Jornal Oficial
da União Europeia

PT
Série L

2025/2462

9.12.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/2462 DA COMISSÃO

de 8 de dezembro de 2025

que altera o Regulamento de Execução (UE) 2024/482 no respeitante às definições, à certificação de séries de produtos de TIC, à continuidade da garantia e aos documentos sobre o estado da arte

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) ([1]), nomeadamente o artigo 49.º, n.º 7,

Considerando o seguinte:

(1) O Regulamento de Execução (UE) 2024/482 da Comissão ([2]) especifica as funções, regras e obrigações, bem como a estrutura do sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC), em conformidade com o enquadramento europeu para a certificação da cibersegurança estabelecido no Regulamento (UE) 2019/881.

(2) A Metodologia Comum de Avaliação que acompanha os Critérios Comuns (CC), uma norma internacional de avaliação da segurança da informação, permite a avaliação da segurança dos produtos de TIC para efeitos de certificação. Neste contexto, alguns produtos de TIC podem ser desenvolvidos a partir da mesma base funcional para oferecer funcionalidades de segurança semelhantes em diferentes plataformas ou aparelhos, sendo, no seu conjunto, também designados por «série de produtos». No entanto, a conceção, o *hardware*, o *firmware* ou o *software* podem variar de um produto de TIC para outro. Cabe ao organismo de certificação decidir, caso a caso, se é possível certificar uma série de produtos. As condições para a certificação de séries de produtos poderão ser ilustradas mais pormenorizadamente nas orientações de apoio do EUCC.

(3) A fim de preservar a fiabilidade dos produtos certificados, é essencial definir o que constitui uma alteração importante e uma alteração menor do alvo da avaliação ou do seu ambiente, incluindo o seu ambiente operacional ou de desenvolvimento. Por conseguinte, é necessário precisar essas noções tendo em conta as especificações técnicas existentes e amplamente utilizadas do Grupo de Altos Funcionários para a Segurança dos Sistemas de Informação (SOG-IS) e dos participantes no Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI (ARCC).

(4) As alterações menores caracterizam-se frequentemente pelo seu efeito limitado na declaração de fiabilidade do produto fornecida pelo certificado EUCC emitido. Assim, devem ser geridas no âmbito de procedimentos de manutenção e não exigem uma reavaliação das funcionalidades de segurança do produto. São exemplos de alterações menores que devem ser tratadas no quadro da manutenção, nomeadamente mas não só, as alterações de redação, as alterações do ambiente do alvo de avaliação que não alterem o alvo de avaliação certificado e as alterações do alvo de avaliação certificado que não afetem os elementos de prova da garantia. As alterações do ambiente de desenvolvimento também podem ser consideradas menores, desde que não tenham impacto ulterior nas medidas de garantia existentes. No entanto, podem, em alguns casos, implicar uma avaliação parcial das medidas pertinentes.

([1]) JO L 151 de 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.
([2]) Regulamento de Execução (UE) 2024/482 da Comissão, 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) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Por alteração importante, entende-se qualquer alteração do alvo de avaliação certificado ou do seu ambiente suscetível de afetar negativamente a garantia indicada no certificado EUCC. Por conseguinte, deve exigir uma reavaliação. Entre os exemplos de alterações importantes contam-se as alterações do conjunto de requisitos de garantia declarados, exceto no que diz respeito aos requisitos de garantia da família CC ALC_FLR (correção de falhas); as alterações dos controlos de confidencialidade ou integridade do ambiente de desenvolvimento, sempre que tais alterações possam afetar o desenvolvimento ou a produção seguros do alvo de avaliação ou alterações do alvo de avaliação para resolver uma vulnerabilidade passível de ser explorada. Além disso, um conjunto de alterações menores que, coletivamente, tenham um impacto significativo na segurança também pode ser considerado uma alteração importante. Importa ainda reconhecer que, ainda que a correção de erros incida apenas num aspeto específico do alvo de avaliação, a sua imprevisibilidade e o seu potencial impacto na garantia podem torná-la uma alteração importante se comprometer as garantias de segurança dadas pela certificação.

(6) As alterações no ambiente de ameaças de um produto de TIC certificado inalterado poderão exigir uma reavaliação. Os possíveis resultados desse processo de reavaliação, em particular o seu impacto no certificado EUCC, devem estar claramente estabelecidos. Se uma reavaliação for concluída com êxito, o organismo de certificação deve confirmar o certificado ou emitir um novo certificado com a data de validade prorrogada. Se um processo de reavaliação não for bem-sucedido, o organismo de certificação deve retirar o certificado e, eventualmente, emitir um novo certificado com um âmbito diferente. Essas disposições devem aplicar-se, *mutatis mutandis*, à reavaliação dos perfis de proteção.

