2024/2979

4.12.2024

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 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-A, n.º 23,

Considerando o seguinte:

(1) O Regime Europeu para a Identidade Digital, instituído pelo Regulamento (UE) n.º 910/2014, é uma componente crucial da criação de um ecossistema de identidade digital seguro e interoperável em toda a União. Tendo como pedra angular as carteiras europeias de identidade digital («carteiras»), o regime visa facilitar o acesso das pessoas singulares e coletivas aos serviços em todos os Estados-Membros, assegurando simultaneamente a proteção dos dados pessoais e da privacidade.

(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 a todas as atividades de tratamento de dados pessoais ao abrigo do presente regulamento.

(3) O artigo 5.º-A, n.º 23, do Regulamento (UE) n.º 910/2014 incumbe a Comissão, se necessário, de estabelecer as especificações e os procedimentos pertinentes. Tal é alcançado através de quatro regulamentos de execução, que abordam os protocolos e as interfaces [Regulamento de Execução (UE) 2024/2982 da Comissão ([4])], a integridade e as funcionalidades essenciais [Regulamento de Execução (UE) 2024/2979 da Comissão ([5])], os dados de identificação pessoal e os certificados eletrónicos de atributos [Regulamento de Execução (UE) 2024/2977 da Comissão ([6])], bem como as notificações à Comissão [Regulamento de Execução (UE) 2024/2980 da Comissão ([7])]. O presente regulamento estabelece os requisitos aplicáveis à integridade e às funcionalidades essenciais das carteiras europeias de identidade digital.

([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]) 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, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) 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 das carteiras europeias de identidade digital (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Regulamento de Execução (UE) 2024/2977 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 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).

([7]) Regulamento de Execução (UE) 2024/2980 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 às notificações à Comissão relativas ao ecossistema da carteira europeia de identidade digital (JO L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) 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 ([8]) e, em especial, na arquitetura e no quadro de referência. Em conformidade com o considerando 75 do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho ([9]), 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.

(5) A fim de assegurar uma comunicação precisa, uma diferenciação técnica e uma clara atribuição de responsabilidades, é necessário estabelecer a distinção entre diferentes componentes e configurações de carteiras. Deve entender-se por solução de carteira o sistema completo fornecido por um fornecedor de carteiras que é necessário para explorar uma carteira. Tal deve incluir os componentes de *software* e *hardware*, bem como os serviços, as definições e as configurações necessários para assegurar o bom funcionamento da mesma. Uma solução de carteira pode estar localizada nos dispositivos e ambientes dos utentes e na estrutura de retaguarda (*backend*) do fornecedor. Deve entender-se por unidade de carteira uma configuração específica da solução de carteira para um utente individual. Deve incluir a aplicação instalada no dispositivo ou ambiente de um utente da carteira com a qual este interage diretamente (a «instância de carteira») e as características de segurança necessárias para proteger os dados e as transações dos utentes. Estas características de segurança devem envolver *software* ou *hardware* especiais para cifrar e salvaguardar informações sensíveis. A instância de carteira deve fazer parte da unidade da carteira e permitir que o utente da carteira aceda às funcionalidades da mesma.

(6) São necessárias aplicações criptográficas seguras de carteiras, como componentes especiais separados dentro de uma unidade de carteira, não só para a proteção de ativos críticos, como chaves criptográficas privadas, mas também para a disponibilização de funcionalidades cruciais, como a apresentação de certificados eletrónicos de atributos. A utilização de especificações técnicas comuns pode facilitar o acesso dos fornecedores de carteiras digitais a elementos seguros incorporados. As aplicações criptográficas seguras de carteiras podem ser disponibilizadas de várias formas e para vários tipos de dispositivos criptográficos seguros de carteiras. Caso os fornecedores de carteiras disponibilizem aplicações criptográficas seguras de carteiras personalizadas sob a forma de *applets* Java Card para elementos seguros incorporados, devem seguir as normas enumeradas no anexo I ou especificações técnicas equivalentes.

(7) As unidades de carteira devem permitir que os fornecedores de dados de identificação pessoal ou de certificados eletrónicos de atributos verifiquem se estão a emitir esses dados ou certificados para unidades de carteira autênticas do utente da carteira.

