI EN 319 412-2

1) 2.1 Referências normativas

— [2] ETSI EN 319 412-5 V2.5.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 5: «QCStatements»].

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

2) 4.2.2 Assinatura

— GEN-4.2.2-2 O algoritmo de assinatura deve ser selecionado em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [9].

— NOTA nula e sem efeito.

3) 4.2.3.1 Pessoas coletivas emitentes

— GEN-4.2.3.1-3 Se for conhecida a existência de um número de registo adequado, a identidade do emitente deve conter o atributo «organizationIdentifier» (identificador da organização) com um valor desse número de registo, tal como indicado no registo oficial correspondente que estabelece esse número de registo.

4) 4.2.5 Informações sobre a chave pública do sujeito

— GEN-4.2.5-2 A chave pública do sujeito deve ser selecionada em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [9].

— NOTA nula e sem efeito.

5) 4.2.6 Número de série

— GEN-4.2.6-01 O «serialNumber» (número de série) do certificado (conforme especificado em IETF RFC 5280 [1] cláusula 4.1.2.2) deve ser único para cada certificado emitido pelo TSP.

ANEXO II

Lista de normas de referência e especificações para certificados qualificados de selos eletrónicos

Aplicam-se as normas ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-3 V1.3.1 («ETSI EN 319 412-3»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2») e ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5»), com as seguintes adaptações:

1) Para a norma ETSI EN 319 411-2

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 EN 319 411-1 V1.5.1 (2025-04) «Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); requisitos de política e de segurança para os prestadores de serviços de confiança que emitem certificados; parte 1: requisitos gerais], com as seguintes adaptações:

A cláusula 2.1, referências normativas, da norma ETSI EN 319 411-1 V1.5.1 é alterada do seguinte modo:

— [9] 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].

— [10] ETSI EN 319 412-2 V2.4.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 2: perfil de certificado para certificados emitidos a pessoas singulares].

— [14] ETSI EN 319 412-1 V1.6.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 1: descrição geral e estruturas de dados comuns].

— [3] ETSI EN 319 412-5 V2.5.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 5: «QCStatements»].

— [5] ETSI EN 319 412-1 V1.6.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 1: descrição geral e estruturas de dados comuns].

— [6] CEN/TS 419261:2015 «Security requirements for trustworthy systems managing certificates and time-stamps» (Requisitos de segurança para sistemas fiáveis de gestão de certificados e selos temporais) (produzidos pela CEN).

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

— [8] Regulamento de Execução (UE) 2024/482, 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).

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

— [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).

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

2) 5.2 Requisitos relativos à declaração de práticas de certificação

— OVR-5.2-02 As CP identificadas pela documentação do TSP devem especificar os requisitos relativos aos perfis de certificados a utilizar.

3) 5.3 Nome e identificação da política de certificação

— OVR-5.3-01 Se forem introduzidas alterações numa CP, tal como descrita na cláusula 4.2.2, que afetem a aplicabilidade, o identificador da política deve ser alterado.

4) 6.1 Responsabilidades em matéria de publicação e criação de repositórios

— OVR-6.1-02 As informações identificadas no DIS-6.1-04 da norma ETSI EN 319 411-1 [2] devem estar disponíveis pública e internacionalmente.

5) 6.2.2 Validação inicial de identidade

— REG-6.2.2-01A A recolha de atributos e elementos de prova sobre a identidade do sujeito, bem como a respetiva validação, deve ser especificada em conformidade com os atos de execução adotados nos termos do artigo 24.º, n.º 1-C, do Regulamento (UE) n.º 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] e [QCP-l-qscd] A identidade da pessoa coletiva e, se aplicável, quaisquer atributos específicos dessa pessoa devem ser verificados em conformidade com os atos de execução adotados nos termos do artigo 24.º, n.º 1-C, do Regulamento (UE) n.º 910/2014 [i.1].

— NOTA 3 Ver nota 2.

6) 6.3.3 Emissão do certificado

— GEN-6.3.3-01 São aplicáveis os requisitos GEN-6.3.3-01 a GEN-6.3.3-10 identificados na norma ETSI EN 319 411-1 [2], cláusula 6.3.3.

— GEN-6.3.3-02 O identificador da CP é [OPÇÃO]:

a) [QCP-1]

— conforme especificado na cláusula 5.3, alínea b), e/ou

— um OID, atribuído pelo TSP, por outras partes interessadas pertinentes ou por uma normalização posterior para uma política de certificação que reforce os requisitos de política aplicáveis correspondentes definidos no presente documento.

b) [QCP-1-qscd]

— conforme especificado na cláusula 5.3, alínea d), e/ou

— um OID, atribuído pelo TSP, por outras partes interessadas pertinentes ou por uma normalização posterior para uma política de certificação que reforce os requisitos de política aplicáveis definidos no presente documento.

7) 6.3.5 Utilização de certificados e de pares de chaves

— SDP-6.3.5-02A [CONDICIONAL] Se gerir o QSCD para o sujeito, o TSP deve ser um prestador qualificado de serviços de confiança que fornece um serviço de confiança qualificado para a gestão de um dispositivo qualificado de criação de selos eletrónicos à distância, em conformidade com o Regulamento (UE) n.º 910/2014 [i.1].

— SDP-6.3.5-11A As obrigações do assinante (ver cláusula 6.3.4) incluem, se o assinante ou o sujeito gerar as chaves do sujeito:

a) A obrigação de gerar as chaves do sujeito através de um algoritmo conforme com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [7] para as utilizações da chave certificada, tal como identificado na CP; e

b) A obrigação de utilizar o tamanho de chave e um algoritmo conforme com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [7] para as utilizações da chave certificada, tal como identificado na CP, durante o período de validade do certificado.