(7) O anexo I do Regulamento de Execução (UE) 2024/482 enumera documentos sobre o estado da arte aplicáveis à avaliação de produtos de TIC e perfis de proteção. Esses documentos sobre o estado da arte devem ser atualizados de modo a refletir os últimos desenvolvimentos, relacionados, nomeadamente, com a evolução tecnológica, o panorama das ciberameaças, as práticas do setor ou as normas internacionais. Esta atualização afigura-se oportuna para os documentos sobre o estado da arte relativos aos requisitos mínimos de segurança dos sítios, à aplicação de potenciais de ataque aos cartões inteligentes, à aplicação de potenciais de ataque a dispositivos de *hardware* com caixas de segurança, à aplicação de critérios comuns aos circuitos integrados e à avaliação de produtos compostos para cartões inteligentes e dispositivos similares. Além disso, não estão incluídos os documentos sobre o estado da arte relativos à avaliação e certificação de produtos compostos que utilizam a versão mais recente das normas dos Critérios Comuns, à reutilização dos resultados da avaliação das auditorias no local e às clarificações sobre a interpretação dos perfis de proteção relacionados com dispositivos qualificados de criação de assinaturas eletrónicas, tacógrafos e módulos de segurança físicos. A fim de assegurar uma avaliação uniforme dos produtos de TIC no âmbito do EUCC, deve alterar-se o anexo I de modo a incluir os documentos sobre o estado da arte novos ou atualizados, na sequência da sua aprovação pelo Grupo Europeu para a Certificação da Cibersegurança (GECC).

(8) Além disso, importa aditar ao sistema o documento sobre o estado da arte «ADV_SPM.1 interpretation for CC:2022 transition» [Interpretação de ADV_SPM.1 para a transição para CC:2022], a fim de assegurar que os processos de certificação baseados em perfis de proteção específicos possam continuar a utilizar a modelização formal (ADV_SPM.1) até os perfis de proteção correspondentes serem atualizados, por exemplo, com o aditamento de uma configuração de perfil de proteção de garantia múltipla conforme com os CC:2022 que suporte ADV_SPM.1. A fim de proporcionar ao mercado tempo suficiente para a transição para as normas atualizadas dos Critérios Comuns, é necessário prever disposições transitórias específicas para os perfis de proteção «Security IC Platform PP with Augmentation Packages» [PP para plataformas de circuitos integrados de segurança com pacotes de aumento] (v1.0), BSI-CC-PP-0084-2014, «Java Card System — Closed Configuration» [Sistema Java Card — Configuração fechada] (v3.1), BSI-CC-PP-0101-V2-2020 ou «Java Card System — Open Configuration» [Sistema Java Card — Configuração aberta] (v3.1), BSI-CC-PP-0099-V2-2020. Para evitar perturbações do mercado, convém estabelecer que o documento sobre o estado da arte relativo à interpretação de ADV_SPM.1 para a transição para os CC:2022 é aplicável aos processos de certificação iniciados antes da adoção do presente regulamento. A aplicação deste documento deve, no entanto, limitar-se ao estritamente necessário, tendo em conta o tempo exigido para finalizar a atualização dos perfis de proteção correspondentes. Mais precisamente, para os processos de certificação que utilizam os perfis de proteção «Security IC Platform PP with Augmentation Packages» (v1.0), BSI-CC-PP-0084-2014 ou «Java Card System — Closed Configuration» (v3.1), BSI-CC-PP-0101-V2-2020, o documento sobre o estado da arte deve aplicar-se aos processos iniciados antes de 1 de outubro de 2026. Relativamente aos processos de certificação que utilizam o perfil de proteção «Java Card System — Open Configuration» (v3.1), BSI-CC-PP-0099-V2-2020, o documento sobre o estado da arte deve aplicar-se apenas aos processos iniciados antes da data de entrada em vigor do presente regulamento, tendo em conta que já está disponível uma nova versão deste perfil de proteção.

(9) Uma alteração dos documentos sobre o estado da arte durante um processo de certificação poderia perturbar a avaliação do produto e atrasar a emissão do certificado. Por conseguinte, há que prever disposições transitórias adequadas para os documentos sobre o estado da arte novos ou atualizados, que permitam aos fornecedores, aos ITSEF, aos organismos de certificação e a outras partes interessadas efetuar os ajustamentos necessários. Os documentos sobre o estado da arte aplicáveis, novos ou atualizados, devem dizer respeito aos pedidos de certificação, incluindo os pedidos de reavaliação, devendo ser possível que os processos de certificação em curso continuem a recorrer a versões anteriores dos documentos sobre o estado da arte.

(10) Os anexos II e III do Regulamento de Execução (UE) 2024/482 enumeram, respetivamente, os perfis de proteção certificados nos níveis AVA_VAN 4 ou 5 e os perfis de proteção recomendados. Várias referências estão incompletas ou tornaram-se obsoletas devido a uma atualização dos perfis de proteção. Importa completá-las e, além disso, incluir novas referências para assegurar uma cobertura mais abrangente dos circuitos integrados seguros, dos cartões inteligentes e dos dispositivos conexos e da computação de confiança.

(11) É necessário alterar o artigo 19.º do Regulamento de Execução (UE) 2024/482, a fim de clarificar que o anexo IV se aplica, com as modificações que se impõem, à revisão dos certificados EUCC para perfis de proteção.

(12) Tendo em conta que a meta de segurança é um elemento fundamental para compreender o âmbito de um processo de certificação, é igualmente necessário que a ENISA publique a meta de segurança correspondente a cada certificado EUCC no seu sítio Web.

(13) Os organismos de certificação devem ainda fornecer à ENISA uma versão inglesa da meta de segurança e do relatório de certificação, a fim de permitir à agência disponibilizar essas informações em inglês no sítio Web correspondente, em conformidade com o artigo 42.º, n.º 2, do Regulamento de Execução (UE) 2024/482. Por esse motivo, os requerentes da certificação devem fornecer aos organismos de certificação uma versão inglesa da meta de segurança, sempre que tal lhes seja solicitado.