(8) A fim de assegurar a proteção de dados desde a conceção e por defeito, as carteiras devem ser dotadas das técnicas avançadas de reforço da privacidade que estiverem disponíveis. Estas características devem prever a possibilidade de as carteiras poderem ser utilizadas sem que o utente da carteira possa ser rastreado entre diferentes utilizadores de carteiras, se aplicável no cenário de utilização. Por exemplo, os fornecedores de carteiras devem ponderar a adoção de medidas avançadas de proteção da privacidade em relação aos certificados de unidades de carteira, como a utilização de certificados de unidades de carteira efémeros ou a emissão por lotes. Além disso, as políticas de divulgação incorporadas devem alertar os utentes da carteira contra a divulgação inadequada ou ilegal de atributos dos certificados eletrónicos de atributos.

(9) Os certificados de unidades de carteira devem permitir aos utilizadores de carteiras que solicitem atributos às unidades de carteira verificar o estado de validade da unidade de carteira com que estão a comunicar, pois os certificados de unidades de carteira devem ser revogados quando uma unidade de carteira deixar de ser considerada válida. As informações relativas ao estado de validade das unidades de carteira devem ser disponibilizadas de forma interoperável, a fim de garantir que possam ser utilizadas por todos os utilizadores de carteiras. Além disso, nos casos em que os utentes das carteiras percam as suas unidades de carteira ou deixem de ter controlo sobre as mesmas, os fornecedores de carteiras devem permitir que solicitem a revogação das respetivas unidades de carteira. A fim de garantir a privacidade e a ausência de associação, os Estados-Membros devem também utilizar técnicas de preservação da privacidade para o certificado da unidade de carteira. Tal pode incluir a utilização de múltiplos certificados de unidade de carteira para diferentes fins, divulgando apenas as informações estritamente necessárias sobre a carteira para permitir uma transação, ou a limitação da vida útil do certificado de unidade de carteira como alternativa à utilização de identificadores de revogação.

([8]) JO L 210 de 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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).

(10) A fim de assegurar que todas as carteiras são tecnicamente capazes de receber e apresentar dados de identificação pessoal e certificados eletrónicos de atributos em cenários transfronteiriços sem prejudicar a interoperabilidade, as carteiras devem suportar tipos predeterminados de formatos de dados e a divulgação seletiva. Conforme estabelecido no Regulamento (UE) n.º 910/2014, a divulgação seletiva é um conceito que habilita o proprietário dos dados a divulgar apenas determinadas partes de um conjunto de dados mais vasto, a fim de que a entidade recetora obtenha apenas as informações necessárias à prestação de um serviço solicitado pelo utente. Uma vez que as carteiras devem permitir ao utente divulgar atributos seletivamente, as normas enumeradas no anexo II devem ser aplicadas de forma a permitir esta característica. Além disso, as carteiras podem suportar outros formatos e funcionalidades, de modo a facilitar casos de utilização específicos.

(11) O registo das transações é um instrumento importante para proporcionar transparência sobre como proporcionar uma panorâmica das transações ao utente da carteira. Além disso, os registos devem ser utilizados para permitir a partilha rápida e fácil de determinadas informações, a pedido do utente da carteira, com as autoridades de controlo competentes criadas nos termos do artigo 51.º do Regulamento (UE) 2016/679, em caso de comportamento suspeito dos utilizadores de carteiras.

(12) Para que o utente de uma carteira possa assinar eletronicamente, deve ser-lhe emitido um certificado qualificado, vinculado a um dispositivo qualificado de criação de assinaturas eletrónicas. O utente da carteira deve ter acesso a uma aplicação de criação de assinaturas. Embora a emissão de certificados qualificados seja um serviço de prestadores qualificados de serviços de confiança, os fornecedores de carteiras ou outras entidades devem poder disponibilizar os outros componentes. Por exemplo, os dispositivos qualificados de criação de assinaturas eletrónicas podem ser geridos por prestadores qualificados de serviços de confiança enquanto serviço ou podem estar localizados no dispositivo do utente da carteira, nomeadamente como um cartão inteligente. Do mesmo modo, as aplicações de criação de assinaturas podem ser integradas na instância de carteira, ser uma aplicação separada no dispositivo do utente da carteira ou ser disponibilizadas à distância.

(13) Os objetos de portabilidade e exportação de dados podem registar os dados de identificação pessoal e os certificados eletrónicos de atributos que foram emitidos para uma determinada unidade de carteira. Estes objetos permitem aos utentes das carteiras extrair os dados pertinentes da sua unidade de carteira, a fim de reforçar o seu direito à portabilidade dos dados. Incentivam-se os fornecedores de carteiras a utilizar as mesmas soluções técnicas para implementar igualmente processos de salvaguarda e recuperação destinados a unidades de carteira, permitindo recuperar unidades de carteira perdidas ou transferir informações de um fornecedor de carteiras para outro, se for caso disso e na medida em que tal possa ser feito sem prejudicar o direito à proteção de dados e a segurança do ecossistema da identidade digital.

