2024/2981

4.12.2024

REGULAMENTO DE EXECUÇÃO (UE) 2024/2981 DA COMISSÃO

de 28 de novembro de 2024

que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante à certificação das carteiras europeias de identidade digital

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 5.º-C, n.º 6,

Considerando o seguinte:

(1) Nos termos do artigo 5.º-C do Regulamento (UE) n.º 910/2014, a certificação das carteiras europeias de identidade digital («carteiras») deve ser efetuada em conformidade com os requisitos funcionais, de cibersegurança e de proteção de dados, a fim de assegurar um elevado nível de segurança e confiança nas carteiras. Esses requisitos de certificação devem ser harmonizados em todos os Estados-Membros, de modo a evitar a fragmentação do mercado e criar um quadro sólido.

(2) O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([2]) e, se for caso disso, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([3]) aplicam-se às atividades de tratamento de dados pessoais ao abrigo do presente regulamento.

(3) A Comissão avalia periodicamente as novas tecnologias, práticas, normas ou especificações técnicas. A fim de assegurar o mais elevado nível de harmonização entre os Estados-Membros para o desenvolvimento e a certificação das carteiras, as especificações técnicas estabelecidas no presente regulamento baseiam-se nos trabalhos realizados com base na Recomendação (UE) 2021/946 da Comissão, de 3 de junho de 2021, relativa a um conjunto de instrumentos comuns a nível da União para uma abordagem coordenada do quadro europeu para a identidade digital ([4]) e, em especial, na arquitetura e no quadro de referência que dela fazem parte. Em conformidade com o considerando 75 do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho ([5]), a Comissão deve rever e atualizar o presente regulamento de execução, se necessário, a fim de assegurar que o mesmo acompanha a evolução mundial, a arquitetura e o regime de referência e de seguir as boas práticas no mercado interno.

(4) A fim de certificar a conformidade com os requisitos de cibersegurança incluídos no quadro de certificação, a certificação das soluções de carteiras deve referir-se, quando disponíveis e pertinentes, aos sistemas europeus de certificação da cibersegurança criados nos termos do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho ([6]). Na ausência desses sistemas, ou caso abranjam parcialmente os requisitos de cibersegurança, o presente regulamento estabelece os requisitos gerais aplicáveis aos sistemas nacionais de certificação, abrangendo os requisitos funcionais, de cibersegurança e de proteção de dados.

([1]) JO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) 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).
([3]) 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).
([4]) JO L 210 de 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) 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).
([6]) 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) (JO L 151 de 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Nos termos do artigo 5.º-A, n.º 11, do Regulamento (UE) n.º 910/2014, as carteiras devem ser certificadas tendo em conta um nível de garantia elevado, conforme estabelecido no Regulamento (UE) n.º 910/2014, bem como no Regulamento de Execução (UE) 2015/1502 da Comissão ([7]). A solução global de carteira tem de alcançar esse nível de garantia. Nos termos do presente regulamento, alguns componentes da solução de carteira podem ser certificados a um nível de garantia inferior, desde que tal seja devidamente justificado e não prejudique o nível de garantia elevado alcançado pela solução global.

(6) Todos os sistemas nacionais de certificação devem designar um proprietário do sistema que será responsável pelo desenvolvimento e manutenção do sistema de certificação. O proprietário do sistema pode ser um organismo de avaliação da conformidade, um organismo ou autoridade governamental, uma associação profissional, um grupo de organismos de avaliação da conformidade ou qualquer organismo adequado, podendo ser diferente do organismo que explora o sistema nacional de certificação.

(7) O objeto da certificação deve incluir os componentes de *software* da solução de carteira, como a instância de carteira. A aplicação criptográfica segura de carteiras («WSCA»), o dispositivo criptográfico seguro de carteiras («WSCD») e as plataformas em que estes componentes de *software* são executados, embora façam parte do ambiente operacional, só devem ser incluídos no objeto da certificação se forem disponibilizados pela solução de carteira. Noutros casos, e em especial quando estes dispositivos e plataformas forem disponibilizados por utilizadores finais, os fornecedores devem estabelecer pressupostos sobre o ambiente operacional da solução de carteira, incluindo sobre esses dispositivos e plataformas, e aplicar medidas para confirmar que esses pressupostos sejam verificados na prática. A fim de assegurar a proteção dos ativos críticos através de *hardware* e *software* de sistemas utilizados para gerir e proteger chaves criptográficas criadas, armazenadas ou processadas pelo WSCD, o WSCD tem de satisfazer normas elevadas de certificação, conforme refletido em normas internacionais como os Critérios Comuns («EUCC»), estabelecido no Regulamento de Execução (UE) 2024/482 da Comissão ([8]), pela avaliação EAL4 dos Critérios Comuns e pela análise avançada da vulnerabilidade metodológica, nomeadamente comparável ao nível AVA_VAN.5. Estas normas de certificação devem ser utilizadas, o mais tardar, quando a certificação da conformidade das carteiras for efetuada na sequência de um sistema europeu de certificação da cibersegurança adotado nos termos do Regulamento (UE) 2019/881.

(8) Para dispor de carteiras totalmente móveis, seguras e de fácil utilização, é necessário disponibilizar soluções invioláveis normalizadas e certificadas que as apoiem, como elementos seguros incorporados, dispositivos externos como cartões inteligentes, ou plataformas SIM incorporadas em dispositivos móveis. É importante assegurar o acesso atempado a elementos seguros incorporados para as carteiras e os meios de identificação eletrónica nacionais, bem como coordenar os esforços dos Estados-Membros neste domínio. O Grupo de Cooperação Europeia para a Identidade Digital instituído nos termos do artigo 46.º-E, n.º 1, do Regulamento (UE) n.º 910/2014 («grupo de cooperação») deve, por conseguinte, criar um subgrupo específico para este efeito. Em consulta com as partes interessadas pertinentes, este subgrupo deve chegar a acordo sobre um roteiro conjunto para o acesso a elementos seguros incorporados, que a Comissão terá em conta no relatório de revisão sobre o Regulamento (UE) n.º 910/2014. Além disso, a fim de facilitar a adoção da carteira a nível nacional, a Comissão deve, em cooperação com os Estados-Membros, elaborar e atualizar continuamente um manual para os casos de utilização no âmbito da arquitetura e do regime de referência.

(9) O objeto da certificação dos sistemas nacionais de certificação deve incluir igualmente os processos utilizados para disponibilizar e explorar a solução de carteira, mesmo que a definição ou execução desses processos seja subcontratada a terceiros. A fim de demonstrar que os processos satisfazem os requisitos dos sistemas, é possível utilizar as informações sobre a garantia como elementos de prova, desde que seja utilizada uma análise da dependência para determinar se as informações sobre a garantia são suficientes. As informações sobre a garantia são apresentadas sob muitas formas diferentes, incluindo relatórios e certificados de conformidade, que podem ser privados, nacionais, europeus ou internacionais, com base em normas ou especificações técnicas. O objetivo da análise da dependência consiste em avaliar a qualidade das informações disponíveis sobre a garantia em relação aos componentes de uma carteira.

([7]) Regulamento de Execução (UE) 2015/1502 da Comissão, de 8 de setembro de 2015, que estabelece as especificações técnicas mínimas e os procedimentos para a atribuição dos níveis de garantia dos meios de identificação eletrónica, nos termos do artigo 8.º, n.º 3, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno (JO L 235 de 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) 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/2024/482/oj).

(10) De acordo com os procedimentos estabelecidos para o efeito, o grupo de cooperação deve poder emitir pareceres e recomendações sobre os projetos de sistemas nacionais de certificação que lhe são apresentados. Estes sistemas nacionais de certificação devem ser específicos da arquitetura da carteira e devem existir perfis específicos para cada arquitetura específica suportada.

(11) A fim de assegurar um entendimento comum e uma abordagem harmonizada da avaliação dos riscos mais críticos que possam afetar a disponibilização e o funcionamento das carteiras, deve ser elaborado um registo dos riscos e ameaças a ter em consideração aquando da conceção de soluções de carteiras, independentemente da sua arquitetura específica. Na identificação dos riscos a incluir no registo, devem ser tidos em conta os objetivos de cibersegurança descritos no Regulamento (UE) n.º 910/2014, como a confidencialidade, a integridade e a disponibilidade da solução de carteira, bem como a privacidade dos utentes e dos dados. A devida consideração dos riscos e ameaças incluídos neste registo de riscos deve fazer parte dos requisitos dos sistemas nacionais de certificação. Para acompanhar o panorama das ameaças em constante evolução, importa manter e atualizar regularmente o registo de riscos, em colaboração com o grupo de cooperação.

(12) Ao estabelecerem os seus sistemas de certificação, os proprietários dos sistemas devem realizar uma avaliação dos riscos para aperfeiçoar e completar os riscos e ameaças constantes do registo com riscos e ameaças específicos à arquitetura ou à implementação da solução de carteira. A avaliação dos riscos deve ter em conta a forma como os riscos e ameaças aplicáveis podem ser adequadamente tratados. Os fornecedores de carteiras devem completar a avaliação dos riscos do sistema para identificar quaisquer riscos e ameaças específicos à sua implementação e propor medidas de tratamento adequadas para a avaliação pelo organismo de certificação.

(13) A fim de demonstrar que a arquitetura de uma solução de carteira cumpre os requisitos de segurança aplicáveis, cada sistema ou perfil específico da arquitetura deve conter, pelo menos, uma descrição da arquitetura da solução de carteira, uma lista de requisitos de segurança aplicáveis à arquitetura da solução de carteira, um plano de avaliação para confirmar que uma solução de carteira baseada nesta arquitetura cumpre esses requisitos e uma avaliação dos riscos. Os sistemas nacionais de certificação devem exigir que os fornecedores de carteiras demonstrem de que forma a conceção da solução de carteira que disponibilizam corresponde à arquitetura de referência e especifica os controlos de segurança e os planos de validação da solução de carteira específica. Os sistemas nacionais de certificação devem também definir uma atividade de avaliação da conformidade, a fim de verificar se a conceção da carteira reflete adequadamente a arquitetura de referência do perfil selecionado. Os sistemas nacionais de certificação devem cumprir os requisitos estabelecidos no artigo 51.º do Regulamento (UE) 2019/881, com exceção das alíneas e) e f) relativas aos registos.

(14) No que diz respeito à certificação de produtos, deve ser autorizada a utilização de certificados de conformidade emitidos no âmbito do sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns («EUCC»), e de certificados de conformidade emitidos ao abrigo de sistemas nacionais de certificação no contexto do acordo de reconhecimento mútuo SOG-IS. Além disso, deve ser autorizada a utilização de outros sistemas nacionais de certificação para componentes de produtos menos sensíveis, como os estabelecidos de acordo com a norma CEN EN 17640 para a metodologia de avaliação da cibersegurança a tempo fixo.

(15) A marca de confiança da UE para carteiras de identidade digital («marca de confiança») deve ser utilizada para indicar, de forma clara, simples e reconhecível, que uma carteira foi disponibilizada em conformidade com o Regulamento (UE) n.º 910/2014. Por conseguinte, deve ser considerada uma marca de conformidade para uma solução de carteira certificada ao abrigo de sistemas nacionais de certificação. Os sistemas nacionais de certificação não devem definir quaisquer outras marcas de conformidade.

(16) A fim de dissuadir as fraudes, os sistemas nacionais de certificação devem definir as medidas a tomar caso a certificação ao abrigo do sistema seja invocada de forma fraudulenta.

(17) A fim de assegurar uma gestão eficiente das notificações de vulnerabilidade, os fornecedores de soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas devem definir e aplicar processos para avaliar a gravidade e o potencial impacto das vulnerabilidades. Os sistemas nacionais de certificação devem estabelecer um limiar acima do qual o organismo de certificação deve ser notificado. Essa obrigação de notificação não deve afetar os critérios estabelecidos pela legislação em matéria de proteção de dados e pelas autoridades de proteção de dados dos Estados-Membros para a notificação de violações de dados pessoais. Podem ser estabelecidas eventuais sinergias entre a notificação obrigatória da violação ou do comprometimento das soluções de carteiras e a notificação de violações de dados pessoais nos termos do Regulamento (UE) 2016/679. A avaliação realizada pelo organismo de certificação a um relatório de análise de impacto da vulnerabilidade não deve prejudicar a avaliação realizada por uma autoridade de proteção de dados a uma avaliação de impacto sobre a proteção de dados nos termos dos artigos 35.º e 36.° do Regulamento (UE) 2016/679.

(18) Os fornecedores de soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas devem notificar o proprietário do sistema de quaisquer justificações para exceções à avaliação da vulnerabilidade exigida para a avaliação do WSCD e da WSCA nos termos do anexo IV.

(19) O cancelamento de um certificado de conformidade pode ter consequências graves, como a revogação de todas as unidades de carteira implantadas. Por conseguinte, os organismos de certificação só devem ponderar o cancelamento se uma vulnerabilidade não corrigida for suscetível de afetar significativamente a fiabilidade da solução de carteira ou a fiabilidade de outra solução de carteira.

(20) Deve ser criado um processo específico de atualização dos sistemas nacionais de certificação para gerir a transição entre versões sucessivas dos sistemas, em especial no que diz respeito às ações a tomar pelo titular do certificado no que diz respeito a futuras avaliações, manutenção, recertificação e avaliações especiais.

(21) A fim de facilitar a transparência, os fornecedores de carteiras devem partilhar publicamente informações de segurança sobre a sua solução de carteira.

(22) Caso os sistemas nacionais de certificação recorram a informações sobre a garantia provenientes de outros sistemas ou fontes de certificação, deve ser efetuada uma análise da dependência para verificar se a documentação de garantia, por exemplo, os relatórios de garantia e os certificados de conformidade, está disponível e é adequada para as soluções de carteiras e para o sistema de identificação eletrónica ao abrigo do qual são disponibilizadas. A base para esta análise da dependência deve ser a avaliação dos riscos das soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas. A avaliação deve determinar se a documentação de garantia disponível para uma determinada solução de carteira e para o sistema de identificação eletrónica ao abrigo do qual é disponibilizada é adequada para proporcionar uma garantia correspondente ao nível de avaliação visado. A avaliação deve também atualizar a análise da dependência ou reavaliá-la totalmente, se necessário.

(23) Os organismos de certificação devem emitir certificados de conformidade nos sistemas nacionais de certificação, juntamente com um relatório de certificação acessível ao público, conforme referido no artigo 5.º-D, n.º 2, alínea a), do Regulamento (UE) n.º 910/2014. O correspondente relatório de avaliação da certificação deve ser disponibilizado ao grupo de cooperação.

(24) Os sistemas nacionais de certificação devem estabelecer uma avaliação anual de fiscalização, a fim de assegurar que os processos em torno da gestão e manutenção das carteiras funcionam de forma eficaz, o que significa que funcionam conforme definido nas políticas que determinam os processos. A avaliação bienal da vulnerabilidade é um requisito decorrente do Regulamento (UE) n.º 910/2014, a fim de assegurar que a solução de carteira continua a abranger adequadamente os riscos e ameaças de cibersegurança identificados no registo de riscos, incluindo qualquer evolução do cenário de ameaças. As noções de avaliações de fiscalização, avaliações de recertificação e avaliações especiais devem estar em conformidade com a norma EN ISO/IEC 17021-1:2015.