(14) Não é necessário que a referência ao nome do organismo de certificação figure na identificação única do certificado, uma vez que o número de identificação do organismo de certificação é suficiente para o identificar de forma inequívoca. O mês de emissão também não tem de ser indicado, uma vez que a contagem dos certificados é realizada numa base anual. Por conseguinte, por uma questão de simplificação, esse requisito deve ser suprimido. Uma vez que o ano de emissão do certificado corresponde à emissão do primeiro certificado, essa mesma data deve figurar na identificação única dos certificados emitidos após uma revisão, a fim de assegurar a rastreabilidade.

(15) O Regulamento de Execução (UE) 2024/482 deve, portanto, ser alterado em conformidade.

(16) As medidas previstas no presente regulamento estão em conformidade com o parecer do comité criado pelo artigo 66.º do Regulamento (UE) 2019/881,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

O Regulamento de Execução (UE) 2024/482 é alterado do seguinte modo:

1) Ao artigo 2.º são aditados os seguintes pontos 16, 17 e 18:

«16) "Série de produtos", um conjunto de produtos de TIC de um requerente, desenvolvido a partir da mesma base funcional para dar resposta aos mesmos imperativos de segurança e cuja conceção, *hardware*, *firmware* ou *software* pode variar de um produto de TIC para outro;

17) "Alteração menor", qualquer alteração do alvo de avaliação certificado ou do seu ambiente que não afete negativamente a garantia indicada no certificado EUCC;

18) "Alteração importante", qualquer alteração do alvo de avaliação certificado ou do seu ambiente suscetível de afetar negativamente a garantia indicada no certificado EUCC.»;

2) Ao artigo 5.º é aditado o seguinte n.º 3:

«3. Um organismo de certificação pode autorizar a certificação de uma série de produtos.»;

3) No artigo 9.º, n.º 2, a alínea a) passa a ter a seguinte redação:

«a) Fornecer ao organismo de certificação e ao ITSEF todas as informações necessárias, completas e corretas, bem como as informações adicionais necessárias, se solicitadas, incluindo uma versão inglesa da meta de segurança;»;

4) No artigo 11.º, n.º 3, a alínea b) passa a ter a seguinte redação:

«b) A identificação única do certificado, constituída pelos seguintes elementos:

1) O nome do sistema;

2) O número de identificação, em conformidade com o artigo 3.º do Regulamento de Execução (UE) 2024/3143, do organismo de certificação que emitiu o certificado;

3) O ano de emissão do certificado inicial;

4) O número de identificação atribuído pelo organismo de certificação que emitiu o certificado.»;

5) No artigo 19.º, o n.º 1 passa a ter a seguinte redação:

«1. A pedido do titular do certificado ou por outras razões justificadas, o organismo de certificação pode decidir rever um certificado EUCC para um perfil de proteção. A revisão é efetuada em conformidade com o anexo IV. O organismo de certificação determina o âmbito da revisão. Se necessário para a revisão, o organismo de certificação solicita ao ITSEF que efetue uma reavaliação do perfil de proteção certificado.»;

6) O artigo 42.º é alterado do seguinte modo:

a) Ao n.º 1 é aditada a seguinte alínea i):

«i) A meta de segurança correspondente a cada certificado EUCC.»;

b) O n.º 2 passa a ter a seguinte redação:

«2. As informações a que se refere o n.º 1 são disponibilizadas, pelo menos, em inglês. Para o efeito, os organismos de certificação fornecem à ENISA as versões linguísticas originais dos relatórios de certificação e das metas de segurança, bem como a versão inglesa desses documentos, sem demora injustificada.»;

7) No artigo 48.º, o n.º 4 passa a ter a seguinte redação:

«4. Salvo disposição em contrário no anexo I ou II, os documentos sobre o estado da arte são aplicáveis aos processos de certificação, incluindo a reavaliação, iniciados a partir da data de aplicação do ato modificativo pelo qual os documentos sobre o estado da arte foram incorporados no anexo I ou II.»;

8) O anexo I é substituído pelo texto que consta do anexo I do presente regulamento;

9) O anexo II é substituído pelo texto que consta do anexo II do presente regulamento;

10) O anexo III é substituído pelo texto que consta do anexo III do presente regulamento;

11) O anexo IV é alterado em conformidade com o anexo IV do presente regulamento;

12) O anexo V é alterado em conformidade com o anexo V do presente regulamento;

13) O anexo IX é substituído pelo texto que consta do anexo VI 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 8 de dezembro de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO I

«*ANEXO I*

Documentos sobre o estado da arte que apoiam os domínios técnicos e outros documentos sobre o estado da arte