(14) A geração de pseudónimos específicos dos utilizadores de carteiras deve permitir aos utentes das carteiras autenticarem-se sem facultar informações desnecessárias aos utilizadores de carteiras. Tal como estabelecido no Regulamento (UE) n.º 910/2014, os utentes das carteiras não devem ser impedidos de recorrer a serviços sob pseudónimo, sempre que não exista qualquer requisito jurídico de recorrer à identidade jurídica para fins de autenticação. Por conseguinte, as carteiras devem incluir uma funcionalidade para gerar pseudónimos escolhidos e geridos pelos utentes, que possibilite a sua autenticação quando acedem a serviços em linha. A aplicação das especificações estabelecidas no anexo V deve permitir estas funcionalidades em conformidade. Além disso, os utilizadores de carteiras não devem solicitar aos utentes que facultem quaisquer dados para além dos indicados no registo dos utilizadores para a utilização prevista das carteiras. Os utentes das carteiras devem poder verificar os dados de registo dos utilizadores a qualquer momento.

(15) Conforme estabelecido no Regulamento (UE) 2024/1183, os Estados-Membros não devem restringir, direta ou indiretamente, o acesso a serviços públicos ou privados a pessoas singulares ou coletivas que optem por não utilizar carteiras e devem disponibilizar soluções alternativas adequadas.

(16) 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 ([10]) e emitiu o seu parecer em 30 de setembro de 2024.

([10]) 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).

(17) As medidas previstas no presente regulamento estão em conformidade com o parecer do Comité referido no artigo 48.º 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 regras para a integridade e as funcionalidades essenciais das 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 da Comissão, em especial a arquitetura e o quadro de referência.

Artigo 2.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «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;

2) «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;

3) «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;

4) «Fornecedor de dados de identificação pessoal», uma pessoa singular ou coletiva responsável pela emissão e revogação dos dados de identificação pessoal e pela garantia de que os dados de identificação pessoal de um utente estão criptograficamente vinculados a uma unidade de carteira;

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

6) «Utilizador de carteira», um utilizador que tenciona recorrer a unidades de carteira para a prestação de serviços públicos ou privados por meio de interação digital;

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

8) «Certificado de unidade de carteira», um objeto de dados que descreve os componentes da unidade de carteira ou permite a autenticação e validação desses componentes;

9) «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;

10) «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;

11) «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;

12) «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;

13) «Operação criptográfica de carteira», um mecanismo criptográfico necessário no contexto da autenticação do utente da carteira e da emissão ou apresentação de dados de identificação pessoal ou certificados eletrónicos de atributos;

14) «Certificado de acesso de utilizador de carteira», um certificado de assinaturas ou selos eletrónicos que autenticam e validam o utilizador da carteira, emitido por um fornecedor de certificados de acesso de utilizadores de carteiras;

15) «Fornecedor de certificados de acesso de utilizadores de carteiras», uma pessoa singular ou coletiva mandatada por um Estado-Membro para emitir certificados de acesso de utilizadores de carteiras a utilizadores de carteiras registados nesse Estado-Membro.

CAPÍTULO II

INTEGRIDADE DAS CARTEIRAS EUROPEIAS DE IDENTIDADE DIGITAL

Artigo 3.º

Integridade da unidade de carteira

1. As unidades de carteira não devem executar qualquer das funcionalidades enumeradas no artigo 5.º-A, n.º 4, do Regulamento (UE) n.º 910/2014, exceto a autenticação do utente da carteira para aceder à unidade de carteira, até que a unidade de carteira tenha autenticado com êxito o utente da carteira.

2. Para cada unidade de carteira, os fornecedores de carteiras devem apor uma assinatura ou um selo em, pelo menos, um certificado de unidade de carteira em conformidade com os requisitos estabelecidos no artigo 6.º. O certificado utilizado para apor uma assinatura ou um selo no certificado de unidade de carteira deve ser emitido ao abrigo de um certificado enumerado na lista de confiança referida no Regulamento de Execução (UE) 2024/2980.

Artigo 4.º

Instâncias de carteiras

1. As instâncias de carteiras devem utilizar, pelo menos, um dispositivo criptográfico seguro de carteiras para gerir ativos críticos.