(25) Um ciclo de certificação termina com a expiração do certificado de conformidade ou com a emissão de um novo certificado de conformidade na sequência de uma avaliação de recertificação bem-sucedida. A avaliação da recertificação deve incluir uma avaliação de todos os componentes do objeto da certificação, incluindo uma avaliação da eficácia e, se for caso disso, uma avaliação da vulnerabilidade. Durante a recertificação, deve ser possível reutilizar os resultados de avaliações anteriores de componentes que não tenham sido alterados.

(26) Quando for adotado um sistema europeu de certificação da cibersegurança, os sistemas nacionais de certificação com o mesmo âmbito devem deixar de emitir certificações após um período de transição definido, conforme referido no artigo 57.º, n.º 1, do Regulamento (UE) 2019/881.

(27) Os sistemas nacionais de certificação devem basear-se nos quadros existentes e reutilizar elementos de prova, conforme adequado, a fim de assegurar a harmonização e a interoperabilidade. Os Estados-Membros podem celebrar acordos para a reutilização transfronteiriça de sistemas de certificação ou de partes dos mesmos. A Comissão Europeia e a ENISA devem, em colaboração com o grupo de cooperação, apoiar os Estados-Membros no desenvolvimento e manutenção dos seus sistemas nacionais de certificação que assegurem a partilha de conhecimentos e as boas práticas.

(28) 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 ([9]) e emitiu o seu parecer em 30 de setembro de 2024.

(29) As medidas previstas no presente regulamento estão em conformidade com o parecer do Comité referido no artigo 48.º, n.º 1, do Regulamento (UE) n.º 910/2014,

ADOTOU O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e âmbito de aplicação

O presente regulamento estabelece normas de referência, assim como especificações e procedimentos para criar um quadro sólido para a certificação de carteiras, a atualizar periodicamente, a fim de acompanhar a evolução da tecnologia e das normas, bem como os trabalhos realizados com base na Recomendação (UE) 2021/946, relativa a um conjunto de instrumentos comuns a nível da União para uma abordagem coordenada do quadro europeu para a identidade digital, em especial a arquitetura e o quadro de referência.

Artigo 2.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Solução de carteira», uma combinação de *software*, *hardware*, serviços, definições e configurações, incluindo instâncias de carteiras, uma ou várias aplicações criptográficas seguras de carteiras e um ou vários dispositivos criptográficos seguros de carteiras;

2) «Proprietário do sistema», uma organização responsável pelo desenvolvimento e manutenção de um sistema de certificação;

3) «Objeto da certificação», produtos, processos e serviços, ou uma combinação dos mesmos, aos quais se aplicam os requisitos especificados;

4) «Aplicação criptográfica segura de carteiras», uma aplicação que gere ativos críticos através da ligação e da utilização das funções criptográficas e não criptográficas disponibilizadas pelo dispositivo criptográfico seguro de carteiras;

5) «Instância de carteira», a aplicação instalada e configurada no dispositivo ou ambiente do utente de uma carteira, que faz parte de uma unidade de carteira e que o utente da carteira utiliza para interagir com a unidade de carteira;

([9]) 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).

6) «Dispositivo criptográfico seguro de carteiras», um dispositivo inviolável que disponibiliza um ambiente ligado à aplicação criptográfica segura de carteiras e que esta utiliza para proteger ativos críticos e assegurar funções criptográficas para a execução segura de operações críticas;

7) «Registo de riscos», um registo de informações pertinentes para o processo de certificação sobre os riscos identificados;

8) «Fornecedor de carteiras», uma pessoa singular ou coletiva que disponibiliza soluções de carteiras;

9) «Organismo de certificação», um organismo terceiro de avaliação da conformidade que explora sistemas de certificação;

10) «Unidade de carteira», uma configuração única de uma solução de carteira que inclui instâncias de carteiras, aplicações criptográficas seguras de carteiras e dispositivos criptográficos seguros de carteiras disponibilizada pelo fornecedor de uma carteira a um utente individual da carteira;

11) «Ativos críticos», ativos dentro de uma unidade de carteira ou relacionados com a mesma, que se revestem de uma importância de tal forma extraordinária que o comprometimento da sua disponibilidade, confidencialidade ou integridade teria um efeito debilitante muito grave na capacidade de recorrer à unidade de carteira;

12) «Utente da carteira», um utente que controla a unidade de carteira;

13) «Incidente», um incidente na aceção do artigo 6.º, ponto 6, da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho ([10]);

14) «Política de divulgação incorporada», um conjunto de regras, incorporadas num certificado eletrónico de atributos pelo seu fornecedor, que indicam as condições que um utilizador de carteira tem de cumprir para aceder ao certificado eletrónico de atributos.

CAPÍTULO II

SISTEMAS NACIONAIS DE CERTIFICAÇÃO

Artigo 3.º

Criação de sistemas nacionais de certificação

1. Os Estados-Membros devem designar um proprietário do sistema para cada sistema nacional de certificação.

2. O objeto da certificação definido nos sistemas nacionais de certificação é a disponibilização e o funcionamento de soluções de carteiras e dos sistemas de identificação eletrónica ao abrigo dos quais são disponibilizadas.

3. Em conformidade com o Regulamento de Execução (UE) 2015/1502, o objeto da certificação nos sistemas nacionais de certificação deve incluir os seguintes elementos:

a) Os componentes de *software*, incluindo as definições e configurações de uma solução de carteira e do sistema de identificação eletrónica ao abrigo do qual as soluções de carteiras são disponibilizadas;

b) Os componentes e plataformas de *hardware* em que os componentes de *software* a que se refere o ponto b) são executados ou dos quais dependem para operações críticas, caso sejam disponibilizados direta ou indiretamente pela solução de carteira e pelo sistema de identificação eletrónica ao abrigo do qual é disponibilizada e caso tenham de cumprir o nível de garantia pretendido para esses componentes de *software*. Caso os componentes e plataformas de *hardware* não sejam disponibilizados pelo fornecedor de carteiras, os sistemas nacionais de certificação devem formular pressupostos para a avaliação dos componentes e plataformas de *hardware*, ao abrigo dos quais seja possível resistir a ataques de elevado potencial, em conformidade com o Regulamento de Execução (UE) 2015/1502, e especificar as atividades de avaliação para confirmar esses pressupostos, conforme referido no anexo IV;

([10]) Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) Os processos que apoiam a disponibilização e o funcionamento de uma solução de carteira, incluindo o processo de integração dos utentes a que se refere o artigo 5.º-A do Regulamento (UE) n.º 910/2014, abrangendo, pelo menos, a inscrição, bem como a gestão e organização dos meios eletrónicos nos termos das secções 2.1, 2.2 e 2.4 do anexo I do Regulamento de Execução (UE) 2015/1502.

4. Os sistemas nacionais de certificação devem incluir uma descrição da arquitetura específica das soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas. Caso os sistemas nacionais de certificação abranjam mais do que uma arquitetura específica, devem incluir um perfil para cada arquitetura específica.

5. Para cada perfil, os sistemas nacionais de certificação devem estabelecer, pelo menos, o seguinte:

a) A arquitetura específica de uma solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada;

b) Os controlos de segurança associados aos níveis de garantia estabelecidos no artigo 8.º do Regulamento (UE) n.º 910/2014;

c) Um plano de avaliação elaborado em conformidade com a secção 7.4.1 da norma EN ISO/IEC 17065:2012;

d) Os requisitos de segurança necessários para fazer face aos riscos e ameaças de cibersegurança enumerados no registo de riscos constante do anexo I do presente regulamento, até ao nível de garantia exigido, bem como para cumprir, se for caso disso, os objetivos definidos no artigo 51.º do Regulamento (UE) 2019/881;

e) Um levantamento dos controlos a que se refere a alínea b) do presente número aos componentes da arquitetura;

f) Uma descrição da forma como os controlos de segurança, o levantamento, os requisitos de segurança e o plano de avaliação a que se referem as alíneas b) a c) permitem aos fornecedores de soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas responder adequadamente aos riscos e ameaças de cibersegurança identificados no registo de riscos a que se refere a alínea d), até ao nível de garantia exigido com base na avaliação dos riscos para aperfeiçoar e completar os riscos e ameaças enumerados no registo de riscos com riscos e ameaças específicos à arquitetura.

6. O plano de avaliação a que se refere o n.º 5, alínea c), deve enumerar as atividades de avaliação a incluir na avaliação das soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas.

7. A atividade de avaliação a que se refere o n.º 6 deve exigir que os fornecedores de soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas facultem informações que cumpram os requisitos enumerados no anexo II.

Artigo 4.º

Requisitos gerais

1. Os sistemas nacionais de certificação devem abranger os requisitos funcionais, de cibersegurança e de proteção de dados ao utilizar, quando disponíveis e aplicáveis, os seguintes sistemas de certificação:

a) Sistemas europeus de certificação da cibersegurança criados nos termos do Regulamento (UE) 2019/881, incluindo o EUCC;

b) Sistemas nacionais de certificação da cibersegurança abrangidos pelo EUCC, em conformidade com o artigo 49.º do Regulamento de Execução (UE) 2024/482.

2. Além disso, os sistemas nacionais de certificação podem referir-se aos seguintes elementos, quando disponíveis e aplicáveis:

a) Outros sistemas nacionais de certificação pertinentes;

b) Normas internacionais, europeias e nacionais;

c) Especificações técnicas que cumpram os requisitos estabelecidos no anexo II do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho ([11]).

3. Os sistemas nacionais de certificação devem:

a) Especificar os elementos enumerados na secção 6.5 da norma EN ISO/IEC 17067:2013;

b) Ser implementados como um sistema do tipo 6, em conformidade com a secção 5.3.8 da norma EN ISO/IEC 17067:2013.

4. Os sistemas nacionais de certificação devem cumprir os seguintes requisitos:

a) Apenas os fornecedores a que se refere o artigo 5.º-A, n.º 2, do Regulamento (UE) n.º 910/2014 são elegíveis para a emissão de certificados ao abrigo dos sistemas nacionais de certificação;

b) Apenas a marca de confiança é utilizada como marca de conformidade;

c) Ao referirem-se ao sistema, os fornecedores de soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas incluem referências ao Regulamento (UE) n.º 910/2014 e ao presente regulamento;

d) Os fornecedores de soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas completam a avaliação dos riscos do sistema a que se refere o artigo 3.º, n.º 5, alínea f), para identificar riscos e ameaças específicos à sua implementação e propor medidas de tratamento adequadas para todos os riscos e ameaças relevantes;

e) As responsabilidades e a ação judicial são estabelecidas e incluem referências à legislação nacional aplicável, que define as responsabilidades e eventuais ações judiciais, caso a certificação ao abrigo do sistema seja utilizada de forma fraudulenta.

5. A avaliação a que se refere o n.º 4, alínea d), é partilhada com o organismo de certificação para avaliação.

Artigo 5.º

Gestão de incidentes e vulnerabilidades

1. Os sistemas nacionais de certificação devem conter requisitos de gestão de incidentes e vulnerabilidades em conformidade com os n.ºs 2 a 9.

2. O titular de um certificado de conformidade de uma solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada deve notificar o respetivo organismo de certificação, sem demora injustificada, de qualquer violação ou comprometimento da solução de carteira, ou do sistema de identificação eletrónica ao abrigo do qual é disponibilizada, suscetível de afetar a sua conformidade com os requisitos dos sistemas nacionais de certificação.

3. O titular de um certificado de conformidade deve estabelecer, manter e aplicar procedimentos e uma política de gestão de vulnerabilidades, tendo em conta os procedimentos estabelecidos nas normas europeias e internacionais existentes, incluindo a norma EN ISO/IEC 30111:2019.

4. O titular do certificado de conformidade deve notificar o organismo de certificação emissor das vulnerabilidades e alterações que afetam a solução de carteira, com base em critérios definidos sobre o impacto dessas vulnerabilidades e alterações.

5. O titular do certificado de conformidade deve elaborar um relatório de análise de impacto da vulnerabilidade para qualquer vulnerabilidade que afete os componentes de *software* da solução de carteira. O relatório deve incluir os seguintes elementos:

a) O impacto da vulnerabilidade na solução de carteira certificada;

b) Os possíveis riscos associados à proximidade ou probabilidade de um ataque;

([11]) Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12). http://data.europa.eu/eli/reg/2012/1025/oj).

c) Se é possível corrigir a vulnerabilidade com recurso aos meios disponíveis;

d) Caso seja possível corrigir a vulnerabilidade com recurso aos meios disponíveis, possíveis formas de a corrigir.

6. Caso seja exigida a notificação a que se refere o n.º 4, o titular do certificado de conformidade deve transmitir ao organismo de certificação, sem demora injustificada, o relatório de análise de impacto da vulnerabilidade a que se refere o n.º 5.

7. O titular de um certificado de conformidade deve estabelecer, manter e aplicar uma política de gestão de vulnerabilidades que cumpra os requisitos estabelecidos no anexo I do Regulamento de Ciber-Resiliência ([12]).

8. Os sistemas nacionais de certificação devem estabelecer requisitos de divulgação de vulnerabilidades aplicáveis aos organismos de certificação.

9. O titular de um certificado de conformidade deve divulgar e registar qualquer vulnerabilidade publicamente conhecida e corrigida na solução de carteira ou num dos repositórios em linha a que se refere o anexo V.

Artigo 6.º

Manutenção dos sistemas nacionais de certificação

1. Os sistemas nacionais de certificação devem incluir um processo de revisão periódica do seu funcionamento. Esse processo deve ter por objetivo confirmar a sua adequação e identificar os aspetos que carecem de melhorias, tendo em conta as reações das partes interessadas.

2. Os sistemas nacionais de certificação devem incluir disposições relativas à sua manutenção. Este processo deve incluir, pelo menos, os seguintes requisitos:

a) Regras para a governação da definição e dos requisitos dos sistemas nacionais de certificação;

b) O estabelecimento de prazos para a emissão de certificados na sequência da adoção de versões atualizadas dos sistemas nacionais de certificação, tanto para certificados de conformidade novos como para os emitidos anteriormente;

c) Uma revisão periódica dos sistemas nacionais de certificação, a fim de assegurar que os requisitos dos sistemas nacionais de certificação são aplicados de forma coerente, tendo em conta, pelo menos, os seguintes aspetos:

— pedidos de esclarecimento dirigidos ao proprietário do sistema relacionados com os requisitos do sistema nacional de certificação,

— reações das partes interessadas e de outras partes,

— responsividade do proprietário do sistema nacional de certificação aos pedidos de informação;

d) Regras para o acompanhamento dos procedimentos e documentos de referência para a evolução das versões de referência dos sistemas nacionais de certificação, incluindo, pelo menos, períodos de transição;

e) Um processo para assegurar a cobertura dos riscos e ameaças de cibersegurança mais recentes enumerados no registo de riscos estabelecido no anexo I do presente regulamento;

f) Um processo de gestão de outras alterações dos sistemas nacionais de certificação.

([12]) Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Os sistemas nacionais de certificação devem conter requisitos para a realização de avaliações de produtos atualmente certificados num determinado período após a revisão do sistema, ou após a publicação de novas especificações ou normas, ou de novas versões das mesmas, que as soluções de carteiras e o sistema de identificação eletrónica ao abrigo do qual são disponibilizadas devem cumprir.

CAPÍTULO III

REQUISITOS RELATIVOS AOS PROPRIETÁRIOS DOS SISTEMAS

Artigo 7.º

Requisitos gerais

1. Os proprietários dos sistemas devem desenvolver e manter sistemas nacionais de certificação, bem como gerir as suas operações.

