Jornal Oficial
da União Europeia

PT
Série L

2025/1942

30.9.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/1942 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 validação de assinaturas eletrónicas qualificadas e aos serviços qualificados de validação 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 33.º, n.º 2, e o artigo 40.º,

Considerando o seguinte:

(1) Os serviços qualificados de validação de assinaturas eletrónicas qualificadas e de selos eletrónicos qualificados asseguram a integridade, a autenticidade e a correção do processo e dos resultados da validação das assinaturas eletrónicas qualificadas e dos selos eletrónicos qualificados, respetivamente. Esses serviços de confiança qualificados desempenham um papel crucial no ambiente empresarial digital ao promoverem a transição dos processos tradicionais em suporte papel para equivalentes eletrónicos.

(2) A presunção de conformidade estabelecida no artigo 33.º, n.º 2, e no artigo 40.º do Regulamento (UE) n.º 910/2014 só deve aplicar-se quando os serviços qualificados de validação de assinaturas eletrónicas qualificadas e de selos eletrónicos qualificados cumprirem as normas técnicas estabelecidas no presente regulamento. Essas 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, bem como a capacidade de verificar o estatuto de qualificado e a validade técnica das assinaturas eletrónicas qualificadas e dos selos eletrónicos 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.

([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 33.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 de normas de referência e especificações aplicáveis a serviços qualificados de validação de assinaturas eletrónicas qualificadas e a serviços qualificados de validação de selos eletrónicos qualificados

Aplicam-se as normas ETSI TS 119 441 V1.2.1 (2023-10) ([1]) («ETSI TS 119 441») e ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) («ETSI TS 119 172-4»), com as seguintes adaptações:

1) Para a norma ETSI TS 119 441

1) 2.1 Referências normativas

— [1] 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] 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].

— [3] 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 de criação e validação de assinaturas digitais AdES; parte 1: criação e validação].

— [4] ISO/IEC 15408-1:2022 — «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].

— [5] Nulo e sem efeito.

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

— [7] Regulamento de Execução (UE) 2024/482 da Comissão, 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) ([3]).

— [8] 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].

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) «Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report» [Assinaturas eletrónicas e infraestruturas (ESI); procedimentos de criação e validação de assinaturas digitais AdES; parte 2: relatório de validação de assinaturas].

— [10] 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) ([4]).

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

— [12] ETSI EN 319 411-1 «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].

([1]) ETSI TS 119 441 — «Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services», V1.2.1 (2023-10) [Assinaturas eletrónicas e infraestruturas (ESI); requisitos de políticas para o prestador de serviços de confiança (TSP) que fornece serviços de validação de assinaturas].

([2]) ETSI TS 119 172-4 — «Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists», V1.1.1 (2021-05) [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].

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

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

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

2) 2.2 Referências informativas

— [i.11] Nulo e sem efeito.

3) 3.3 Abreviaturas

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

4) 4.3.3 Processo

— NOTA 10 Ver ETSI EN 319 102-1 [3] para obter orientações e ETSI TS 119 172-4 [8] para obter orientações adicionais para o caso da assinatura ou do selo qualificado da UE.

5) 6.1 Declaração de práticas do serviço de validação de assinaturas (SVS)

— OVR-6.1-02 A declaração de práticas do SVS deve estar estruturada de acordo com o anexo A.

— OVR-6.1-03 A declaração de práticas do SVS deve enumerar ou fazer referência às políticas do SVS apoiadas [por exemplo, através de identificadores de objeto (OID)] e descrevê-las sucintamente.

6) 6.3 Política de segurança da informação

— OVR-6.3-02 A política de segurança deve documentar os controlos de segurança e privacidade aplicados para proteger os dados pessoais.

7) 7.2 Recursos humanos

— OVR-7.2-02 O pessoal do prestador do serviço de validação de assinaturas (SVSP) 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.