1. Documentos sobre o estado da arte que apoiam os domínios técnicos nos níveis AVA_VAN 4 ou 5:
   (a) Os seguintes documentos relativos à avaliação harmonizada do domínio técnico "cartões inteligentes e dispositivos similares":
      (1) "Minimum ITSEF requirements for security evaluations of smart cards and similar devices" (Requisitos mínimos dos ITSEF para as avaliações de segurança de cartões inteligentes e dispositivos similares), versão 1.1;
      (2) "Minimum Site Security Requirements" (Requisitos mínimos de segurança dos sítios), versão 2;
      (3) "Reusing evaluation results of site audits (STAR)" [Reutilização dos resultados das avaliações das auditorias no local (STAR)], versão 1;
      (4) "Application of Common Criteria to integrated circuits" (Aplicação dos Critérios Comuns aos circuitos integrados), versão 2;
      (5) "Security Architecture requirements (ADV_ARC) for smart cards and similar devices" [Requisitos de arquitetura de segurança (ADV_ARC) para cartões inteligentes e dispositivos similares], versão 1.1;
      (6) "Certification of 'open' smart card products" (Certificação de produtos de cartões inteligentes "abertos"), versão 1.1;
      (7) "Composite product evaluation for smart cards and similar devices for CC3.1" (Avaliação de produtos compostos para cartões inteligentes e dispositivos similares para CC3.1), versão 2;
      (8) "Composite product evaluation and certification for CC:2022" (Avaliação e certificação de produtos compostos para CC:2022), versão 1;
      (9) "Application of Attack Potential to Smartcards and Similar Devices" (Aplicação do potencial de ataque aos cartões inteligentes e dispositivos similares), versão 2;
      (10) "Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices" (Avaliação da segurança e certificação dos dispositivos qualificados de criação de assinaturas/selos eletrónicos), versão 1;
      (11) "ADV_SPM.1 interpretation for CC:2022 transition" (Interpretação de ADV_SPM.1 para a transição para CC:2022), versão 1.1, aplicável aos processos de certificação que utilizam os perfis de proteção seguintes:
         (a) Perfis de proteção "Security IC Platform PP with Augmentation Packages" (PP para plataformas de circuitos integrados de segurança com pacotes de aumento) (v1.0), BSI-CC-PP-0084-2014, ou "Java Card System — Closed Configuration" (Sistema Java Card — Configuração fechada) (v3.1), BSI-CC-PP-0101-V2-2020, para processos iniciados antes de 1 de outubro de 2026;
         (b) Perfil de proteção "Java Card System — Open Configuration" (Sistema Java Card — Configuração aberta) (v3.1), BSI-CC-PP-0099-V2-2020, para processos iniciados antes de 29 de dezembro de 2025;
   (b) Os seguintes documentos relativos à avaliação harmonizada do domínio técnico "dispositivos de *hardware* com caixas de segurança":
      (1) "Minimum ITSEF requirements for security evaluations of hardware devices with security boxes" (Requisitos mínimos dos ITSEF para as avaliações de segurança de dispositivos de *hardware* com caixas de segurança), versão 1.1;
      (2) "Minimum Site Security Requirements" (Requisitos mínimos de segurança dos sítios), versão 2;
      (3) "Reusing evaluation results of site audits (STAR)" [Reutilização dos resultados das avaliações das auditorias no local (STAR)], versão 1;
      (4) "Application of Attack Potential to hardware devices with security boxes" (Aplicação do potencial de ataque a dispositivos de *hardware* com caixas de segurança), versão 2;
      (5) "Hardware assessment in EN 419221-5 (HSM PP)" [Avaliação do *hardware* na norma EN 419221-5 (HSM PP)], versão 1;
      (6) "JIL Tachograph MS PP Clarification" (Clarificação do PP para sensores de movimentos de tacógrafos da JIL), versão 1.
2. Documentos sobre o estado da arte relativos à acreditação harmonizada dos organismos de avaliação da conformidade:
   (a) "Accreditation of ITSEFs for the EUCC" (Acreditação dos ITSEF para o EUCC), versão 1.1, para acreditações emitidas antes de 8 de julho de 2025;
   (b) "Accreditation of ITSEFs for the EUCC" (Acreditação dos ITSEF para o EUCC), versão 1.6c, para acreditações emitidas pela primeira vez ou revistas após 8 de julho de 2025;
   (c) "Accreditation of CBs for the EUCC" (Acreditação dos OC para o EUCC), versão 1.6b.».

ANEXO II

«*ANEXO II*

Perfis de proteção certificados nos níveis AVA_VAN 4 ou 5

1. Para os dispositivos qualificados de criação de assinaturas e selos à distância:

   (a) EN 419241-2:2019 — "Trustworthy Systems Supporting Server Signing — Part 2: Protection Profile for QSCD for Server Signing" (Sistemas de confiança que suportam assinatura em servidor — Parte 2: Perfil de proteção para QSCD para assinatura em servidor) (v0.16), ANSSI-CC-PP-2018/02-M01;

   (b) EN 419221-5:2018 — "Protection profiles for Trust Service Provider Cryptographic modules — Part 5: Cryptographic Module for Trust Services" (Perfis de proteção para módulos criptográficos de prestadores de serviços de confiança — Parte 5: Módulo criptográfico para serviços de confiança) (v0.15), ANSSI-CC-PP--2016/05-M01.

2. Perfis de proteção adotados como documentos sobre o estado da arte:

   [EM BRANCO].».