2. Os proprietários dos sistemas podem subcontratar a terceiros a totalidade ou parte das suas atribuições. Em caso de subcontratação a uma entidade privada, os proprietários dos sistemas devem definir, por meio de um contrato, os deveres e responsabilidades de todas as partes. Os proprietários dos sistemas continuam a ser responsáveis por todas as atividades subcontratadas realizadas pelos seus subcontratantes.

3. Os proprietários dos sistemas devem realizar as suas atividades de acompanhamento, se aplicável, pelo menos com base nas seguintes informações:

a) Informações provenientes dos organismos de certificação, dos organismos nacionais de acreditação e das autoridades de fiscalização do mercado competentes;

b) Informações resultantes de auditorias e de investigações efetuadas pela própria autoridade ou por outra autoridade;

c) Reclamações e recursos recebidos nos termos do artigo 15.º.

4. Os proprietários dos sistemas devem informar o grupo de cooperação das revisões dos sistemas nacionais de certificação. Essa notificação deve facultar informações adequadas para que o grupo de cooperação emita recomendações aos proprietários dos sistemas e pareceres sobre os sistemas nacionais de certificação atualizados.

CAPÍTULO IV

REQUISITOS RELATIVOS AOS FORNECEDORES DE SOLUÇÕES DE CARTEIRAS E AO SISTEMA DE IDENTIFICAÇÃO ELETRÓNICA AO ABRIGO DO QUAL SÃO DISPONIBILIZADAS

Artigo 8.º

Requisitos gerais

1. Os sistemas nacionais de certificação devem conter requisitos de cibersegurança baseados numa avaliação dos riscos de cada arquitetura específica suportada. Esses requisitos de cibersegurança visam tratar os riscos e ameaças de cibersegurança identificados, conforme estabelecido no registo de riscos previsto no anexo I.

2. Em consonância com o artigo 5.º-A, n.º 23, do Regulamento (UE) n.º 910/2014, os sistemas nacionais de certificação devem exigir que as soluções de carteiras e os sistemas de identificação eletrónica ao abrigo dos quais são disponibilizadas sejam resistentes a ataques de elevado potencial para a atribuição do nível de garantia elevado, conforme referido no Regulamento de Execução (UE) 2015/1502.

3. Os sistemas nacionais de certificação devem estabelecer critérios de segurança, que devem incluir os seguintes requisitos:

a) O Regulamento de Ciber-Resiliência, se for caso disso, ou requisitos que cumpram os objetivos de segurança estabelecidos no artigo 51.º do Regulamento (UE) 2019/881;

b) O estabelecimento e a aplicação de políticas e procedimentos relativos à gestão dos riscos associados ao funcionamento de uma solução de carteira, incluindo a identificação e avaliação dos riscos e a atenuação dos riscos identificados;

c) O estabelecimento e a aplicação de políticas e procedimentos relacionados com a gestão das alterações e a gestão das vulnerabilidades, em conformidade com o artigo 5.º do presente regulamento;

d) O estabelecimento e a aplicação de políticas e procedimentos de gestão dos recursos humanos, incluindo requisitos em matéria de conhecimentos especializados, fiabilidade, experiência, formação em matéria de segurança e qualificações do pessoal envolvido no desenvolvimento ou no funcionamento da solução de carteira;

e) Requisitos relativos ao ambiente operacional da solução de carteira, nomeadamente sob a forma de pressupostos sobre a segurança dos dispositivos e plataformas em que funcionam os componentes de *software* da solução de carteira, incluindo WSCD e, se aplicável e pertinente, requisitos de avaliação da conformidade para confirmar que esses pressupostos são verificados nos dispositivos e plataformas pertinentes;

f) Para cada pressuposto não apoiado por um certificado de conformidade ou outra informação de garantia aceitável, uma descrição do mecanismo que o fornecedor de carteiras utiliza para fazer cumprir o pressuposto, bem como uma justificação de que o mecanismo é suficiente para assegurar que o pressuposto é verificado;

g) O estabelecimento e a aplicação de medidas para assegurar a utilização de uma versão atualmente certificada da solução de carteira.

4. Os sistemas nacionais de certificação devem conter requisitos funcionais relativos aos mecanismos de atualização de cada componente de *software* das soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas para as operações enumeradas no anexo III.

5. Os sistemas nacionais de certificação devem exigir que o requerente da certificação faculte ou de qualquer modo disponibilize ao organismo de certificação as seguintes informações e documentação:

a) Elementos de prova relacionados com as informações a que se refere o anexo IV, ponto 1, nomeadamente, se necessário, pormenores sobre a solução de carteira e o respetivo código-fonte, incluindo:

— *informações sobre a arquitetura:* para cada componente da solução de carteira (incluindo componentes de produtos, processos e serviços), uma descrição das suas propriedades essenciais de segurança, incluindo as suas dependências externas,

— *controlos e níveis de garantia:* para cada controlo de segurança da solução de carteira, uma descrição do controlo e do nível de garantia exigido, com base no anexo do Regulamento de Execução (UE) 2015/1502, que estabelece uma série de especificações técnicas e procedimentos aplicáveis aos vários controlos aplicados pelos meios de identificação eletrónica,

— *levantamento dos controlos aos componentes da arquitetura:* uma descrição da forma como os controlos da carteira são aplicados utilizando os diferentes componentes da solução de carteira, com base numa fundamentação que explique por que razão é necessário um determinado nível de garantia e da forma como o controlo é aplicado com todos os aspetos de segurança exigidos ao nível adequado,

— *fundamentação e justificação da cobertura dos riscos:* uma justificação:

— do levantamento dos controlos aos componentes;

— da adequação do plano de avaliação proposto para abranger adequadamente todos os controlos;

— da cobertura proporcionada pelos controlos dos riscos e ameaças de cibersegurança identificados no registo de riscos, complementados por controlos dos riscos e ameaças específicos à execução, ao nível de garantia adequado;

b) As informações enumeradas no anexo V;

c) Uma lista completa dos certificados de conformidade e outras informações sobre a garantia utilizadas como elementos de prova durante as atividades de avaliação;

d) Quaisquer outras informações pertinentes para as atividades de avaliação.

CAPÍTULO V

REQUISITOS RELATIVOS AOS ORGANISMOS DE CERTIFICAÇÃO

Artigo 9.º

Requisitos gerais

1. Os organismos de certificação devem ser acreditados por organismos nacionais de acreditação nomeados nos termos do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho ([13]) em conformidade com a norma EN ISO/IEC 17065:2012, desde que cumpram os requisitos estabelecidos nos sistemas nacionais de certificação em conformidade com o n.º 2.

2. Para efeitos de acreditação, os organismos de certificação devem cumprir todos os seguintes requisitos em matéria de competência:

a) Conhecimentos pormenorizados e técnicos das arquiteturas pertinentes de uma solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada, bem como das ameaças e riscos relevantes para essas arquiteturas;

b) Conhecimentos das soluções de segurança disponíveis e das suas propriedades, em conformidade com o anexo do Regulamento de Execução (UE) 2015/1502;

c) Conhecimentos das atividades realizadas por força dos certificados de conformidade aplicados aos componentes da solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada, como objeto da certificação;

d) Conhecimentos pormenorizados do sistema nacional de certificação aplicável, conforme estabelecido em conformidade com o capítulo II.

3. Os organismos de certificação devem realizar as suas atividades de fiscalização com base, nomeadamente, nas seguintes informações:

a) Informações provenientes dos organismos nacionais de acreditação e das autoridades de fiscalização do mercado competentes;

b) Informações resultantes de auditorias e de investigações efetuadas pela própria autoridade ou por outra autoridade;

c) Reclamações e recursos recebidos nos termos do artigo 15.º.

Artigo 10.º

Subcontratação

Os organismos de certificação podem subcontratar a terceiros as atividades de avaliação, conforme previsto no artigo 13.º. Caso as atividades de avaliação sejam subcontratadas, os sistemas nacionais de certificação devem estabelecer o seguinte:

(1) Todos os subcontratantes do organismo de certificação que realizem atividades de avaliação devem, conforme aplicável e adequado para as atividades a realizar, cumprir os requisitos das normas harmonizadas, como a EN ISO/IEC 17025:2017 para os ensaios, a EN ISO/IEC 17020:2012 para a inspeção, a EN ISO/IEC 17021-1:2015 para a auditoria e a EN ISO/IEC 17029:2019 para a validação e verificação;

(2) Os organismos de certificação devem assumir a responsabilidade por todas as atividades de avaliação subcontratadas a outros organismos e demonstrar que tomaram as medidas adequadas durante a sua acreditação, nomeadamente ao recorrerem à própria acreditação dos seus subcontratantes, se for caso disso;

(3) O grau em que o acordo prévio sobre as necessidades de externalização deve ser obtido junto dos proprietários dos sistemas ou dos clientes cuja solução de carteira está a ser certificada ao abrigo do sistema de certificação.

([13]) Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Artigo 11.º

Notificação à entidade supervisora

Os organismos de certificação devem notificar à entidade supervisora a que se refere o artigo 46.º-A, n.º 1, do Regulamento (UE) n.º 910/2014 a emissão, suspensão e cancelamento dos certificados de conformidade de soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas.

Artigo 12.º

Gestão de incidentes e vulnerabilidades

1. Os organismos de certificação devem suspender, sem demora injustificada, o certificado de conformidade das soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas depois de confirmarem que a violação ou comprometimento de segurança notificado afeta a conformidade com os requisitos dos sistemas nacionais de certificação, da solução de carteira ou do sistema de identificação eletrónica ao abrigo do qual é disponibilizada.

2. Os organismos de certificação devem cancelar o certificado de conformidade que foi suspenso na sequência de uma violação ou comprometimento de segurança que não tenha sido sanado em tempo útil.

3. Os organismos de certificação devem cancelar os certificados de conformidade sempre que uma vulnerabilidade identificada não tenha sido sanada proporcionalmente à sua gravidade e potencial impacto em tempo útil, em conformidade com o artigo 5.º-C, n.º 4, e com o artigo 5.º-E, n.º 2, do Regulamento (UE) n.º 910/2014.

CAPÍTULO VI

ATIVIDADES DE AVALIAÇÃO DA CONFORMIDADE

Artigo 13.º

Atividades de avaliação

1. Os sistemas nacionais de certificação devem conter métodos e procedimentos a utilizar pelos organismos de avaliação da conformidade na realização das suas atividades de avaliação em conformidade com a norma EN ISO/IEC 17065:2012, que devem abranger, pelo menos, os seguintes aspetos:

a) Os métodos e procedimentos para a realização das atividades de avaliação, incluindo os relacionados com o WSCD, conforme estabelecido no anexo IV;

b) A auditoria da implementação da solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada, com base no registo de riscos, estabelecido no anexo I e completado, se necessário, por riscos específicos da aplicação;

c) Atividades funcionais de ensaio, baseadas, quando disponíveis e adequadas, em conjuntos de ensaios definidos de acordo com normas ou especificações técnicas;

d) Avaliação da existência e adequação de processos de manutenção, incluindo, pelo menos, a gestão de versões, a gestão de atualizações e a gestão de vulnerabilidades;

e) Avaliação da eficácia operacional dos processos de manutenção, incluindo, pelo menos, a gestão de versões, a gestão de atualizações e a gestão de vulnerabilidades;

f) Análise da dependência facultada pelo fornecedor de carteiras, incluindo uma metodologia para avaliar a aceitabilidade das informações sobre a garantia, que deve incluir os elementos estabelecidos no anexo VI;

g) Avaliação da vulnerabilidade, ao nível adequado, incluindo:

— uma revisão da conceção da solução de carteira e, se for caso disso, do seu código-fonte,

— ensaio da resistência da solução de carteira contra ataques de elevado potencial para a atribuição do nível de garantia «elevado», em conformidade com a secção 2.2.1 do anexo do Regulamento de Execução (UE) 2015/1502;

h) Avaliação da evolução do ambiente de ameaça e do seu impacto na cobertura dos riscos pela solução de carteira, a fim de determinar quais são as atividades de avaliação necessárias para os vários componentes da solução de carteira.

2. Os sistemas nacionais de certificação devem incluir uma avaliação para determinar se a implementação de soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual essas soluções de carteiras são disponibilizadas corresponde à arquitetura estabelecida no artigo 3.º, n.º 5, alínea a), bem como uma avaliação para determinar se o plano de avaliação proposto, juntamente com a implementação, corresponde ao plano de avaliação a que se refere o artigo 3.º, n.º 5, alínea c).

3. Os sistemas nacionais de certificação devem estabelecer regras de amostragem, a fim de evitar a repetição de atividades de avaliação idênticas e centrar-se em atividades específicas para uma determinada variante. Essas regras de amostragem devem permitir a realização de ensaios funcionais e de segurança apenas numa amostra de variantes de um componente-alvo de uma solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada, bem como numa amostra de dispositivos-alvo. Os sistemas nacionais de certificação devem exigir que todos os organismos de certificação justifiquem o recurso à amostragem.

4. Os sistemas nacionais de certificação devem exigir que o organismo de certificação avalie a WSCA com base nos métodos e procedimentos estabelecidos no anexo IV.

Artigo 14.º

Atividades de certificação

1. Os sistemas nacionais de certificação devem estabelecer uma atividade de certificação para efeitos de emissão de um certificado de conformidade, nos termos da secção V, alínea a), quadro 1, da norma EN ISO/IEC 17067:2013, incluindo os seguintes aspetos:

a) O teor do certificado de conformidade conforme estabelecido no anexo VII;

b) A forma como os resultados da avaliação devem ser comunicados no relatório público de certificação, incluindo, pelo menos, um resumo do plano preliminar de auditoria e validação, conforme estabelecido no anexo VIII;

c) O teor dos resultados da avaliação comunicados no relatório de avaliação da certificação, incluindo os elementos estabelecidos no anexo VIII.

2. O relatório de avaliação da certificação pode ser disponibilizado ao grupo de cooperação e à Comissão.

Artigo 15.º

Reclamações e recursos

Os sistemas nacionais de certificação devem conter procedimentos ou referências à legislação nacional aplicável, que definem o mecanismo de apresentação e tratamento eficazes de reclamações e recursos relacionados com a sua aplicação do sistema de certificação ou de um certificado de conformidade emitido. Estes procedimentos devem incluir a prestação de informações ao autor da reclamação sobre o andamento do processo e sobre a decisão tomada, bem como sobre o seu direito a um recurso judicial efetivo. Os sistemas nacionais de certificação devem exigir que todas as reclamações e recursos que não tenham sido ou não possam ser resolvidos pelo organismo de certificação sejam enviados ao proprietário do sistema para avaliação e resolução.

Artigo 16.º

Atividades de fiscalização

1. Os sistemas nacionais de certificação devem exigir que os organismos de certificação executem atividades de fiscalização que consistam na avaliação da fiscalização dos processos combinada com ensaios ou inspeções aleatórios.

2. Os sistemas nacionais de certificação devem incluir requisitos para que os proprietários dos sistemas acompanhem o cumprimento, por parte dos organismos de certificação, das obrigações que lhes incumbem por força do Regulamento (UE) n.º 910/2014 e dos sistemas nacionais de certificação, se for caso disso.

3. Os sistemas nacionais de certificação devem incluir requisitos para que os organismos de certificação monitorizem o seguinte:

a) O cumprimento, por parte dos titulares de um certificado de conformidade emitido ao abrigo de sistemas nacionais de certificação, das suas obrigações em matéria de certificação nos termos do Regulamento (UE) n.º 910/2014 e dos sistemas nacionais de certificação;

b) A conformidade da solução de carteira certificada com os requisitos estabelecidos nos sistemas nacionais de certificação.