8) 7.5 Controlos criptográficos

— OVR-7.5-02 [CONDICIONAL] Quando são assinados relatórios de validação, o certificado público de assinatura do SVSP correspondente à chave de assinatura privada do SVSP deve ser emitido por uma autoridade de certificação (CA) de confiança, em conformidade com a política de certificação NCP+, como especificado na norma ETSI EN 319 411-1 [12]. Deve ser emitido em conformidade com uma política de certificação adequada especificada na norma ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [CONDICIONAL] Quando são assinados relatórios de validação, a chave de assinatura privada do SVSP 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 [4] 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 [7] [11] e certificado com o nível EAL 4 ou superior; ou

c) Até 31.12.2030, FIPS PUB 140-3 [6] 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 [7] [11], esse dispositivo deve ser configurado e utilizado em conformidade com essa certificação.

— OVR-7.5-04 nulo e sem efeito.

— OVR-7.5-06 A chave de assinatura privada de um SVSP 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.

9) 7.7 Segurança operacional

— OVR-7.7-02 Para garantir que os sistemas em que a aplicação é desenvolvida aplicam medidas de segurança adequadas e se adaptam a ambientes de aplicação específicos, a aplicação de validação de assinaturas (SVA) deve utilizar um ambiente de aplicação mantido com correções de segurança atualizadas.

— OVR-7.7-03 Aplicam-se à SVA os seguintes requisitos especificados na norma ETSI TS 119 101 [1], cláusula 5.2: GSM 1.3.

10) 7.8 Segurança da rede

— OVR-7.8-02 Se for permitido o acesso remoto a sistemas de armazenamento ou tratamento de dados confidenciais, deve ser adotada e descrita uma política formal como parte dos elementos exigidos pelo OVR-6.3-02.

— OVR-7.8-04 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-7.8-05 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-7.8-06 As barreiras de segurança devem ser configuradas de modo a impedir todos os protocolos e acessos não necessários para a operação do SVSP.

11) 7.12 Cessação e planos de cessação da prestação do serviço de validação de assinaturas

— OVR-7.12-02 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].

12) 7.14 Cadeia de abastecimento

— OVR-7.14-01 Aplicam-se os requisitos especificados na norma ETSI EN 319 401 [2], cláusula 7.14.

13) 8.1 Processo de validação de assinaturas

— VPR-8.1-07 A SVA deve cumprir os requisitos da norma ETSI TS 119 101 [1], cláusula 7.4., SIA 1 a SIA 4.

— VPR-8.1-11 [CONDICIONAL] Quando o SVS pretender validar assinaturas eletrónicas qualificadas ou selos eletrónicos qualificados em conformidade com o artigo 32.º, n.º 1, (ou o artigo 40.º, respetivamente) do Regulamento (UE) n.º 910/2014 [i.1], o processo de validação deve seguir os requisitos da norma ETSI TS 119 172-4 [8].

14) 8.2 Protocolo de validação de assinaturas

— SVP-8.2-03 A resposta da validação da assinatura contém o OID da política do SVS.

15) 8.4 Relatório de validação de assinaturas

— SVR-8.4-02 O relatório de validação deve estar em conformidade com a norma ETSI TS 119 102-2 [9].

— SVR-8.4-07 [CONDICIONAL] Quando uma política de validação de assinaturas não é totalmente tratada pelo SVS, para além de indicar as restrições validadas, o relatório deve indicar as restrições que tenham sido ignoradas ou anuladas.

— SVR-8.4-15 O relatório de validação deve indicar claramente a origem de cada prova de existência (PoE) (a partir da assinatura, do cliente, do servidor).

— SVR-8.4-16 O relatório de validação deve conter uma assinatura do relatório de validação, que é a assinatura digital do SVSP.

— SVR-8.4-17 [CONDICIONAL] Quando os relatórios de validação são assinados, o formato e o objetivo da assinatura devem estar em conformidade com a norma ETSI TS 119 102-2 [9].