ANEXO III

«ANEXO III

Perfis de proteção recomendados

Perfis de proteção utilizados na certificação de produtos de TIC, incluindo produtos dos seguintes domínios técnicos:

1. Cartões inteligentes e dispositivos similares
   - (a) Passaporte:
     - (1) "PP Machine Readable Travel Document with 'ICAO Application' Basic Access Control" (PP para documentos de viagem de leitura ótica no âmbito da "aplicação OACI", Controlo de acesso básico) (v1.10), BSI-CC-PP-0055-2009;
     - (2) "PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP)" [PP para documentos de viagem de leitura ótica utilizando o procedimento de inspeção normalizado com PACE (PACE_PP)] (v1), BSI-CC-PP-0068-V2-2011-MA-01;
     - (3) "PP Machine Readable Travel Document with 'ICAO Application' Extended Access Control with PACE" (PP para documentos de viagem de leitura ótica no âmbito da "aplicação OACI", Controlo de acesso alargado com PACE) (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;
   - (b) Dispositivos seguros de criação de assinaturas (SSCD):
     - (1) EN 419211-2:2013 — "Protection profiles for secure signature creation device — Part 2: Device with key generation" (Perfis de proteção para dispositivos seguros de criação de assinaturas — Parte 2: dispositivos com geração de chaves) (v1.03), BSI-CC-PP-0059-2009-MA-02;
     - (2) EN 419211-3:2013 — "Protection profiles for secure signature creation device — Part 3: Device with key import" (Perfis de proteção para dispositivos seguros de criação de assinaturas — Parte 3: dispositivos com importação de chaves) (v1.0.2), BSI-CC-PP-0075-2012-MA-01;
     - (3) EN 419211-4:2013 — "Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application" (Perfis de proteção para dispositivos seguros de criação de assinaturas — Parte 4: Extensão para dispositivos com geração de chaves e canal de confiança para aplicação de geração de certificados) (v1.0.1), BSI-CC-PP-0071-2012-MA-01;
     - (4) EN 419211-5:2013 — "Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application" (Perfis de proteção para dispositivos seguros de criação de assinaturas — Parte 5: Extensão para dispositivos com geração de chaves e canal de confiança para aplicação de criação de assinaturas) (v1.0.1), BSI-CC-PP-0072-2012-MA-01;
     - (5) EN 419211-6:2014 — "Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application" (Perfis de proteção para dispositivos seguros de criação de assinaturas — Parte 6: Extensão para dispositivos com importação de chaves e canal de confiança para aplicação de criação de assinaturas) (v1.0.4), BSI-CC-PP-0076-2013-MA-01;
   - (c) Tacógrafo: "Digital Tachograph — Tachograph Card (TC PP)" [Tacógrafo digital — cartão tacográfico (TC PP)] (v1.0), BSI-CC-PP-0091-2017;
   - (d) Circuitos integrados seguros, plataforma Java Card e eUICC:
     - (1) "Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations" (Perfil de proteção para plataforma SIM universal Java Card em configuração básica e de SCWS) (v2.0.2), ANSSI-CC-PP-2010/04 (básica), ANSSI-CC-PP-2010/05 (básica e de SCWS);
     - (2) "Security IC Platform PP with Augmentation Packages" (PP para plataformas de circuitos integrados de segurança com pacotes de aumento) (v1.0), BSI-CC-PP-0084-2014;
     - (3) "Embedded UICC (eUICC) for Machine-to-Machine Devices" [Cartão de circuito integrado universal embutido (eUICC) para dispositivos do tipo máquina-máquina] (v1.1), BSI-CC-PP-0089-2015;
     - (4) "Cryptographic Service Provider — CSP" (Prestador de serviços criptográficos — PSC) (v0.9.8), BSI-CC-PP-0104-2019;
     - (5) "Cryptographic Service Provider — Time Stamp Service and Audit (PPC-CSP-TS-Au)" [Prestador de serviços criptográficos — Serviço de selos temporais e auditoria (PPC-CSP-TS-Au)], versão 0.9.5, BSI-CC-PP-0107-2019;
     - (6) "Configuration Cryptographic Service Provider — Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl)" [Configuração para prestador de serviços criptográficos — Serviço de selos temporais, auditoria e agrupamento (PPC-CSP-TS-Au-Cl)], versão 0.9.4, BSI-CC-PP-0108-2019;
     - (7) "Java Card System — Closed Configuration" (Sistema Java Card — Configuração fechada) (v3.1), BSI-CC-PP-0101-V2-2020;
     - (8) "Secure Element Protection Profile — GPC_SPE_174" (Perfil de proteção para elementos seguros) (v1.0), CCN-CC-PP-5-2021;
     - (9) "Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile" [Perfil de proteção para subsistemas seguros em sistemas num chipe (3S in SoC)] (v1.8), BSI-CC-PP-0117-V2-2023;
     - (10) "Java Card System — Open Configuration" (Sistema Java Card — Configuração aberta) (v3.2), BSI-CC-PP-0099-V3-2024;
     - (11) "Embedded UICC for Consumer Devices Protection Profile" (Perfil de proteção para UICC embutidos para dispositivos de consumidores) (v2.1), BSI-CC-PP-0100-V2-2025;
   - (e) Módulo de plataforma de confiança: "Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0; Revision 1.59" (Perfil de proteção para módulo de plataforma de confiança específico de PC cliente, família 2.0, nível 0, revisão 1.59) (v1.3), ANSSI-CC-PP-2021/02.