Artigo 17.º

Consequências do incumprimento

Os sistemas nacionais de certificação devem definir as consequências da não conformidade de uma solução de carteira certificada e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada com os requisitos estabelecidos no presente regulamento. Essas consequências devem incluir os seguintes aspetos:

1) A obrigação do organismo de certificação de informar o titular do certificado de conformidade e de lhe solicitar que aplique medidas corretivas;

2) A obrigação de o organismo de certificação informar outras autoridades de fiscalização do mercado competentes sempre que a não conformidade diga respeito à legislação pertinente da União;

3) As condições para a execução de medidas corretivas pelo titular do certificado de conformidade;

4) As condições para a suspensão de um certificado de conformidade pelo organismo de certificação e para o restabelecimento do certificado de conformidade após a não conformidade ser corrigida;

5) As condições de cancelamento de um certificado de conformidade pelo organismo de certificação;

6) As consequências do incumprimento, por parte do organismo de certificação, dos requisitos do sistema nacional de certificação.

CAPÍTULO VII

CICLO DE VIDA DA CERTIFICAÇÃO

Artigo 18.º

Ciclo de vida da certificação

1. A validade dos certificados de conformidade emitidos ao abrigo de sistemas nacionais de certificação deve ser sujeita a atividades de avaliação regular pelo organismo de certificação, realizadas em conformidade com os requisitos estabelecidos no anexo IX.

2. Os sistemas nacionais de certificação devem incluir um processo de recertificação de soluções de carteiras e do sistema de identificação eletrónica ao abrigo do qual são disponibilizadas, a pedido do titular do certificado de conformidade antes do termo da validade do certificado de conformidade inicial. Esse processo de recertificação deve incluir uma avaliação completa da solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada, incluindo uma avaliação da vulnerabilidade, de acordo com os princípios estabelecidos no anexo IX.

3. Os sistemas nacionais de certificação devem incluir um processo de gestão das alterações de uma solução de carteira certificada e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada. Esse processo deve incluir regras para determinar se uma alteração deve ser abrangida pela avaliação especial a que se refere o n.º 4 ou pela verificação da eficácia operacional dos processos de manutenção a que se refere o anexo IV.

4. Os sistemas nacionais de certificação devem incluir um processo de avaliação especial em conformidade com a norma EN ISO/IEC 17065:2012. Esse processo de avaliação especial deve incluir uma seleção das atividades a realizar para dar resposta à questão específica que motivou a avaliação especial.

5. Os sistemas nacionais de certificação devem estabelecer regras relativas ao cancelamento de um certificado de conformidade.

CAPÍTULO VIII

CONSERVAÇÃO DE REGISTOS E PROTEÇÃO DAS INFORMAÇÕES

Artigo 19.º

Conservação de registos

1. Os sistemas nacionais de certificação devem incluir requisitos aplicáveis aos organismos de certificação relativos a um sistema de registos de todas as informações pertinentes produzidas no âmbito das atividades de avaliação da conformidade que realizam, incluindo os dados emitidos e recebidos pelos fornecedores de carteiras e pelos sistemas de identificação eletrónica ao abrigo dos quais são disponibilizadas. Os registos dessas informações devem ser armazenados de forma segura. Os registos podem ser conservados eletronicamente e devem permanecer acessíveis durante o período exigido pelo direito da União ou pelo direito nacional, e durante, pelo menos, cinco anos após o cancelamento ou o termo de validade do certificado de conformidade pertinente.

2. Os sistemas nacionais de certificação devem estabelecer requisitos para que o titular do certificado de conformidade armazene as seguintes informações de forma segura para efeitos do presente regulamento e durante, pelo menos, cinco anos após o cancelamento ou o termo do respetivo certificado de conformidade:

a) Registos das informações facultadas ao organismo de certificação ou a qualquer dos seus subcontratantes durante o processo de certificação;

b) Amostras de componentes de *hardware* que tenham sido incluídos no âmbito da certificação da solução de carteira.

3. Os sistemas nacionais de certificação devem exigir que o titular do certificado de conformidade disponibilize as informações referidas no n.º 1 ao organismo de certificação ou à entidade supervisora a que se refere o artigo 46.º-A, n.º 1, do Regulamento (UE) n.º 910/2014, mediante pedido.

Artigo 20.º

Proteção das informações

No âmbito dos sistemas nacionais de certificação, deve ser exigido a todas as pessoas ou organizações às quais seja concedido acesso a informações na execução de atividades ao abrigo do sistema nacional de certificação que garantam a segurança e a proteção dos segredos comerciais e de outras informações confidenciais, bem como que preservem os direitos de propriedade intelectual e tomem as medidas técnicas e organizativas necessárias e adequadas para garantir essa confidencialidade.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Artigo 21.º

Transição para o sistema europeu de certificação da cibersegurança

O presente regulamento deve ser objeto de revisão aquando da adoção do primeiro sistema europeu de certificação da cibersegurança para soluções de carteiras e para os sistemas de identificação eletrónica ao abrigo dos quais são disponibilizadas, com o objetivo de ter em conta o contributo desse sistema europeu de certificação da cibersegurança para a certificação global das soluções de carteiras e dos sistemas de identificação eletrónica ao abrigo dos quais são disponibilizadas.

Artigo 22.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 28 de novembro de 2024.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO I

REGISTO DE RISCOS PARA CARTEIRAS EUROPEIAS DE IDENTIDADE DIGITAL

Introdução

O registo de riscos descreve os principais riscos e ameaças à segurança e à privacidade aplicáveis às carteiras e que devem ser devidamente tidos em conta em cada arquitetura e aplicação de carteiras. Os **riscos de alto nível** (secção I) estão relacionados com a utilização de carteiras pelos utentes e pelos utilizadores e estão associados a ameaças diretas que visam os ativos das carteiras. Além disso, são identificados alguns **riscos ao nível do sistema** (secção II) para as carteiras, que normalmente resultariam de uma combinação de ameaças aplicáveis a todo o sistema de carteiras.

Tipo de risco	Identificação do risco	Títulos relacionados com o risco
Riscos de alto nível para as carteiras	R1	Criação ou utilização de uma identidade eletrónica existente
	R2	Criação ou utilização de uma identidade eletrónica falsa
	R3	Criação ou utilização de atributos falsos
	R4	Usurpação de identidade
	R5	Roubo de dados
	R6	Divulgação de dados
	R7	Manipulação de dados
	R8	Perda de dados
	R9	Transação não autorizada
	R10	Manipulação da transação
	R11	Repúdio
	R12	Divulgação de dados da transação
	R13	Perturbação do serviço
	R14	Vigilância
Riscos relacionados com o sistema	SR1	Vigilância em grande escala
	SR2	Danos à reputação
	SR3	Incumprimento legal

O registo identifica igualmente **ameaças técnicas** (secção III) que visam a aplicação da solução de carteira. Estas ameaças estão relacionadas com os riscos de alto nível, no sentido em que cada uma delas pode ser utilizada para desencadear muitos riscos de alto nível.

Tipo de ameaça	Identificação da ameaça	Títulos relacionados com a ameaça	Subcategorias de ameaças
Ameaça técnica	TT1	Ataques físicos	1.1. *Roubo*
			1.2. *Fugas de informação*
			1.3. *Adulteração*
	TT2	Erros e configurações incorretas	2.1. *Erros cometidos na gestão de um sistema informático*
			2.2. *Erros ao nível da aplicação ou erros de utilização*
			2.3. *Erros de tempo de desenvolvimento e configurações incorretas do sistema*

Tipo de ameaça	Identificação da ameaça	Títulos relacionados com a ameaça	Subcategorias de ameaças
	TT3	Utilização de recursos não fiáveis	3.1. *Utilização ou configuração erradas dos componentes da carteira*
	TT4	Falha e interrupções	4.1. *Falha ou mau funcionamento dos equipamentos, dispositivos ou sistemas*
			4.2. *Perda de recursos*
			4.3. *Perda de serviços de apoio*
	TT5	Ações maliciosas	5.1. *Interceção de informações*
			5.2. *Mistificação da interface e mistificação da identidade*
			5.3. *Reprodução de mensagens*
			5.4. *Ataque de força bruta*
			5.5. *Vulnerabilidades do software*
			5.6. *Ataques à cadeia de abastecimento*
			5.7. *Software malicioso*
			5.8. *Previsão de número aleatório*

Por último, o registo **enumera as ameaças diretas às carteiras** e cada uma delas está associada a uma seleção (não exaustiva) dos riscos (secção IV).

SECÇÃO I

Riscos de alto nível para as carteiras

R1. Criação ou utilização de uma identidade eletrónica existente

A criação ou utilização de uma identidade eletrónica existente é definida como a criação de uma identidade eletrónica numa carteira que existe no mundo real e que é atribuída a outro utente. Em substância, este risco conduz aos riscos de usurpação de identidade (R4) e de transações não autorizadas (R9).

R2. Criação ou utilização de uma identidade eletrónica falsa

A criação ou utilização de uma identidade eletrónica falsa é definida como a criação de uma identidade eletrónica numa carteira que não existe no mundo real.

R3. Criação ou utilização de atributos falsos

A criação ou utilização de atributos falsos é definida como a criação ou utilização de atributos que não podem ser validados para a emissão pelo fornecedor declarado e nos quais não é possível confiar.

R4. Usurpação de identidade

A usurpação de identidade é definida como a aquisição não autorizada da unidade de carteira ou a perda de fatores de autenticação que permitem assumir a identidade de uma pessoa.

R5. Roubo de dados

O roubo de dados é definido como a extração não autorizada de dados. O roubo de dados está também associado a ameaças, como a interceção de dados (captura não autorizada de dados em trânsito) e a decifragem de dados (descodificação não autorizada de dados cifrados), que são suscetíveis de conduzir, em alguns casos, à divulgação de dados (R6).

R6. Divulgação de dados

A divulgação de dados é definida como a exposição não autorizada de dados pessoais, incluindo categorias especiais de dados pessoais. O risco de violação da privacidade é muito semelhante quando considerado do ponto de vista da privacidade e não do ponto de vista da segurança.

R7. Manipulação de dados

A manipulação de dados é definida como a alteração não autorizada de dados.

R8. Perda de dados

A perda de dados é definida como a situação em que os dados armazenados na carteira se perdem por má utilização ou ação maliciosa. Este risco é frequentemente um risco secundário da manipulação de dados (R7) ou da perturbação do serviço (R13), em que não é possível recuperar a totalidade ou parte dos dados.

R9. Transação não autorizada

As transações não autorizadas são definidas como atividades operacionais realizadas sem autorização ou conhecimento do utente da carteira. Em muitos casos, uma transação não autorizada pode conduzir à usurpação de identidade (R4) ou à divulgação de dados (R6). Está também relacionada com transações não autorizadas, como a utilização indevida de chaves criptográficas.

R10. Manipulação da transação

A manipulação da transação é definida como a alteração não autorizada de operações na carteira. A manipulação da transação é um ataque à integridade e está relacionada com uma violação da integridade dos dados.

R11. Repúdio

O repúdio é definido como uma situação em que uma parte interessada pode recusar a realização de uma ação ou recusar envolver-se numa transação e outras partes interessadas não dispõem de elementos de prova adequados para a contradizer.

R12. Divulgação de dados da transação

A divulgação de dados da transação é definida como a divulgação de informações relacionadas com informações sobre uma transação entre partes interessadas.

R13. Perturbação do serviço

A perturbação do serviço é definida como uma interrupção ou degradação do funcionamento normal da carteira. Um tipo específico de perturbação do serviço consiste no bloqueio do utente, definido como a incapacidade de um utente aceder à sua conta ou carteira.

R14. Vigilância

A vigilância, ou monitorização, é definida como o rastreio ou observação não autorizados das atividades, comunicações ou dados do utente de uma carteira. A vigilância está frequentemente relacionada com a inferência, que é definida como a dedução de informações sensíveis ou pessoais a partir de dados aparentemente inócuos.

SECÇÃO II

Riscos relacionados com o sistema

Estes riscos não são utilizados na lista de ameaças, pois normalmente são consequência de ameaças múltiplas e repetidas de uma forma que ameaça todo o sistema.

SR1. Vigilância em grande escala

A vigilância em grande escala é definida como o rastreio ou a observação das atividades de muitos utentes através da comunicação ou dos dados da sua carteira. A vigilância em grande escala está frequentemente associada à vigilância (R14) e à inferência à escala mundial, em que são combinadas informações sobre muitos utentes para deduzir dados sensíveis ou pessoais sobre os mesmos ou para identificar tendências estatísticas que possam ser utilizadas para conceber novos ataques.

SR2. Danos à reputação

Os danos à reputação são definidos como os danos causados à reputação de uma organização ou organismo governamental. Os danos à reputação também resultarão de outros riscos, caso uma violação ou um incidente seja coberto pelos meios de comunicação social e retrate desfavoravelmente a organização. Os danos à reputação podem conduzir a outros riscos, como a perda de confiança, decorrente das dúvidas razoáveis dos utentes, e a perda do ecossistema, quando todo o ecossistema se desmorona.

SR3. Incumprimento legal

O incumprimento legal é definido como uma situação em que não é possível cumprir as leis, regulamentos ou normas pertinentes. No contexto da carteira, uma vez que a segurança e a privacidade da solução são requisitos legais, é provável que todas as ameaças conduzam a algum tipo de incumprimento legal.

SECÇÃO III

Ameaças técnicas

Nem todas as ameaças técnicas estão associadas a riscos específicos das carteiras, pois muitas delas são meios que podem ser utilizados para realizar ataques correspondentes a muitos riscos diferentes.

TT1. Ataques físicos

1.1. *Roubo*

O roubo é definido como o roubo de dispositivos, suscetível de alterar o bom funcionamento da carteira (caso o dispositivo seja roubado e a unidade de carteira não esteja adequadamente protegida). Tal pode contribuir para muitos riscos, incluindo a usurpação de identidade (R4), o roubo de dados (R5) e as transações não autorizadas (R9).

1.2. *Fugas de informação*

As fugas de informação são definidas como o acesso não autorizado, a exposição de informações ou a partilha após o acesso físico à carteira. Tal pode contribuir, em especial, para a divulgação de dados (R6) e o roubo de dados (R5).

1.3. *Adulteração*

A adulteração é definida como a violação da integridade de um ou vários componentes da unidade de carteira, ou dos componentes dos quais a unidade de carteira depende, por exemplo, o dispositivo do utente ou o seu sistema operativo. Tal pode contribuir, em especial, para a manipulação de dados (R7), a perda de dados (R8) e a manipulação da transação (R10). Quando a adulteração visa componentes de *software*, pode contribuir para muitos riscos.

TT2. Erros e configurações incorretas

2.1. *Erros cometidos na gestão de um sistema informático*

Os erros cometidos na gestão de um sistema informático são definidos como fugas de informação, partilha ou danos causados pela má utilização de ativos informáticos pelos utentes (falta de conhecimento das funcionalidades da aplicação) ou pela configuração ou gestão inadequadas dos ativos informáticos.

2.2. *Erros ao nível da aplicação ou erros de utilização*

Os erros ao nível da aplicação ou erros de utilização são definidos como disfunções da aplicação devidas a um erro na própria aplicação ou a um erro cometido por um dos utilizadores (utentes e utilizadores de carteiras).