8) 6.3.10 Serviços relativos ao estado do certificado

— CSS-6.3.10-08 [CONDICIONAL] Se forem fornecidas CRL, o TSP deve preservar a integridade e a disponibilidade da última lista pelo menos durante o período especificado na CPS, conforme exigido em CSS-6.3.10-12.

9) 6.4.4 Controlos do pessoal

— OVR-6.4.4-02 O pessoal do TSP 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-6.4.4-03 A conformidade com o OVR-6.4.4-02 deve incluir atualizações regulares (pelo menos a cada 12 meses) sobre as novas ameaças e as atuais práticas de segurança.

— OVR-6.4.4-04 Para além das funções de confiança identificadas na norma ETSI EN 319 401 [1] (cláusula 7.2-15), devem ser suportadas as funções de confiança dos agentes de registo e de revogação com responsabilidades definidas na norma TS 419261 [6]. Nos casos em que o prestador QTSP é gerido diretamente ou operado em nome de um Estado-Membro ou de um organismo do setor público, essas funções de confiança adicionais podem ser desempenhadas por um ou mais representantes formais que atuem em nome e por conta dos agentes de registo e revogação que exerçam funções nas administrações locais ou regionais.

10) 6.4.9 Cessação pela CA ou pela RA

— OVR-6.4.9-02 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.1].

11) 6.5.1 Instalação e geração de pares de chaves

— OVR-6.5.1-01A A geração de pares de chaves pela CA deve ser realizada utilizando um algoritmo conforme com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [7] para efeitos de assinatura da CA.

— OVR-6.5.1-01B O tamanho da chave e o algoritmo selecionados para a chave de assinatura da CA devem estar em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [7] para efeitos de assinatura da CA.

— OVR-6.5.1-01C [CONDICIONAL] Se a CA gerar as chaves do sujeito, estas devem estar em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [7] para os fins indicados na CP durante o período de validade do certificado.

12) 6.5.2 Proteção de chaves privadas e controlos da engenharia de módulos criptográficos

— GEN-6.5.2-01 São aplicáveis todos os requisitos identificados na norma ETSI EN 319 411-1 [2], cláusula 6.5.2, exceto os requisitos OVR-6.5.2-01, OVR-6.5.2-03 e OVR-6.5.2-04.

— GEN-6.5.2-02 A geração de pares de chaves do TSP, incluindo as chaves utilizadas por serviços de revogação e registo, deve ser realizada num dispositivo criptográfico seguro que seja um sistema fiável certificado em conformidade com:

  — 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: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

  — o sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC) [8] [9] e certificado com o nível EAL 4 ou superior, ou

  — até 31.12.2030, FIPS PUB 140-3 [11] 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 beneficiar de uma certificação EUCC [8] [9], esse dispositivo deve ser configurado e utilizado em conformidade com essa certificação.

— GEN-6.5.2-03 A chave de assinatura privada da CA deve ser mantida e utilizada num dispositivo criptográfico seguro que cumpra os requisitos GEN-6.5.2-01 e GEN-6.5.2-02.

13) 6.5.7 Controlos de segurança da rede

— OVR-6.5.7-02 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-6.5.7-03 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-6.5.7-04 As barreiras de segurança devem ser configuradas de modo a impedir todos os protocolos e acessos não necessários para a operação do TSP.

14) 6.6.1 Perfil do certificado

— GEN-6.6.1-05 O certificado deve incluir um dos identificadores de política identificados em GEN-6.3.3-02 [OPÇÃO].

2) Para a norma ETSI EN 319 412-3

1) 2.1 Referências normativas

— [2] ETSI EN 319 412-2 V2.4.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 2: perfil do certificado para certificados emitidos a pessoas singulares].

2) 4.2.1 Sujeito

— LEG-4.2.1-6 O atributo «organizationIdentifier» deve conter uma identificação da organização sujeito diferente do nome da organização. Se for conhecida a existência de um número de registo adequado, o atributo «organizationIdentifier» deve conter um valor desse número de registo, tal como indicado no registo oficial correspondente que estabelece esse número de registo.

3) Para a norma ETSI EN 319 412-2:

1) 2.1 Referências normativas

— [2] ETSI EN 319 412-5 V2.5.1 «Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 5: «QCStatements»].

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

2) 2.2 Referências informativas

— [i.7] nulo e sem efeito.

3) 4.2.2 Assinatura

— GEN-4.2.2-2 O algoritmo de assinatura deve ser selecionado em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [9].

— NOTA nula e sem efeito.

4) 4.2.3.1 Pessoas coletivas emitentes

— GEN-4.2.3.1-3 Se for conhecida a existência de um número de registo adequado, a identidade do emitente deve conter o atributo «organizationIdentifier» com um valor desse número de registo, tal como indicado no registo oficial correspondente que estabelece esse número de registo.

5) 4.2.5 Informações sobre a chave pública do sujeito

— GEN-4.2.5-2 A chave pública do sujeito deve ser selecionada em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [9].

— NOTA nula e sem efeito.

6) 4.2.6 Número de série

— GEN-4.2.6-01 O «serialNumber» do certificado (conforme especificado em IETF RFC 5280 [1] cláusula 4.1.2.2) deve ser único para cada certificado emitido pelo TSP.