2. Dispositivos de *hardware* com caixas de segurança

   (a) Pontos de interação (de pagamento) e terminais de pagamento (POI):

      (1) "Point of Interaction 'POI-CHIP-ONLY'" (Ponto de interação "POI-CHIP-ONLY") (v4.0), ANSSI-CC-PP--2015/01;

      (2) "Point of Interaction 'POI-CHIP-ONLY and Open Protocol Package'" (Ponto de interação "Pacote POI--CHIP-ONLY e protocolo aberto") (v4.0), ANSSI-CC-PP-2015/02;

      (3) "Point of Interaction 'POI-COMPREHENSIVE'" (Ponto de interação "POI-COMPREHENSIVE") (v4.0), ANSSI-CC-PP-2015/03;

      (4) "Point of Interaction 'POI-COMPREHENSIVE and Open Protocol Package'" (Ponto de interação "Pacote POI-COMPREHENSIVE e protocolo aberto") (v4.0), ANSSI-CC-PP-2015/04;

      (5) "Point of Interaction 'POI-PED-ONLY'" (Ponto de interação "POI-PED-ONLY") (v4.0), ANSSI-CC-PP--2015/05;

      (6) "Point of Interaction 'POI-PED-ONLY and Open Protocol Package'" (Ponto de interação "Pacote POI-PED--ONLY e protocolo aberto") (v4.0), ANSSI-CC-PP-2015/06;

   (b) Módulo de segurança físico:

      (1) "Cryptographic Module for CSP Signing Operations with Backup — PP CMCSOB 14167-2" (Módulo criptográfico para operações de assinatura de PSC com salvaguarda — PP CMCSOB 14167-2) (v0.35), ANSSI-CC-PP-2015/08;

      (2) "Cryptographic Module for CSP Key Generation Services — PP CMCKG 14167-3" (Módulo criptográfico para serviços de geração de chaves de PSC — PP CMCKG,14167-3) (v0.20), ANSSI-CC-PP-2015/09;

      (3) "Cryptographic Module for CSP Signing Operations without Backup — PP CMCSO 14167-4" (Módulo criptográfico para operações de assinatura de PSC sem salvaguarda — PP CMCSO, 14167-4) (v0.32), ANSSI-CC-PP-2015/10;

   (c) Tacógrafo:

      (1) "Digital Tachograph — Motion Sensor (MS PP)" [Tacógrafo digital — sensor de movimentos (MS PP)] (v1.0), BSI-CC-PP-0093-2017;

      (2) "Digital Tachograph — Vehicle Unit (VU PP)" [Tacógrafo digital — unidade-veículo (VU PP)] (v1.15), BSI--CC-PP-0094-V2-2021;

      (3) "Digital Tachograph — External GNSS Facility (EGF PP)" [Tacógrafo digital — módulo GNSS externo (EGF PP)] (v1.10), BSI-CC-PP-0092-V2-2021;

3. Outros: "Trusted Execution Environment Protection Profile — GPD_SPE_021" (Perfil de proteção para o ambiente de execução de confiança — GPD_SPE_021) (v1.3), ANSSI-CC-PP-2014/01-M02.».

ANEXO IV

O anexo IV do Regulamento de Execução (UE) 2024/482 é alterado do seguinte modo:

1) No ponto IV.2, o ponto 4 passa a ter a seguinte redação:

«4. O organismo de certificação deve rever o relatório técnico de avaliação atualizado e elaborar um relatório de reavaliação. O estado do certificado inicial é então alterado em conformidade com o artigo 13.º ou o artigo 19.º. Se o processo de reavaliação for bem sucedido, aplica-se o artigo 13.º, n.º 2, alínea a) ou alínea c), à certificação de produtos e o artigo 19.º, n.º 2, alínea a) ou alínea c), à certificação de perfis de proteção. Se o processo de reavaliação não for bem-sucedido, aplica-se o artigo 13.º, n.º 2, alínea b) ou alínea d), à certificação de produtos e o artigo 19.º, n.º 2, alínea b) ou alínea d), à certificação de perfis de proteção.».

2) O ponto IV.3 é alterado do seguinte modo:

a) O título do ponto IV.3 passa a ter a seguinte redação:

«IV.3 **Alterações de um produto de TIC certificado — Manutenção e reavaliação»;**

b) Os pontos 4 e 5 passam a ter a seguinte redação:

«4. Após o exame, o organismo de certificação determina a amplitude de uma alteração como menor ou importante de acordo com o seu impacto na garantia indicada no certificado EUCC.

5. Se o organismo de certificação confirmar as alterações como menores, não é emitido um novo certificado para o produto de TIC modificado em conformidade com o artigo 13.º, n.º 2, alínea a), ou com o artigo 19.º, n.º 2, alínea a), e é elaborado um relatório de manutenção do relatório de certificação inicial.»;

c) É inserido o seguinte ponto 5-A:

«5-A Em caso de alteração das medidas de garantia no ambiente de desenvolvimento, incluindo o aditamento de requisitos de garantia da família CC ALC_FLR (correção de falhas), o organismo de certificação pode solicitar ao ITSEF que realize a avaliação de um subconjunto de medidas de garantia afetadas. O ITSEF emite um relatório técnico de avaliação parcial, com base no qual o organismo de certificação confirma que as alterações são menores ou importantes. Se o organismo de certificação confirmar que as alterações são menores, aplica-se o disposto no ponto IV.3, ponto 5, do presente anexo. Se o organismo de certificação confirmar que as alterações são importantes, aplica-se o disposto no ponto IV.3, ponto 7, do presente anexo.».

ANEXO V

O ponto V.1 do anexo V do Regulamento de Execução (UE) 2024/482 passa a ter a seguinte redação:

«V.1 **Relatório de certificação**

1. Com base nos relatórios técnicos de avaliação fornecidos pelo ITSEF, o organismo de certificação elabora um relatório de certificação, que deve ser publicado juntamente com o certificado EUCC e a meta de segurança correspondentes.