2.3. *Erros de tempo de desenvolvimento e configurações incorretas do sistema*

Os erros de tempo de desenvolvimento e configurações incorretas do sistema são definidos como disfunções ou vulnerabilidades causadas por ativos informáticos ou processos operacionais mal desenvolvidos ou configurados (especificações inadequadas dos produtos informáticos, usabilidade inadequada, interfaces inseguras, fluxos inadequados de políticas e procedimentos, erros de conceção).

TT3. Utilização de recursos não fiáveis

A utilização de recursos não fiáveis é definida como uma atividade conducente a danos não intencionais devidos a relações de confiança mal definidas, como confiar num fornecedor terceiro sem garantias suficientes.

3.1. *Utilização ou configuração erradas dos componentes da carteira*

Uma utilização ou configuração erradas dos componentes da carteira é definida como danos não intencionais causados aos componentes da carteira devidos a uma utilização incorreta ou má configuração por utentes da carteira ou programadores sem formação suficiente, ou devidos à falta de adaptação às alterações do cenário de ameaça, normalmente, a utilização de componentes de terceiros vulneráveis ou de plataformas de tempo de execução.

TT4. Falha e interrupções

4.1. *Falha ou mau funcionamento dos equipamentos, dispositivos ou sistemas*

Uma falha ou mau funcionamento dos equipamentos é definida como danos não intencionais causados a ativos informáticos devidos a uma falha ou mau funcionamento dos equipamentos, incluindo a infraestrutura do fornecedor e os dispositivos do utente.

4.2. *Perda de recursos*

A perda de recursos é definida como uma falha ou disfunção devida à indisponibilidade desses recursos, por exemplo, como peças sobresselentes.

4.3. *Perda de serviços de apoio*

A perda de serviços de apoio é definida como uma falha ou disfunção devida à indisponibilidade dos serviços de apoio necessários para o bom funcionamento do sistema, incluindo a conectividade da rede da infraestrutura do fornecedor e do dispositivo do utente.

TT5. Ações maliciosas

5.1. *Interceção de informações*

A interceção de informações é definida como a recolha de informações indevidamente protegidas na transmissão, incluindo ataques por interposição (*man-in-the-middle*).

5.2. *Mistificação da interface e mistificação da identidade*

A mistificação da interface é definida como a recolha de informações fornecidas pelo utente na sequência de uma interação enganosa, muitas vezes associada à mistificação da identidade de meios de comunicação e sítios Web legítimos. Estas ameaças visam o utente e, normalmente, contribuem para a usurpação de identidade (R4) e para as transações não autorizadas (R9), muitas vezes através do roubo de dados (R5) ou da divulgação de dados (R6).

5.3. *Reprodução de mensagens*

A reprodução de mensagens é definida como a reutilização de mensagens anteriormente intercetadas, a fim de realizar transações não autorizadas, muitas vezes ao nível do protocolo. Esta ameaça técnica contribui principalmente para transações não autorizadas, o que pode conduzir a outros riscos, dependendo da transação.

5.4. *Ataque de força bruta*

O ataque de força bruta é definido como uma violação da segurança, muitas vezes da confidencialidade, através da realização de um grande número de interações até que as respostas forneçam informações valiosas.

5.5. *Vulnerabilidades do software*

A ameaça relacionada com vulnerabilidades do *software* é uma violação da segurança através da exploração de uma vulnerabilidade do *software* nos componentes da carteira ou nos componentes de *software* e *hardware* utilizados na aplicação da carteira, incluindo vulnerabilidades publicadas e vulnerabilidades não publicadas (0 dias).

5.6. *Ataques à cadeia de abastecimento*

Um ataque à cadeia de abastecimento é definido como uma violação da segurança através de ataques perpetrados contra o fornecedor do fornecedor de carteiras ou dos seus utentes, a fim de permitir novos ataques à própria carteira.

5.7. *Software malicioso*

O *software* malicioso é definido como uma violação da segurança através de aplicações maliciosas que realizam ações indesejadas e ilegítimas na carteira.

5.8. *Previsão de número aleatório*

A previsão de número aleatório é definida como a facilitação de ataques de força bruta através de uma previsão parcial ou completa dos números aleatórios gerados.

SECÇÃO IV

Ameaças às carteiras

Esta última secção apresenta uma seleção de cenários de ameaça típicos específicos das carteiras, cujo levantamento é realizado em função dos principais riscos de alto nível conexos, conforme enumerados *supra*. Esta lista indica as ameaças que devem ser abrangidas, mas não constitui uma lista exaustiva de ameaças, as quais dependem, em grande medida, da arquitetura da solução de carteira selecionada e da evolução do ambiente de ameaça. Além disso, na avaliação dos riscos e nas medidas propostas, o fornecedor de carteiras só pode ser responsável pelos componentes abrangidos pelo âmbito da certificação (*).

IDENTIFICAÇÃO *Identificador*	Descrição da ameaça *Descrição da ameaça identificada (*)*	Título do risco *Riscos relacionados*
TR1	Um atacante pode revogar pseudónimos sem motivo justificado.	Criação ou utilização de uma identidade eletrónica falsa (R2)
TR2	Um atacante pode emitir identidades eletrónicas falsificadas que não existem.	Criação ou utilização de uma identidade eletrónica falsa (R2)
TR3	Um atacante pode começar a emitir PID (dados de identificação pessoal, do inglês *personal identification data*) não autorizados.	Criação ou utilização de uma identidade eletrónica falsa (R2)
TR4	Um atacante pode levar um administrador a introduzir um fornecedor errado de PID na lista de confiança de fornecedores de PID.	Criação ou utilização de uma identidade eletrónica falsa (R2)
TR5	Um atacante pode contornar o serviço remoto de prova da identidade.	Criação ou utilização de uma identidade eletrónica existente (R1)/Criação ou utilização de uma identidade eletrónica falsa (R2)
TR6	Um atacante pode contornar o serviço físico de prova da identidade.	Criação ou utilização de uma identidade eletrónica existente (R1)/Criação ou utilização de uma identidade eletrónica falsa (R2)
TR7	Um atacante pode contornar os serviços de prova da identidade relacionados com a utilização de um certificado remoto (qualificado).	Criação ou utilização de uma identidade eletrónica existente (R1)/Criação ou utilização de uma identidade eletrónica falsa (R2)
TR8	Um atacante pode ter acesso a uma carteira que não está vinculada a uma pessoa.	Criação ou utilização de uma identidade eletrónica existente (R1)/Criação ou utilização de uma identidade eletrónica falsa (R2)
TR9	Um atacante pode invalidar os controlos técnicos e processuais para criar PID incorretos.	Criação ou utilização de uma identidade eletrónica existente (R1)/Criação ou utilização de uma identidade eletrónica falsa (R2)
TR10	Um atacante pode ativar uma nova carteira num WSCD inválido.	Criação ou utilização de uma identidade eletrónica existente (R1)/Criação ou utilização de uma identidade eletrónica falsa (R2)
TR11	Um atacante pode contornar o serviço de prova da identidade relacionado com a utilização de meios de identificação eletrónica existentes.	Criação ou utilização de uma identidade eletrónica existente (R1)/Usurpação de identidade (R4)/Transação não autorizada (R9)
TR12	Um atacante pode contornar a verificação efetuada pelo fornecedor de PID de que a carteira é controlada pelo utente e fazer com que sejam emitidos PID para uma carteira comprometida que está sob o controlo do atacante.	Criação ou utilização de uma identidade eletrónica existente (R1)/Usurpação de identidade (R4)/Transação não autorizada (R9)

IDENTIFICAÇÃO *Identificador*	Descrição da ameaça *Descrição da ameaça identificada (*)*	Título do risco *Riscos relacionados*
TR13	Um atacante pode inserir PID válidos numa unidade de carteira inválida.	Criação ou utilização de uma identidade eletrónica existente (R1)/Usurpação de identidade (R4)/Transação não autorizada (R9)
TR14	Um fornecedor de PID pode emitir identidades falsificadas, em casos em que as identidades estão relacionadas com pessoas existentes.	Criação ou utilização de uma identidade eletrónica existente (R1)/Usurpação de identidade (R4)/Transação não autorizada (R9)
TR15	Um atacante pode associar PID à carteira errada, pois o fornecedor de PID não pode associar os dados à carteira correta.	Criação ou utilização de uma identidade eletrónica existente (R1)/Usurpação de identidade (R4)/Transação não autorizada (R9)
TR16	Um atacante pode fazer com que o utente aprove a ativação de uma nova unidade/instância de carteira que se encontra sob o controlo do atacante, controlando também subsequentemente os certificados.	Criação ou utilização de uma identidade eletrónica existente (R1)/Criação ou utilização de uma identidade eletrónica falsa (R2)/Usurpação de identidade (R4)/Transação não autorizada (R9)
TR17	Um atacante pode emitir PID de outro Estado para aceder a dados/ativos digitais de cidadãos visados.	Criação ou utilização de uma identidade eletrónica existente (R1)/Usurpação de identidade (R4)/Transação não autorizada (R9)
TR18	Um atacante pode invalidar os controlos técnicos e processuais para criar (Q)EAA (certificado eletrónico de atributos [qualificado], do inglês *[qualified] electronic attestation of attributes*) falsos.	Criação ou utilização de atributos falsos (R3)
TR19	Um atacante pode apresentar (Q)EAA que não foram emitidos para si de forma válida.	Criação ou utilização de atributos falsos (R3)
TR20	Um atacante pode atacar o mecanismo de ligação criptográfica da carteira entre os PID e um (Q)EAA que não lhe devia ser emitido.	Criação ou utilização de atributos falsos (R3)
TR21	Um atacante pode utilizar um (Q)EAA numa carteira, embora a contraparte física do (Q)EAA tenha caducado ou seja inválida.	Criação ou utilização de atributos falsos (R3)
TR22	Um atacante pode contornar a verificação efetuada pelo fornecedor do (Q)EAA de que o utente controla a carteira e fazer com que seja emitido um (Q)EAA para uma carteira comprometida que está sob o controlo do atacante.	Criação ou utilização de atributos falsos (R3)
TR23	Um atacante pode falsificar certificados eletrónicos de atributos.	Criação ou utilização de atributos falsos (R3)
TR24	Um atacante pode injetar certificados eletrónicos de atributos falsificados numa carteira.	Criação ou utilização de atributos falsos (R3)
TR25	A carteira pode apresentar atributos a um utilizador sem a aprovação de um utente.	Divulgação de dados (R6)
TR26	Podem ser apresentados PID, (Q)EAA ou pseudónimos a um utilizador errado.	Divulgação de dados (R6)
TR27	Um atacante pode iniciar uma renovação mal-intencionada do EAA.	Divulgação de dados (R6)
TR28	Um atacante pode levar um utente a aprovar indevidamente um pedido de certificados eletrónicos de atributos (mistificação da interface ou outro).	Divulgação de dados (R6)

IDENTIFICAÇÃO *Identificador*	Descrição da ameaça *Descrição da ameaça identificada (*)*	Título do risco *Riscos relacionados*
TR29	Um atacante pode divulgar atributos da carteira e identificar o utente da carteira quando a identificação não é necessária/permitida.	Divulgação de dados (R6)
TR30	Um atacante pode invalidar os controlos técnicos e processuais para extrair dados.	Divulgação de dados (R6)
TR31	Um pedido pode ser divulgado ao atacante.	Divulgação de dados (R6)
TR32	Um atacante pode obter informações sobre a política de divulgação incorporada para atributos e apresentar atributos contidos no pedido atual das unidades de carteira.	Divulgação de dados (R6)
TR33	Um atacante pode extrair registos ou excertos dos mesmos.	Divulgação de dados (R6)
TR34	Um atacante pode saber se uma carteira está instalada no mesmo dispositivo que utiliza, ou noutro, e obter informações sobre o mesmo.	Divulgação de dados (R6)
TR35	Um atacante pode obter um fator de conhecimento utilizado para autenticar o utente na WSCA.	Divulgação de dados (R6)
TR36	O certificado eletrónico de atributos relativo a uma pessoa que é apresentado em várias transações com um utilizador, ou entre diferentes utilizadores, permite, de forma não intencional, associar várias transações à pessoa pertinente.	Divulgação de dados (R6)
TR37	Uma lista pública de revogação de certificados/utilizadores pode conter informações sobre a utilização que o utente faz do seu certificado (por exemplo, localização, endereço IP, etc.).	Divulgação de dados (R6)
TR38	Não sendo capazes de provar o consentimento do utente para os atributos partilhados, os utilizadores podem comprometer a integridade dos registos.	Divulgação de dados (R6)
TR39	Um atacante pode rastrear ilegalmente os utentes das carteiras utilizando identificadores únicos/rastreáveis.	Divulgação de dados (R6)/Vigilância (R14)
TR40	Um utilizador composto por várias unidades/entidades, cada uma com um âmbito diferente quanto ao que está autorizada a solicitar/tratar, pode solicitar e tratar dados sem estar legalmente habilitado.	Divulgação de dados (R6)/Transação não autorizada (R9)
TR41	Um atacante pode subverter os controlos de integridade e autenticidade efetuados aos PID pela carteira, a fim de serem sempre bem-sucedidos.	Manipulação de dados (R7)
TR42	Um atacante pode contornar ou subverter o desempenho dos controlos realizados pela carteira, que verificam a integridade e a autenticidade dos atributos solicitados, a fim de serem sempre bem-sucedidos.	Manipulação de dados (R7)
TR43	Um atacante pode contornar ou subverter o desempenho dos controlos realizados pela carteira, que verificam todos os atributos solicitados pertencentes ao mesmo utente, a fim de serem sempre bem-sucedidos.	Manipulação de dados (R7)
TR44	Um atacante pode contornar ou subverter o desempenho dos controlos realizados pela carteira para verificar se os PID são válidos e se foram emitidos por um fornecedor de PID de confiança, a fim de obter sempre um resultado positivo.	Manipulação de dados (R7)

IDENTIFICAÇÃO *Identificador*	Descrição da ameaça *Descrição da ameaça identificada (*)*	Título do risco *Riscos relacionados*
TR45	Um atacante pode contornar ou subverter o desempenho dos controlos realizados pela carteira para verificar se um QEAA é válido e se foi emitido por um fornecedor de confiança qualificado, que está registado para emitir o QEAA, a fim de obter sempre um resultado positivo.	Manipulação de dados (R7)
TR46	Um atacante pode contornar ou subverter o desempenho dos controlos realizados pela carteira para verificar se os PID foram revogados pelo respetivo fornecedor, a fim de obter sempre um resultado positivo.	Manipulação de dados (R7)
TR47	Um atacante pode contornar ou subverter o desempenho dos controlos realizados pela carteira para verificar se o (Q)EAA foi revogado pelo respetivo fornecedor, a fim de obter sempre um resultado positivo.	Manipulação de dados (R7)
TR48	Um atacante pode alterar os conteúdos dos dados de cópias de segurança e de recuperação que deveriam estar exclusivamente sob o controlo do utente.	Manipulação de dados (R7)/Perda de dados (R8)
TR49	Um atacante pode alterar o histórico de transações de uma determinada instância de carteira a partir dos registos de atividades.	Manipulação de dados (R7)/Perda de dados (R8)
TR50	Um atacante pode espiar a ligação entre a carteira e os utilizadores.	Roubo de dados (R5)/Divulgação de dados (R6)
TR51	Um atacante pode convencer um utente a partilhar dados pessoais (ou seja, PID, EAA, pseudónimos, assinaturas eletrónicas, registos e outros dados) consigo ou com um terceiro, quando esse utente não pretendia fazê-lo.	Roubo de dados (R5)/Divulgação de dados (R6)
TR52	Um atacante pode ler o histórico de transações de uma determinada instância de carteira a partir dos registos de atividades.	Roubo de dados (R5)/Divulgação de dados (R6)
TR53	Um atacante pode exportar ou extrair material de chave criptográfica do WSCD.	Roubo de dados (R5)/Divulgação de dados (R6)/Transação não autorizada (R9)
TR54	Um atacante pode ler os conteúdos dos dados de cópias de segurança e de recuperação que deveriam estar exclusivamente sob o controlo do utente.	Roubo de dados (R5)/Divulgação de dados (R6)
TR55	Um atacante pode contornar o método de autenticação do utente para utilizar um pseudónimo gerado por uma unidade de carteira.	Usurpação de identidade (R4)
TR56	Um atacante pode propor aos utentes uma aplicação que imite uma carteira legítima específica.	Usurpação de identidade (R4)
TR57	Um atacante pode exportar dados de carteiras, incluindo PID, (Q)EAA ou registos.	Usurpação de identidade (R4)
TR58	Um atacante pode exportar material de vinculação criptográfica.	Usurpação de identidade (R4)
TR59	Um atacante pode usurpar identidades através das chaves criptográficas da carteira.	Usurpação de identidade (R4)
TR60	Um atacante pode duplicar a unidade da carteira pessoal de outro utente no seu próprio dispositivo e utilizá-la.	Usurpação de identidade (R4)/Criação ou utilização de uma identidade eletrónica existente (R1)