16) 9 Quadro para a definição de políticas de serviços de validação com base numa política de serviços de confiança definida no presente documento:

— OVR-9-05 [CONDICIONAL] Aquando da elaboração de uma política de SVS com base numa política de serviços de confiança definida no presente documento, deve ser realizada uma avaliação dos riscos para avaliar os requisitos operacionais e determinar os requisitos de segurança a incluir na política para a comunidade e a aplicabilidade declaradas.

— OVR-9-06 [CONDICIONAL] Aquando da elaboração de uma política de SVS com base numa política de serviços de confiança definida no presente documento, a política deve ser aprovada e alterada em conformidade com um processo de revisão definido, incluindo as responsabilidades pela manutenção da política.

— OVR-9-07 [CONDICIONAL] Aquando da elaboração de uma política de SVS com base numa política de serviços de confiança definida no presente documento, deve existir um processo de revisão definido para assegurar que a política é apoiada pelas declarações de práticas.

— OVR-9-08 [CONDICIONAL] Aquando da elaboração de uma política de SVS com base numa política de serviços de confiança definida no presente documento, o TSP deve disponibilizar as políticas por si apoiadas à sua comunidade de utentes.

— OVR-9-09 [CONDICIONAL] Aquando da elaboração de uma política de SVS com base numa política de serviços de confiança definida no presente documento, devem ser disponibilizadas aos assinantes as revisões das políticas apoiadas pelo TSP.

17) Anexo B (normativo) Serviço qualificado de validação de assinaturas eletrónicas qualificadas (QES) na aceção do artigo 33.º do Regulamento (UE) n.º 910/2014:

— VPR-B-02 [CONDICIONAL] Se o SVSP for um prestador qualificado de serviços de validação de assinaturas (QSVSP), a implementação deve estar em conformidade com a norma ETSI TS 119 172-4 [8].

— NOTA 2 nula e sem efeito.

— OVR-B-04 [CONDICIONAL] Se o SVSP for um QSVSP, os ensaios previstos no OVR-B-03 devem verificar diferentes casos de utilização, positivos e negativos.

— VPR-B-11 [CONDICIONAL] Se o SVSP for um QSVSP, deve controlar o cálculo de dispersão (executar o cálculo do lado do servidor ou controlar o cliente se tal for permitido do lado do cliente).

— NOTA 5 nula e sem efeito.

— NOTA 6 nula e sem efeito.

— VPR-B-15 [CONDICIONAL] Se o SVSP for um QSVSP, o relatório de validação deve estar em conformidade com a norma ETSI TS 119 102-2 [9] para que os requisitos VPR-B-13 e VPR-B-14 sejam cumpridos.

— VPR-B-16 [CONDICIONAL] Se o SVSP for um QSVSP, a implementação deve estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [10], para a utilização das técnicas criptográficas adequadas durante a prestação de serviços qualificados de validação de QES.

18) Anexo C (informativo) Levantamento dos requisitos do Regulamento (UE) n.º 910/2014, segundo parágrafo da secção relativa ao fornecimento de validação em conformidade com o artigo 32.º, n.º 1:

— para assegurar a verificação de todas as condições exigidas pelo artigo 32.º, n.º 1, e pelo artigo 40.º do Regulamento (UE) n.º 910/2014 [i.1], é necessário um algoritmo de validação correto. Este fornece o mesmo resultado determinístico para uma assinatura ou selo submetido a validação. A política de validação de assinaturas é crucial para este efeito. A norma ETSI TS 119 172-4 [8], baseada no algoritmo de validação especificado na norma ETSI EN 319 102-1 [3], foi emitida nesta perspetiva.

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 de 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 (2024-11) «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 24 horas para o certificado de assinatura. Não é fixado qualquer valor para «RevocationFreshnessConstraints» para certificados que não o certificado de assinatura, incluindo os certificados comprovativos dos selos temporais.

3) 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:

a) O processo é interrompido;

b) A assinatura deve ser tecnicamente considerada indeterminada, ou seja, não é uma assinatura eletrónica qualificada da UE nem um selo eletrónico qualificado da UE;

c) 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.