2. O relatório de certificação é a fonte de informações pormenorizadas e práticas sobre o produto de TIC e a sua implantação segura. Deve, por conseguinte, incluir todas as informações acessíveis ao público e partilháveis que sejam pertinentes para os utilizadores e as partes interessadas. O relatório de certificação pode fazer referência a informações acessíveis ao público e partilháveis.

3. O relatório de certificação deve incluir, pelo menos, as seguintes informações:
   (a) Síntese;
   (b) Identificação do produto de TIC;
   (c) Dados de contacto relacionados com a avaliação do produto de TIC;
   (d) Políticas de segurança;
   (e) Pressupostos e clarificação do âmbito;
   (f) Informações arquitetónicas;
   (g) Informações suplementares de cibersegurança, se for caso disso;
   (h) Síntese da avaliação do produto de TIC e configuração avaliada;
   (i) Resultados da avaliação e informações relativas ao certificado;
   (j) Observações e recomendações, se for caso disso;
   (k) Anexos, se for caso disso;
   (l) Referência à meta de segurança do produto de TIC submetido a certificação;
   (m) Quando disponível, a marca ou o rótulo associado ao sistema;
   (n) Glossário, se for caso disso;
   (o) Bibliografia.

4. A síntese a que se refere o ponto 3, alínea a), é um resumo sucinto de todo o relatório de certificação. Deve fornecer uma panorâmica clara e concisa dos resultados da avaliação e incluir as seguintes informações:
   (a) Nome do produto de TIC avaliado;
   (b) Nome do ITSEF que efetuou a avaliação;
   (c) Data de conclusão da avaliação;
   (d) Data de emissão do certificado;
   (e) Se for caso disso, data de emissão do certificado inicial;
   (f) Período de validade;
   (g) Identificação única do certificado, tal como descrita no artigo 11.º;
   (h) Breve descrição dos resultados do relatório de certificação, incluindo:
      i) a versão e, se for caso disso, a publicação dos Critérios Comuns aplicados à avaliação,
      ii) o pacote de garantia dos Critérios Comuns ou a lista de componentes de garantia de segurança, o nível AVA_VAN aplicado durante a avaliação e o nível de garantia correspondente, conforme estabelecido no artigo 52.º do Regulamento (UE) 2019/881, a que o certificado EUCC se refere,
      iii) se for caso disso, o perfil ou perfis de proteção com os quais o produto de TIC se declara conforme,
      iv) a referência à política de segurança do produto de TIC avaliado,
      v) a declaração ou declarações de exoneração de responsabilidade, se for caso disso.

5. A identificação a que se refere o ponto 3, alínea b), deve identificar claramente o produto de TIC avaliado e incluir as seguintes informações:

   (a) A identificação única do produto de TIC avaliado;

   (b) Uma enumeração dos componentes do produto de TIC que fazem parte da avaliação, com o número da versão de cada componente;

   (c) A referência a outros requisitos para o ambiente operacional do produto de TIC certificado.

6. Os dados de contacto a que se refere o n.º 3, alínea c), devem incluir, pelo menos, as seguintes informações:

   (a) Nome do criador;

   (b) Nome e dados de contacto do titular do certificado EUCC;

   (c) Nome do organismo de certificação que emitiu o certificado;

   (d) Autoridade nacional responsável pela certificação da cibersegurança;

   (e) Nome do ITSEF que efetuou a avaliação e, se for caso disso, lista de subcontratantes.

7. A política de segurança a que se refere o ponto 3, alínea d), deve conter a descrição da política de segurança do produto de TIC enquanto conjunto de serviços de segurança e as políticas ou regras que o produto de TIC avaliado deve aplicar ou cumprir. Deve conter também as seguintes informações:

   (a) Uma descrição dos procedimentos de gestão das vulnerabilidades e de divulgação das vulnerabilidades do titular do certificado, a completar apenas com informações que possam ser disponibilizadas ao público;

   (b) A política de continuidade da garantia do titular do certificado, incluindo, se for caso disso, a descrição dos processos de produção ou de gestão do ciclo de vida do titular do certificado, em conformidade com o ponto IV.1 do anexo IV;

   (c) Se for caso disso, a existência de um procedimento de gestão de atualizações corretivas e o resultado da sua avaliação em conformidade com o ponto IV.4 do anexo IV.

8. Os pressupostos e a clarificação do âmbito de aplicação a que se refere o ponto 3, alínea e), devem conter informações sobre as circunstâncias e os objetivos relacionados com a utilização prevista do produto, conforme referido no artigo 7.º, n.º 1, alínea c), e incluir o seguinte:

   (a) Pressupostos sobre a utilização e implantação do produto de TIC sob a forma de requisitos mínimos, tais como o cumprimento de requisitos adequados de instalação, configuração e *hardware*;

   (b) Pressupostos sobre o ambiente para o funcionamento conforme do produto de TIC;

   (c) Descrição de quaisquer ameaças ao produto de TIC que não sejam travadas pelas funções de segurança avaliadas do produto de acordo com a utilização prevista, se tal for considerado pertinente para um potencial utilizador do produto de TIC.