IDENTIFICAÇÃO *Identificador*	Descrição da ameaça *Descrição da ameaça identificada* (*)	Título do risco *Riscos relacionados*
TR61	As autoridades de outro Estado podem solicitar ao utente que mostre e/ou partilhe todos os dados da carteira numa situação de proximidade, nomeadamente ao atravessar a fronteira desse Estado.	Usurpação de identidade (R4)/Vigilância (R14)
TR62	Um utente não consegue transferir os seus registos de transações após a falha de um dispositivo seu, o que resulta numa perda da rastreabilidade de transações anteriores na nova carteira.	Repúdio (R11)
TR63	Um utente não consegue recuperar os seus registos de transações após a falha de um dispositivo seu, o que resulta numa perda da rastreabilidade na nova carteira.	Repúdio (R11)
TR64	Os utilizadores podem ter dificuldades em provar o consentimento para assinaturas eletrónicas à distância.	Repúdio (R11)
TR65	Um atacante pode inundar a(s) ligação(ões) com pedidos durante a ligação aos utilizadores.	Perturbação do serviço (R13)
TR66	Um atacante pode inundar um serviço de aprovisionamento de estados com ligações a utilizadores.	Perturbação do serviço (R13)
TR67	Um atacante pode fazer com que a apresentação de atributos apareça como contestada/recusada, apesar de a apresentação de atributos indicar a sua validade.	Perturbação do serviço (R13)
TR68	Um atacante pode revogar PID sem motivo justificado.	Perturbação do serviço (R13)
TR69	Um atacante pode revogar PID sem o consentimento do utente.	Perturbação do serviço (R13)
TR70	Um atacante pode revogar um (Q)EAA sem motivo justificado.	Perturbação do serviço (R13)
TR71	Um atacante pode revogar um (Q)EAA sem o consentimento do utente.	Perturbação do serviço (R13)
TR72	Um atacante pode desencadear vários pedidos de identificação sem que estes sejam reconhecidos como pedidos órfãos intencionais.	Perturbação do serviço (R13)
TR73	Um atacante pode enviar vários pedidos sem qualquer transação de seguimento.	Perturbação do serviço (R13)
TR74	Um atacante pode permitir que um utilizador solicite a identificação sem uma correspondência entre a identificação (resposta) e o controlo total.	Perturbação do serviço (R13)
TR75	Um atacante pode enviar uma resposta a um pedido após o seu tempo-limite, ou situações semelhantes que conduzam a uma perturbação do serviço.	Perturbação do serviço (R13)
TR76	Um utilizador pode enviar vários pedidos inválidos.	Perturbação do serviço (R13)
TR77	Um atacante pode enviar vários pedidos inválidos a um fornecedor de carteiras.	Perturbação do serviço (R13)
TR78	Um atacante pode fazer com que um Estado-Membro seja incapaz de revogar um fornecedor de PID que não é de confiança da lista de confiança de fornecedores de PID.	Perturbação do serviço (R13)
TR79	Um atacante pode impedir a suspensão ou revogação de uma carteira.	Perturbação do serviço (R13)

IDENTIFICAÇÃO *Identificador*	Descrição da ameaça *Descrição da ameaça identificada (*)*	Título do risco *Riscos relacionados*
TR80	Um atacante pode bloquear transações realizadas por utilizadores, utentes e/ou pelo fornecedor de PID.	Perturbação do serviço (R13)
TR81	Um atacante pode desativar um WSCD ou torná-lo indisponível.	Perturbação do serviço (R13)
TR82	Um atacante pode impedir o fornecedor de PID de revogar ou suspender os PID.	Perturbação do serviço (R13)/Transação não autorizada (R9)
TR83	Um utilizador pode inferir dados de identificação do utente para além dos dados que foram partilhados consigo.	Vigilância (R14)
TR84	Um grupo de utilizadores ou fornecedores de PID em conivência pode inferir dados de identidade do utente para além dos dados de que tenha conhecimento.	Vigilância (R14)
TR85	Um atacante pode monitorizar e rastrear um utente utilizando os dados de identificação pessoal do utente num caso em que identificação deste não é necessária.	Vigilância (R14)
TR86	Um atacante pode combinar uma apresentação «falsificada» de combinações de (Q)EAA.	Manipulação da transação (R10)
TR87	Um atacante pode ativar/assumir o comando da carteira à distância (por exemplo, uma aplicação bancária que incorpora um pedido de autenticação ou de certificação) sem o consentimento explícito ou o controlo exclusivo do utente, em situações em que o utente não tem conhecimento (por exemplo, latência) ou não consegue ver o utilizador.	Manipulação da transação (R10)
TR88	Os atacantes podem alterar os metadados de um pedido (nome do serviço, utilizações, etc.).	Manipulação da transação (R10)
TR89	Os atacantes podem alterar as informações da resposta (estado do serviço, valor aleatório, etc.).	Manipulação da transação (R10)
TR90	Os atacantes podem alterar as informações dos atributos de um pedido (solicitações em excesso, etc.).	Manipulação da transação (R10)
TR91	Um utilizador pode reproduzir elementos de uma sessão anterior noutra sessão.	Manipulação da transação (R10)
TR92	Um atacante pode substituir ou alterar PID durante a respetiva transferência do fornecedor de PID para a unidade de carteira.	Manipulação da transação (R10)
TR93	Um atacante pode substituir ou alterar PID durante a respetiva transferência da unidade de carteira para o utilizador em linha.	Manipulação da transação (R10)
TR94	Um atacante pode substituir ou alterar PID durante a respetiva transferência da unidade de carteira para o utilizador fora de linha.	Manipulação da transação (R10)
TR95	Um atacante pode emitir PID sem o consentimento do utente.	Transação não autorizada (R9)
TR96	Um atacante pode utilizar políticas de divulgação incorporadas revogadas ou inválidas, possivelmente sem o conhecimento dos utilizadores.	Transação não autorizada (R9)
TR97	Um atacante pode induzir enganosamente a carteira a verificar assinaturas eletrónicas erradas.	Transação não autorizada (R9)
TR98	Um atacante pode utilizar a carteira fora do controlo do utente.	Transação não autorizada (R9)

IDENTIFI-CAÇÃO *Identificador*	Descrição da ameaça *Descrição da ameaça identificada (*)*	Título do risco *Riscos relacionados*
TR99	Um atacante pode convencer um utente a autenticar e aprovar transações com um atacante ou um terceiro não autorizado.	Transação não autorizada (R9)
TR100	Um atacante pode fazer com que um utente assine por via eletrónica, sem apresentar os conteúdos ao utente ou após apresentar conteúdos incorretos.	Transação não autorizada (R9)
TR101	Um atacante pode contornar o controlo do acesso da conta do utente junto do fornecedor de carteiras.	Transação não autorizada (R9)
TR102	Um atacante pode assumir a identidade de utilizadores durante a ligação aos mesmos.	Transação não autorizada (R9)/Divulgação de dados (R6)
TR103	O utente por detrás da ligação entre o utilizador e o navegador pode ser diferente do utente por detrás da ligação entre o utilizador e a carteira.	Transação não autorizada (R9)/Divulgação de dados (R6)/Usurpação de identidade (R4)
TR104	Um atacante pode convencer o utente a revogar a sua carteira sem motivo.	Transação não autorizada (R9)/Perturbação do serviço (R13)
TR105	Um atacante pode realizar ataques por interposição.	Transação não autorizada (R9)/Divulgação de dados (R6)/Vigilância (R14)
TR106	Um atacante pode apresentar atributos inválidos ou revogados de uma carteira que não se liga periodicamente à rede.	Efeito em vários riscos
TR107	Um atacante pode roubar informações de um utente por meio da mistificação da identidade de uma carteira.	Efeito em vários riscos
TR108	Um atacante pode assumir a identidade do utente reproduzindo/imitando um pedido de dados (por exemplo, autenticação), que apareceria como válido.	Efeito em vários riscos
TR109	Um atacante pode reproduzir uma política de divulgação incorporada em relação a um utente, a fim de imitar um pedido aprovado.	Efeito em vários riscos
TR110	Um atacante pode explorar a falta de informação dos utentes das carteiras, ou atrasos indevidos, após uma violação ou comprometimento da segurança.	Efeito em vários riscos
TR111	Um atacante pode alterar uma instância de carteira legítima anteriormente instalada, a fim de aditar funcionalidades maliciosas.	Efeito em vários riscos
TR112	Um atacante pode alterar uma instância de carteira legítima e propô-la aos utentes como legítima.	Efeito em vários riscos
TR113	Um atacante pode invalidar o próprio mecanismo de autenticação do utente para contornar a autenticação do utente da carteira.	Efeito em vários riscos
TR114	Um atacante pode introduzir códigos maliciosos ou portas traseiras («backdoors») no código da carteira durante a sua implantação no dispositivo do utente.	Efeito em vários riscos
TR115	Um atacante pode introduzir códigos maliciosos ou portas traseiras no código da carteira durante o seu desenvolvimento.	Efeito em vários riscos
TR116	Um atacante pode manipular a geração de números aleatórios, a fim de reduzir suficientemente a sua entropia para permitir ataques.	Efeito em vários riscos

IDENTIFICAÇÃO *Identificador*	Descrição da ameaça *Descrição da ameaça identificada* (*)	Título do risco *Riscos relacionados*
TR117	Um atacante pode manipular dispositivos dos utentes na cadeia de abastecimento, a fim de incluir códigos ou configurações que não cumpram as condições de utilização da carteira.	Efeito em vários riscos
TR118	Um atacante pode ativar uma unidade de carteira utilizando um WSCD que foi objeto de mistificação da identidade e que controla.	Efeito em vários riscos
TR119	Um atacante pode ler informações enviadas à WSCA e/ou ao WSCD.	Efeito em vários riscos
TR120	Um atacante pode enviar informações arbitrárias à WSCA.	Efeito em vários riscos
TR121	Um atacante pode roubar informações intercetando os intercâmbios entre a WSCA e o WSCD.	Efeito em vários riscos
TR122	Um atacante pode enviar informações arbitrárias ao WSCD.	Efeito em vários riscos
TR123	Um atacante pode enviar informações ao WSCD, contornando a WSCA.	Efeito em vários riscos
TR124	Um atacante pode recorrer a mistificação da interface para encaminhar os utentes para uma carteira e uma aplicação Web de gestão de PID falsas.	Efeito em vários riscos
TR125	Um atacante pode substituir as chaves de uma carteira por outras chaves para criar mensagens a utilizar noutro ataque.	Efeito em vários riscos
TR126	Um atacante pode alterar ou destruir as chaves de uma carteira, tornando inutilizáveis algumas funções da carteira.	Efeito em vários riscos
TR127	Um atacante pode controlar um *software* malicioso para aceder aos dados armazenados na carteira.	Efeito em vários riscos
TR128	Um atacante pode aceder a elementos de prova gerados na carteira.	Efeito em vários riscos
TR129	Os fornecedores de carteiras podem aceder a objetos na carteira.	Efeito em vários riscos
TR130	Os fornecedores de carteiras podem aceder a elementos de prova gerados na carteira.	Efeito em vários riscos
TR131	Um atacante pode roubar um dispositivo de carteira desbloqueado.	Efeito em vários riscos
TR132	Um atacante pode manipular o sistema para impedir que determinados eventos sejam registados.	Efeito em vários riscos
TR133	Um atacante pode intercetar a comunicação entre a instância de carteira e a WSCA ou reproduzir/imitar um utente (por exemplo, desviando o mecanismo de autenticação).	Efeito em vários riscos

ANEXO II

CRITÉRIOS PARA AVALIAR A ACEITABILIDADE DAS INFORMAÇÕES SOBRE A GARANTIA

Nome	Objeto	Aspetos a ter em atenção
EUCC	Produtos TIC	Sobre o emitente: nenhum (organismos de certificação acreditados) Sobre o âmbito: — verificar o perfil de proteção e a meta de segurança, — verificar o nível de garantia da avaliação e os aumentos. Sobre a garantia: — verificar as restrições na documentação do utente, — para a composição, pode exigir o acesso ao relatório técnico de avaliação.
EUCS (quando disponível)	Serviços de computação em nuvem	Sobre o emitente: nenhum (organismos de certificação acreditados) Sobre o âmbito: — verificar a descrição do serviço de computação em nuvem, — verificar o nível de avaliação e os perfis de extensão. Sobre a garantia: — verificar as informações relativas à transparência e, se necessário, as informações sobre a composição.
Sistemas de Critérios Comuns utilizados na UE, incluindo sistemas SOG-IS	Produtos TIC	Sobre o emitente: nenhum (Estados-Membros) Sobre o âmbito: — verificar o perfil de proteção e a meta de segurança, — verificar o nível de garantia da avaliação e os aumentos. Sobre a garantia: — verificar as restrições na documentação do utente, — para a composição, pode exigir o acesso ao relatório técnico de avaliação.
EN 17640:2018 (FITCEM, incluindo CSPN, BSZ, LINCE, BSZA)	Produtos TIC	Sobre o emitente: — verificar o sistema e os requisitos aplicáveis aos organismos de certificação. Sobre o âmbito: — verificar a descrição do produto, — verificar as declarações de segurança, — verificar o nível de garantia. Sobre a garantia: — verificar as atividades realizadas e as conclusões do relatório.
Sistemas de certificação de dispositivos qualificados de criação de assinaturas, em conformidade com o artigo 30.º do Regulamento (UE) n.º 910/2014	QSCD	Sobre o emitente: — verificar o sistema e os requisitos aplicáveis aos organismos de certificação. Sobre o âmbito: — verificar a descrição do produto, — verificar as declarações de segurança, — verificar o nível de garantia. Sobre a garantia: — verificar as atividades realizadas.

Nome	Objeto	Aspetos a ter em atenção
EN ISO/IEC 27001:2022	SGSI	Sobre o emitente: nenhum (organismos de certificação acreditados) Sobre o âmbito: — verificar a descrição do sistema de gestão, — verificar a declaração de aplicabilidade. Sobre a garantia: — verificar as atividades realizadas.
SOC2	Organizações	Sobre o emitente: — verificar o respetivo estatuto de revisor oficial de contas. Sobre o âmbito: — verificar a declaração de gestão e a descrição dos controlos, — verificar a declaração de aplicabilidade. Sobre a garantia: — verificar as conclusões do relatório, — verificar as cartas de transição, se necessário.
MDSCert (GSMA) (quando disponível)	Dispositivos móveis	Sobre o emitente: — verificar os requisitos aplicáveis aos organismos de certificação. Sobre o âmbito: — verificar o nível de garantia de segurança, — verificar os requisitos do sistema. Sobre a garantia: — verificar as atividades e as conclusões do relatório.
Outros sistemas	Qualquer componente	Sobre o sistema: — verificar a pertinência e as disposições do sistema. Sobre o emitente: — verificar os requisitos aplicáveis aos organismos de certificação. Sobre o âmbito: — verificar os requisitos do sistema, — verificar a meta de segurança ou documento semelhante que descreva os requisitos funcionais e de garantia de segurança, — verificar a descrição do produto e os requisitos funcionais de segurança selecionados. Sobre a garantia: — verificar as atividades e as conclusões do relatório.

ANEXO III

REQUISITOS FUNCIONAIS PARA SOLUÇÕES DE CARTEIRAS

Nos termos do artigo 5.º-A, n.ºs 4, 5, 8 e 14, do Regulamento (UE) n.º 910/2014, os critérios funcionais que uma solução de carteira certificada e que o sistema de identificação eletrónica ao abrigo do qual é disponibilizada têm de cumprir devem incluir os requisitos funcionais para as operações enumeradas nos seguintes regulamentos:

(1) Regulamento de Execução (UE) 2024/2979 da Comissão ([1]) que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante à integridade e às funcionalidades essenciais;

(2) Regulamento de Execução (UE) 2024/2982 da Comissão ([2]) que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante aos protocolos e às interfaces que devem ser suportados pelo Regime Europeu para a Identidade Digital;

(3) Regulamento de Execução (UE) 2024/2977 da Comissão ([3]) que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante aos dados de identificação pessoal e aos certificados eletrónicos de atributos emitidos para carteiras europeias de identidade digital.

([1]) Regulamento de Execução (UE) 2024/2979 da Comissão, de 28 de novembro de 2024, que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante à integridade e às funcionalidades essenciais (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Regulamento de Execução (UE) 2024/2982 da Comissão, de 28 de novembro de 2024, que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante aos protocolos e às interfaces que devem ser suportados pelo Regime Europeu para a Identidade Digital (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Regulamento de Execução (UE) 2024/2977, de 28 de novembro de 2024, da Comissão que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante aos dados de identificação pessoal e aos certificados eletrónicos de atributos emitidos para carteiras europeias de identidade digital (JO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

ANEXO IV

MÉTODOS E PROCEDIMENTOS PARA AS ATIVIDADES DE AVALIAÇÃO

1. **Auditoria da implementação de uma solução de carteira**

As atividades de avaliação da conformidade devem consistir na seleção de atividades de avaliação específicas.

Os sistemas nacionais de certificação devem especificar uma atividade de avaliação para avaliar as informações facultadas, abrangendo, pelo menos, o seguinte:

a) Uma análise das informações facultadas, a fim de confirmar a sua adequação para uma das arquiteturas especificadas nos sistemas nacionais de certificação;

b) Uma análise da cobertura dos riscos e ameaças de cibersegurança identificados no registo de riscos do anexo I pelos controlos de segurança descritos.

A análise referida nas alíneas a) e b) deve basear-se na fundamentação e na justificação apresentadas pelo fornecedor de carteiras.

2. **Atividades de avaliação relacionadas com o dispositivo criptográfico seguro de carteiras**

(1) As operações críticas, incluindo cálculos criptográficos, não têm de ser totalmente aplicadas no WSCD. No entanto, a parte aplicada no WSCD, quando funciona como parte da solução de carteira, deve garantir a proteção das operações críticas que realiza contra ataques de elevado potencial, em conformidade com o Regulamento de Execução (UE) 2015/1502 da Comissão ([1]).

(2) O WSCD, ou parte do mesmo, pode ser objeto de certificação, caso seja fornecido pelo titular ou pelo requerente do certificado, ou estar fora do seu âmbito, caso esteja incorporado num dispositivo fornecido pelo utilizador final. Além disso, os sistemas nacionais de certificação devem especificar as atividades de avaliação para verificar a adequação do WSCD, nos dois casos seguintes:

   a) Se a WSCA depender do WSCD específico (ou seja, se tiver de ser avaliada como um produto composto com base no WSCD), a avaliação da WSCA deve exigir o acesso a informações adicionais relacionadas com a certificação do WSCD, incluindo, em especial, o seu relatório técnico de avaliação;

   b) Se uma arquitetura tida em consideração no sistema utilizar vários WSCD, ou se algumas das operações relativas a ativos críticos forem realizadas fora do WSCD, os sistemas nacionais de certificação devem incluir atividades de avaliação para assegurar que a solução global proporciona o nível de segurança previsto.

(3) Como pré-requisito para a certificação ao abrigo dos sistemas nacionais de certificação, o WSCD deve ser avaliado em função dos requisitos de nível de garantia elevado estabelecidos no Regulamento de Execução (UE) 2015/1502.

   a) Quando estiverem preenchidas as condições previstas no artigo 3.º, n.º 3, alínea b), a avaliação do WSCD, ou de parte do mesmo, deve incluir uma avaliação da vulnerabilidade, conforme estabelecido na norma EN ISO/IEC 15408-3:2022, ao nível AVA_VAN.5, nos termos do anexo I do Regulamento de Execução (UE) 2024/482 da Comissão ([2]), a menos que seja devidamente justificado ao organismo de certificação que as características de segurança da WSCA permitem utilizar um nível de avaliação inferior, mantendo simultaneamente o mesmo nível de garantia global elevado que o estabelecido no Regulamento de Execução (UE) 2015/1502.

([1]) Regulamento de Execução (UE) 2015/1502 da Comissão, de 8 de setembro de 2015, que estabelece as especificações técnicas mínimas e os procedimentos para a atribuição dos níveis de garantia dos meios de identificação eletrónica, nos termos do artigo 8.º, n.º 3, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno (JO L 235 de 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/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).

(4) Além disso, na documentação relativa a cada arquitetura específica, os sistemas nacionais de certificação devem formular pressupostos para esta avaliação do WSCD, ao abrigo dos quais seja possível resistir a ataques de elevado potencial, nos termos do Regulamento de Execução (UE) 2015/1502, e especificar as atividades de avaliação para confirmar esses pressupostos, bem como para confirmar, após a emissão do certificado, que os pressupostos continuam a ser verificados. Os sistemas nacionais devem também exigir que os candidatos à certificação aperfeiçoem estes pressupostos para a sua aplicação específica e descrevam as medidas adotadas para garantir que os pressupostos são verificados ao longo do ciclo de vida da certificação.

(5) Em todos os casos, os sistemas nacionais de certificação devem incluir uma atividade de avaliação para verificar se as informações sobre a garantia disponíveis para o WSCD são adequadas para efeitos da solução de carteira, através de uma análise dessas informações, como a meta de segurança para os certificados EUCC, incluindo as seguintes atividades:

a) Verificar se o âmbito da avaliação é adequado, o que, no caso dos certificados EUCC, significa, por exemplo, verificar se a meta de segurança declarada é conforme com um dos perfis de proteção recomendados no EUCC;

b) Verificar se os pressupostos sobre o ambiente operacional são compatíveis com a solução de carteira, o que, no caso dos certificados EUCC, por exemplo, significa que estes pressupostos estão contemplados na meta de segurança;

c) Verificar se as recomendações constantes das orientações ou documentação para os utentes são compatíveis com as condições em que o WSCD deve ser utilizado na solução de carteira;

d) Verificar se os pressupostos formulados no sistema nacional de certificação sobre os WSCD são verificados e abrangidos pelas informações sobre a garantia.

(6) Caso algumas das verificações não sejam totalmente conclusivas, os sistemas nacionais de certificação devem exigir que os organismos de certificação especifiquem requisitos de compensação para a aplicação criptográfica segura de carteiras (WSCA) baseada no WSCD, a incluir na avaliação da WSCA. Se tal não for possível, os sistemas nacionais de certificação devem considerar o WSCD como sendo inadequado, o que significa que não deve ser emitido um certificado de conformidade à solução de carteira.

3. **Atividades de avaliação relacionadas com a aplicação criptográfica segura de carteiras (WSCA)**

(1) Os sistemas nacionais de certificação devem exigir que uma WSCA, como parte de uma solução de carteira, seja avaliada em função dos requisitos de, pelo menos, um nível de garantia elevado, conforme estabelecido no Regulamento de Execução (UE) 2015/1502.

(2) Esta avaliação deve incluir uma avaliação da vulnerabilidade, conforme estabelecido na norma EN ISO/IEC 15408-3:2022, ao nível AVA_VAN.5, nos termos do anexo I do Regulamento de Execução (UE) 2024/482, a menos que seja devidamente justificado ao organismo de certificação que as características de segurança da WSCA permitem utilizar um nível de avaliação inferior, mantendo simultaneamente o mesmo nível de garantia global elevado que o estabelecido no Regulamento de Execução (UE) 2015/1502.

(3) Quando a WSCA não é disponibilizada pelo fornecedor de carteiras, os sistemas nacionais de certificação devem formular pressupostos para esta avaliação da WSCA, ao abrigo dos quais seja possível resistir a ataques de elevado potencial, nos termos do Regulamento de Execução (UE) 2015/1502, e especificar as atividades de avaliação para confirmar esses pressupostos, bem como para confirmar, após a emissão do certificado, que os pressupostos continuam a ser verificados. Os sistemas nacionais devem também exigir que os candidatos à certificação aperfeiçoem estes pressupostos para a sua implementação específica e descrevam as medidas adotadas para garantir que os pressupostos são verificados ao longo do ciclo de vida da certificação.

(4) Em todos os casos, os sistemas nacionais de certificação devem incluir uma atividade de avaliação para verificar se as informações sobre a garantia disponíveis para a WSCA são adequadas para efeitos da solução de carteira, através de uma análise dessas informações, como a meta de segurança para os certificados EUCC, incluindo as seguintes atividades:

a) Verificar se o âmbito da avaliação é adequado, o que, no caso dos certificados EUCC, significa, por exemplo, verificar se a meta de segurança declarada é conforme com um dos perfis de proteção recomendados no EUCC;

b) Verificar se os pressupostos sobre o ambiente operacional são compatíveis com a solução de carteira, o que, no caso dos certificados EUCC, por exemplo, significa que estes pressupostos estão contemplados na meta de segurança;

c) Verificar se as recomendações constantes das orientações ou documentação para os utentes são compatíveis com as condições em que a WSCA deve ser utilizada na solução de carteira;

d) Verificar se os pressupostos formulados no sistema nacional de certificação sobre as WSCA são verificados e abrangidos pelas informações sobre a garantia.

(5) Os sistemas nacionais de certificação devem exigir que a avaliação da WSCA abranja todos os controlos de segurança aplicados por esta WSCA.

4. **Atividades de avaliação relacionadas com o dispositivo do utilizador final**

Uma vez que o registo de riscos, conforme estabelecido no anexo I do presente regulamento, identifica riscos diretamente relacionados com a segurança do dispositivo do utilizador final, os sistemas nacionais de certificação devem especificar requisitos de segurança para os dispositivos do utilizador final. Todavia, dado que estes dispositivos são disponibilizados pelo utilizador final e não pelo fornecedor de carteiras, estes requisitos devem ser abrangidos por pressupostos.

Para cada pressuposto, a solução de carteira deve incluir um mecanismo para verificar, em cada unidade de carteira, se o dispositivo do utilizador final subjacente satisfaz o pressuposto. Esses mecanismos devem ser considerados controlos de segurança e abrangidos por atividades de avaliação, a fim de demonstrar a sua adequação e a sua eficácia ao nível de garantia adequado.

Apresentam-se a seguir dois exemplos:

a) O dispositivo de um utilizador final pode incluir um WSCD certificado, o que tem de ser demonstrado. Normalmente, tal seria feito com recurso a um mecanismo criptográfico para verificar a presença no WSCD certificado de um segredo criptográfico que só está disponível no WSCD certificado. Neste caso, esse segredo criptográfico deve ser considerado um ativo crítico e ser abrangido pela certificação do WSCD e/ou da WSCA;

b) Um requisito típico para os dispositivos dos utilizadores finais consistiria em terem de ser objeto de atualizações de segurança. Uma vez que este requisito está relacionado com a instância de carteira, o mecanismo utilizado para verificar a disponibilidade de atualizações de segurança só tem de ser abrangido por atividades de avaliação com um nível de garantia adequado para a instância de carteira, em especial porque é provável que seja integrado na instância de carteira.

5. **Atividades de avaliação relacionadas com a instância de carteira**

(1) A avaliação da instância de carteira deve ter em conta os dois principais desafios seguintes:

a) É provável que a instância de carteira exista num conjunto de variantes da mesma aplicação de base, sendo cada variante especializada para uma categoria específica de dispositivos de utilizadores finais;

b) É provável que as diferentes variantes da instância de carteira necessitem de atualizações frequentes para acompanhar o desenvolvimento da plataforma de segurança subjacente, por exemplo, caso sejam identificadas vulnerabilidades que exijam alterações das aplicações.

(2) A avaliação da instância de carteira deve ter em conta estes desafios específicos. Uma das consequências imediatas é que o quadro dos Critérios Comuns pode não ser adequado em todos os casos. Por conseguinte, devem ser ponderadas metodologias de avaliação alternativas, sempre que necessário. Os sistemas nacionais de certificação devem ponderar a utilização da metodologia constante da norma EN 17640:2018 para o seguinte:

a) Como parte do próprio sistema;

b) Através de sistemas nacionais baseados na metodologia;

c) Através de sistemas nacionais baseados em princípios semelhantes, mas criados antes do desenvolvimento da metodologia constante da norma EN 17640:2018.

(3) Além disso, uma vez que pode haver um valor acrescentado limitado na realização de uma avaliação específica completa de cada variante, os sistemas nacionais de certificação devem ponderar a especificação de critérios que permitam a amostragem, a fim de evitar a repetição de atividades de avaliação idênticas e de se centrar em atividades específicas de uma determinada variante. Os sistemas nacionais de certificação devem exigir que todos os organismos de certificação justifiquem o recurso à amostragem.

(4) Os sistemas nacionais de certificação devem incluir atualizações da instância de carteira no processo global de gestão das alterações especificado para a solução de carteira. Devem igualmente estabelecer regras sobre os procedimentos a executar pelo fornecedor de carteiras para cada atualização (por exemplo, análise do impacto das alterações nos controlos de segurança) e sobre as atividades de avaliação que o organismo de certificação deve realizar em relação a atualizações em condições especificadas (por exemplo, avaliar a eficácia operacional de um controlo de segurança modificado). O processo de gestão de alterações é um dos processos cuja eficácia operacional deve ser verificada anualmente, em conformidade com o artigo 18.º, n.º 3.

6. **Atividades de avaliação relacionadas com os serviços e processos utilizados para o fornecimento e o funcionamento da solução de carteira**

(1) Para a avaliação dos serviços e processos que desempenham um papel no fornecimento e no funcionamento da solução de carteira e no sistema de identificação eletrónica ao abrigo do qual é disponibilizada, a equipa de avaliação deve recolher elementos de prova através da realização de atividades de avaliação que podem incluir atividades de auditoria, inspeção, verificação e validação.