   As informações a que se refere o primeiro parágrafo devem ser tão claras e compreensíveis quanto possível, a fim de permitir que os potenciais utilizadores do produto de TIC certificado tomem decisões informadas sobre os riscos associados à sua utilização.

9. As informações arquitetónicas a que se refere o ponto 3, alínea f), devem incluir uma descrição de alto nível do produto de TIC e dos seus principais componentes, com base nos resultados concretos definidos na família de garantia de Critérios Comuns: Development — TOE Design (ADV_TDS) [Desenvolvimento — Conceção do alvo de avaliação (ADV_TDS)].

10. As informações suplementares de cibersegurança a que se refere o ponto 3, alínea g), devem incluir a ligação para o sítio Web do titular do certificado EUCC a que se refere o artigo 55.º do Regulamento (UE) 2019/881.

11. A avaliação e a configuração do produto de TIC a que se refere o ponto 3, alínea h), descrevem o esforço de ensaio do criador e do avaliador, descrevendo a abordagem, a configuração e a profundidade dos ensaios. Devem incluir, no mínimo, as seguintes informações:

    (a) Uma identificação dos componentes de garantia utilizados com base nas normas referidas no artigo 3.º;

    (b) A versão dos documentos sobre o estado da arte e outros critérios de avaliação da segurança utilizados na avaliação;

    (c) As regulações e a configuração do alvo de avaliação utilizado para os ensaios e a análise da vulnerabilidade;

    (d) Qualquer perfil de proteção que tenha sido utilizado, incluindo as seguintes informações: o nome do perfil de proteção, a versão, a data e o certificado.

12. Os resultados da avaliação e as informações relativas ao certificado a que se refere o ponto 3, alínea i), devem incluir informações sobre o nível de garantia alcançado, conforme referido no artigo 4.º do presente regulamento e no artigo 52.º do Regulamento (UE) 2019/881.

13. As observações e recomendações referidas no ponto 3, alínea j), são utilizadas para transmitir informações adicionais sobre os resultados da avaliação. Essas observações e recomendações podem referir-se a deficiências do produto de TIC detetadas durante a avaliação ou a características particularmente úteis.

14. Os anexos referidos no ponto 3, alínea k), são utilizados para resumir quaisquer informações adicionais que possam ser úteis para os destinatários do relatório, mas que não se enquadrem logicamente nas secções previstas do relatório, incluindo nos casos em que é apresentada uma descrição completa da política de segurança.

15. A meta de segurança a que se refere o ponto 3, alínea l), deve remeter para a meta de segurança avaliada. A meta de segurança avaliada deve ser fornecida juntamente com o relatório de certificação para efeitos de publicação no sítio Web referido no artigo 50.º, n.º 1, do Regulamento (UE) 2019/881. Se for necessária uma sanitização da meta de segurança avaliada antes da publicação, esta deve ser efetuada em conformidade com o ponto V.2 do anexo V do presente regulamento.

16. As marcas ou os rótulos associados ao sistema EUCC a que se refere o ponto 3, alínea m), devem ser inseridos no relatório de certificação em conformidade com as regras e os procedimentos estabelecidos no artigo 11.º.

17. O glossário referido no ponto 3, alínea n), é utilizado para aumentar a legibilidade do relatório, fornecendo definições de acrónimos ou termos cujos significados possam não ser evidentes.

18. A bibliografia a que se refere o ponto 3, alínea o), deve incluir referências a todos os documentos utilizados na elaboração do relatório de certificação. Essas informações devem incluir, no mínimo, os seguintes elementos:

    (a) Os critérios de avaliação da segurança, os documentos sobre o estado da arte e outras especificações pertinentes utilizadas;

    (b) O relatório técnico de avaliação;

    (c) O relatório técnico de avaliação para a avaliação de produtos compostos, se for caso disso;

    (d) A documentação técnica de referência;

    (e) Orientações em matéria de segurança dos criadores;

    (f) Lista de configuração do criador.

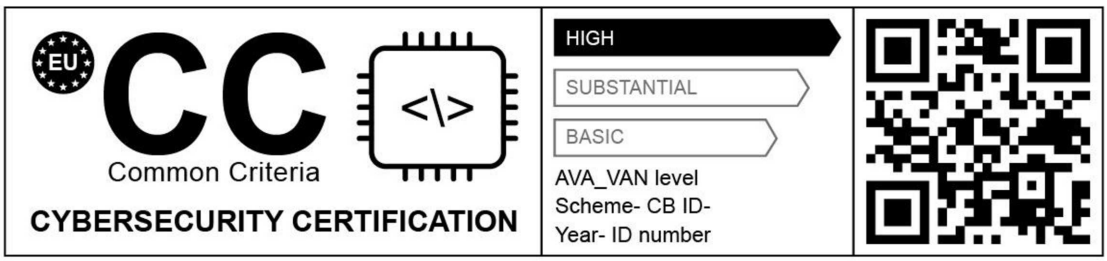
    A fim de garantir a reprodutibilidade da avaliação, toda a documentação referida tem de ser identificada de forma inequívoca com a respetiva data de publicação e o respetivo número de versão.».

ANEXO VI

«ANEXO IX

Marca e rótulo

1. Formato da marca e do rótulo:



2. Se a marca e o rótulo forem reduzidos ou ampliados, devem ser respeitadas as proporções indicadas no ponto 1.

3. Quando fisicamente presentes, a marca e o rótulo devem ter, pelo menos, 5 mm de altura.».