(2) O organismo de certificação deve confirmar a suficiência e adequação dos elementos de prova para fornecer garantias suficientes de que os serviços e processos cumprem os requisitos de certificação, verificando o seguinte:

a) A exatidão das informações apresentadas na descrição dos processos e serviços;

b) A adequação da conceção e dos controlos dos processos e serviços para o cumprimento dos critérios de avaliação;

c) A eficácia operacional de uma aplicação destes controlos durante um período especificado antes da avaliação.

(3) A exatidão da descrição e a eficácia operacional de uma aplicação de controlos podem ser consideradas objetivos da verificação, na aceção da norma ISO/IEC 17000:2020, das declarações correspondentes do fornecedor de carteiras (ou seja, confirmação da equidade dos acontecimentos já ocorridos ou dos resultados já obtidos), ao passo que a adequação da conceção e dos controlos dos serviços e processos para o cumprimento dos critérios de avaliação pode ser considerada um objetivo da validação, na aceção da norma ISO/IEC 17000:2020, da correspondente declaração pelo fornecedor de carteiras (ou seja, confirmação da plausibilidade relativamente a uma utilização futura prevista ou a um resultado previsto).

(4) Tendo em conta que uma solução de carteira não pode funcionar antes de ser certificada, não é possível confirmar a eficácia operacional com base no funcionamento efetivo da solução. Por conseguinte, deve ser confirmada com base em elementos de prova recolhidos durante os ensaios ou os projetos-piloto.

(5) Podem já existir sistemas nacionais de certificação para serviços e processos específicos, por exemplo, para a integração de utentes. Se for caso disso, os sistemas nacionais de certificação devem ter em conta a utilização desses sistemas.

7. **Atividades de avaliação relacionadas com os serviços de TIC utilizados para o fornecimento e o funcionamento da solução de carteira**

(1) Algumas arquiteturas de carteiras podem recorrer a serviços de TIC específicos, incluindo serviços de computação em nuvem para o fornecimento e o funcionamento de uma solução de carteira, e estes serviços podem alojar dados sensíveis, bem como operações sensíveis. Nesse caso, os sistemas nacionais de certificação devem especificar requisitos de segurança para estes serviços de TIC.

(2) Já existem muitos sistemas de certificação para serviços de TIC, serviços de computação em nuvem e outras fontes de informações sobre a garantia, incluindo os enumerados no anexo II. Os sistemas nacionais de certificação devem basear-se, quando disponíveis e aplicáveis, nos mecanismos existentes, através de um dos seguintes mecanismos:

a) Impor a utilização de um sistema específico ou de uma seleção de sistemas, especificando as condições em que os serviços de TIC ou de computação em nuvem devem ser avaliados através desses sistemas;

b) Deixar a escolha da avaliação ao fornecedor de carteiras e utilizar a atividade de análise da dependência para apreciar a adequação das informações sobre a garantia obtidas através dessas avaliações.

(3) Em ambos os casos, os sistemas nacionais de certificação devem especificar as atividades de avaliação adicionais necessárias para analisar ou complementar as informações obtidas através desses sistemas.

ANEXO V

LISTA DE INFORMAÇÕES PUBLICAMENTE DISPONÍVEIS SOBRE CARTEIRAS

1. As informações a divulgar ao público nos termos do artigo 8.º, n.º 5, devem incluir, pelo menos, o seguinte:
   a) Quaisquer limitações à utilização de uma solução de carteira;
   b) Orientações e recomendações do fornecedor de carteiras para ajudar os utilizadores finais na configuração, instalação, aplicação, funcionamento e manutenção seguros das carteiras;
   c) O período durante o qual é oferecido aos utilizadores finais apoio em matéria de segurança, em especial no que diz respeito à disponibilidade de atualizações relacionadas com a cibersegurança;
   d) Os contactos do fabricante, do prestador ou do fornecedor e os métodos aceites para receber informações sobre vulnerabilidades comunicadas pelos utilizadores finais ou pelos investigadores em matéria de segurança;
   e) Uma referência aos repositórios em linha que enumeram vulnerabilidades divulgadas publicamente relacionadas com carteiras e a quaisquer recomendações pertinentes em matéria de cibersegurança.

2. As informações a que se refere o n.º 1 devem ser disponibilizadas de forma clara, exaustiva e facilmente acessível, num espaço acessível ao público, a qualquer pessoa que pretenda utilizar uma solução de carteira.

ANEXO VI

METODOLOGIA PARA AVALIAR A ACEITABILIDADE DAS INFORMAÇÕES SOBRE A GARANTIA

1. **Avaliação da disponibilidade da documentação de garantia**

Os avaliadores devem enumerar a documentação de garantia disponível para cada componente pertinente da solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada. Em seguida, os avaliadores devem avaliar a relevância global de cada documento de garantia para a análise da dependência.

Na análise, deve ter-se em conta os seguintes aspetos:

(1) A própria documentação de garantia:

a) O tipo de documentação de garantia, com todos os pormenores exigidos

(exemplos desses documentos são os certificados de conformidade de acordo com a norma EN ISO/IEC 27001:2022 ou tipo 1 ou tipo 2 para os relatórios ISAE);

b) O período abrangido ou o período de validade

[este período pode ser complementado com uma carta de transição (um documento que abranja o período entre a data do termo do período de referência do atual relatório ISAE e a publicação de um novo relatório ISAE) ou uma declaração semelhante];

c) O quadro aplicável (por exemplo, a norma existente);

d) Se a documentação de garantia inclui um levantamento dos requisitos do sistema.

(2) A competência profissional e a imparcialidade do emitente do relatório de garantia:

a) Nome do organismo de certificação e, se disponível, nome do avaliador principal;

b) Comprovativos da competência do organismo de certificação e do avaliador (por exemplo, acreditação, certificação pessoal, etc.);

c) Comprovativos da imparcialidade do organismo de certificação e do avaliador (por exemplo, acreditação, etc.).

2. **Avaliação da garantia relativa a requisitos individuais**

Os avaliadores devem verificar se a documentação de garantia disponível para a solução de carteira e o sistema de identificação eletrónica ao abrigo do qual é disponibilizada é adequada para determinar que a solução de carteira satisfaz as expectativas em relação aos requisitos individuais do sistema de certificação.

Esta avaliação deve ser efetuada para cada componente pertinente da solução de carteira e para o sistema de identificação eletrónica ao abrigo do qual é disponibilizada, formulando um pressuposto sobre os controlos de segurança da solução de carteira.

Para cada um desses pressupostos, a equipa de avaliação deve determinar se a garantia facultada na documentação de garantia disponível é ou não adequada.

A determinação da adequação da garantia deve basear-se nos seguintes elementos:

(1) As informações exigidas estão disponíveis, com o nível de garantia esperado, na documentação de garantia;

(2) As informações disponíveis na documentação de garantia não abrangem todo o âmbito do requisito, mas os controlos adicionais ou os controlos compensatórios (ou seja, os controlos internos que reduzem o risco de deficiências de controlo existentes ou potenciais) aplicados na solução da carteira ou no sistema de identificação eletrónica ao abrigo do qual é disponibilizada permitem aos avaliadores determinar que as informações são adequadas;

(3) As informações disponíveis na documentação de garantia não oferecem o nível de garantia esperado, mas os controlos aplicados para avaliar e monitorizar o fornecedor de carteiras permitem aos avaliadores determinar que as informações são adequadas;

(4) Caso a documentação de garantia mencione não conformidades na conceção ou aplicação dos controlos utilizados para cumprir um pressuposto, as medidas corretivas propostas e aplicadas pelo fornecedor de carteiras e analisadas pelos seus avaliadores devem ser adequadas para garantir que o pressuposto é efetivamente cumprido.

ANEXO VII

CONTEÚDO DO CERTIFICADO DE CONFORMIDADE

1. Um identificador único atribuído pelo organismo de certificação que emite o certificado de conformidade.

2. Informações relacionadas com a solução de carteira certificada e os sistemas de identificação eletrónica ao abrigo dos quais é disponibilizada, bem como sobre o titular do certificado de conformidade, incluindo os seguintes elementos:
   a) Nome da solução de carteira:
   b) nome dos sistemas de identificação eletrónica ao abrigo dos quais a solução de carteira é disponibilizada,
   c) versão da solução de carteira que foi avaliada,
   d) nome, endereço e dados de contacto do titular do certificado de conformidade,
   e) hiperligação para o sítio Web do titular do certificado de conformidade que contém as informações que devem ser disponibilizadas ao público.

3. Informações relacionadas com a avaliação e certificação da solução de carteira e dos sistemas de identificação eletrónica ao abrigo dos quais é disponibilizada, incluindo os seguintes elementos:
   a) Nome, endereço e dados de contacto do organismo de certificação que emitiu o certificado de conformidade;
   b) Se diferente do organismo de certificação, nome do organismo de avaliação da conformidade que efetuou a avaliação, juntamente com informações sobre a sua acreditação;
   c) Nome do proprietário do sistema;
   d) Referências ao Regulamento (UE) n.º 910/2014 e ao presente regulamento;
   e) Uma referência ao relatório de certificação associado ao certificado de conformidade;
   f) Uma referência ao relatório de avaliação da certificação associado ao certificado de conformidade;
   g) Uma referência às normas utilizadas para a avaliação, incluindo as respetivas versões;
   h) A data de emissão do certificado de conformidade;
   i) O período de validade do certificado de conformidade.

ANEXO VIII

CONTEÚDO DO RELATÓRIO PÚBLICO DE CERTIFICAÇÃO E DO RELATÓRIO DE AVALIAÇÃO DA CERTIFICAÇÃO

1. O relatório público de certificação deve conter, pelo menos, os seguintes elementos:

   a) Síntese;

   b) Identificação da solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada;

   c) Uma descrição da solução de carteira e do sistema de identificação eletrónica ao abrigo do qual é disponibilizada;

   d) As informações de segurança a disponibilizar ao público, conforme descrito no anexo V, ou uma referência a essas informações;

   e) Um resumo do plano preliminar de auditoria e validação;

   f) Um resumo da revisão e da decisão de certificação.

2. O relatório de avaliação da certificação deve conter, pelo menos:

   a) Uma descrição da conceção da solução de carteira, do sistema de identificação e do processo de integração, juntamente com a avaliação de riscos e o plano de validação específico;

   b) Uma descrição da forma como a solução de carteira cumpre os requisitos de nível de garantia elevado e da forma como tal é demonstrado pelos resultados da avaliação da certificação da solução de carteira realizada em conformidade com o presente regulamento;

   c) Uma descrição do resultado da avaliação da conformidade da solução de carteira e do sistema de identificação eletrónica ao abrigo do qual as unidades de carteira correspondentes são disponibilizadas, em especial a conformidade com o seguinte:

      — os requisitos estabelecidos no artigo 5.º-A, n.ºs 4, 5 e 8, do Regulamento (UE) n.º 910/2014,

      — o requisito de separação lógica estabelecido no artigo 5.º-A, n.º 14, do Regulamento (UE) n.º 910/2014,

      — se for caso disso, as normas e especificações técnicas a que se refere o artigo 5.º-A, n.º 24, do Regulamento (UE) n.º 910/2014, descrevendo simultaneamente a forma como esses requisitos se relacionam com os requisitos normativos correspondentes especificados pelos sistemas nacionais de certificação;

   d) Um resumo do resultado da execução do plano de validação, incluindo todas as não conformidades identificadas.

ANEXO IX

CALENDÁRIO DAS AVALIAÇÕES DE FISCALIZAÇÃO OBRIGATÓRIAS

1. O artigo 18.º especifica os requisitos para o ciclo de vida da certificação, em especial a realização de atividades de avaliação periódicas. Essas atividades devem incluir, pelo menos, o seguinte:

   a) Uma avaliação completa do objeto da avaliação da conformidade na avaliação inicial e em cada avaliação de recertificação, incluindo uma funcionalidade de atualização de qualquer componente do produto;

   b) Uma avaliação da vulnerabilidade na avaliação inicial e em cada avaliação de recertificação e, pelo menos, de dois em dois anos nas avaliações de fiscalização, que abranja, pelo menos, as alterações do objeto da avaliação da conformidade e as alterações do ambiente de ameaça desde a última avaliação da vulnerabilidade;

   c) Atividades adicionais, como testes de penetração em caso de aumento do nível de risco ou o surgimento de novas ameaças;

   d) Uma avaliação da eficácia operacional dos processos de manutenção, pelo menos todos os anos, nas avaliações de fiscalização e de recertificação, abrangendo, pelo menos, os processos de controlo das versões, atualização e gestão da vulnerabilidade;

   e) Na sequência de uma revisão e de uma decisão de certificação bem-sucedidas, a emissão de um certificado de conformidade após a avaliação inicial e após cada avaliação de recertificação.

2. O quadro 1 apresenta um calendário de referência baseado num ciclo de quatro anos, em que:

   a) O ano 1 tem início quando o certificado de conformidade é emitido pela primeira vez; e

   b) Todas as atividades de avaliação devem ser realizadas no prazo de 12 meses a contar da avaliação do ano anterior.

3. O calendário estabelecido no quadro 1 é uma recomendação para assegurar a recertificação atempada e evitar perturbações no fornecimento da solução de carteira. Podem ser possíveis outros calendários, desde que a validade do certificado de conformidade não exceda cinco anos, conforme previsto no artigo 5.º-C, n.º 4, do Regulamento (UE) n.º 910/2014.

4. Para além das avaliações regulares, pode ser desencadeada uma avaliação especial a pedido do organismo de certificação ou do titular do certificado de conformidade, na sequência de uma alteração significativa do objeto da certificação ou do ambiente de ameaça.

5. Qualquer avaliação, incluindo avaliações de fiscalização e avaliações especiais, pode conduzir à emissão de um novo certificado de conformidade, em especial em caso de alterações significativas do objeto da certificação, mas com o mesmo prazo de validade que o certificado de conformidade original.

Quadro 1

Um ciclo completo de avaliação de quatro anos

Calendário	Tipo de aval.	Atividades
Ano 0	Inicial	— Avaliação completa do objeto da certificação, incluindo a avaliação da vulnerabilidade — Incluindo uma funcionalidade para efetuar atualizações a cada componente de *software* — Avaliação dos processos de manutenção, excluindo a sua eficácia operacional — Emissão do certificado de conformidade e início do ciclo de quatro anos
Ano 1	Vigilância	— Avaliação da eficácia operacional dos processos de manutenção — Pelo menos, verificação da versão, atualização, gestão da vulnerabilidade — Avaliação das alterações com impacto na segurança do produto

Calendário	Tipo de aval.	Atividades
Ano 2	Vigilância	— Avaliação da vulnerabilidade da solução completa — Avaliação da eficácia operacional dos processos de manutenção — Pelo menos, controlo da versão, atualização, gestão da vulnerabilidade — Avaliação das alterações com impacto na segurança do produto
Ano 3	Vigilância	— Avaliação da eficácia operacional dos processos de manutenção — Pelo menos, verificação da versão, atualização, gestão da vulnerabilidade — Avaliação das alterações com impacto na segurança do produto
Ano 4	Recertificação	(1) Avaliação completa do objeto da certificação, incluindo a avaliação da vulnerabilidade (2) Avaliação simplificada de funcionalidades/processos que não se alteraram (3) Incluindo uma funcionalidade para efetuar atualizações a cada componente de *software* (4) Avaliação dos processos de manutenção, incluindo a sua eficácia operacional (5) Emissão de um novo certificado de conformidade