2. Os fornecedores de carteiras devem assegurar a integridade, a autenticidade e a confidencialidade da comunicação entre as instâncias de carteiras e as aplicações criptográficas seguras de carteiras.

3. Caso os ativos críticos estejam relacionados com a realização de uma identificação eletrónica com um nível de garantia elevado, as operações criptográficas de carteiras ou outras operações de tratamento de ativos críticos devem ser realizadas em conformidade com os requisitos relativos às características e à conceção dos meios de identificação eletrónica com nível de garantia elevado, conforme estabelecido no Regulamento de Execução (UE) 2015/1502 da Comissão ([11]).

Artigo 5.º

Aplicações criptográficas seguras de carteiras

1. Os fornecedores de carteiras devem assegurar que as aplicações criptográficas seguras de carteiras:

a) Realizam operações criptográficas de carteira que envolvam ativos críticos que não os necessários para que a unidade de carteira autentique o utente da carteira unicamente nos casos em que essas aplicações tenham autenticado com êxito os utentes das carteiras;

([11]) 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).

b) Caso autentiquem os utentes das carteiras no contexto da realização de uma identificação eletrónica com um nível de garantia elevado: realizam a autenticação dos utentes das carteiras, em conformidade com os requisitos relativos às características e à conceção dos meios de identificação eletrónica com um nível de garantia elevado, conforme estabelecido no Regulamento de Execução (UE) 2015/1502;

c) São capazes de gerar novas chaves criptográficas de forma segura;

d) São capazes de efetuar o apagamento seguro de ativos críticos;

e) São capazes de gerar uma prova da posse de chaves privadas;

f) Protegem as chaves privadas geradas por essas aplicações criptográficas seguras de carteiras durante a existência das chaves;

g) Cumprem os requisitos relativos às características e à conceção dos meios de identificação eletrónica com um nível de garantia elevado, conforme estabelecido no Regulamento de Execução (UE) 2015/1502;

h) São os únicos componentes capazes de executar operações criptográficas de carteiras e qualquer outra operação com ativos críticos no contexto da realização de uma identificação eletrónica com um nível de garantia elevado.

2. Sempre que os fornecedores de carteiras decidam disponibilizar uma aplicação criptográfica segura de carteiras para um elemento seguro incorporado, devem basear a sua solução técnica nas especificações técnicas enumeradas no anexo I ou noutras especificações técnicas equivalentes.

Artigo 6.º

Autenticidade e validade da unidade de carteira

1. Os fornecedores de carteiras devem assegurar que cada unidade de carteira contém certificados de unidades de carteira.

2. Os fornecedores de carteiras devem assegurar que os certificados de unidades de carteira a que se refere o n.º 1 contêm chaves públicas e que as chaves privadas correspondentes estão protegidas por um dispositivo criptográfico seguro de carteiras.

3. Os fornecedores de carteiras devem:

a) Informar os utentes das carteiras sobre os seus direitos e obrigações em relação à sua unidade de carteira;

b) Disponibilizar mecanismos, independentes das unidades de carteira, para a identificação e autenticação seguras dos utentes das carteiras;

c) Assegurar que os utentes das carteiras têm o direito de solicitar a revogação dos seus certificados de unidades de carteira, utilizando os mecanismos de autenticação referidos na alínea b).

Artigo 7.º

Revogação de certificados de unidades de carteira

1. Os fornecedores de carteiras são as únicas entidades capazes de revogar os certificados de unidades de carteira para unidades de carteira que disponibilizaram.

2. Os fornecedores de carteiras devem estabelecer uma política acessível ao público que especifique as condições e o prazo para a revogação dos certificados de unidades de carteira.

3. Caso os fornecedores de carteiras tenham revogado certificados de unidades de carteira, devem informar os utentes das carteiras afetados no prazo de 24 horas a contar da revogação das suas unidades de carteira, incluindo o motivo da revogação e as consequências para o utente da carteira. Estas informações devem ser facultadas de forma concisa, facilmente acessível e numa linguagem clara e simples.

4. Caso os fornecedores de carteiras tenham revogado certificados de unidades de carteira, devem disponibilizar ao público o estado de validade do certificado de unidade de carteira de uma forma que preserve a privacidade e descrever a localização dessas informações no certificado de unidade de carteira.

CAPÍTULO III

FUNCIONALIDADES E CARACTERÍSTICAS ESSENCIAIS DAS CARTEIRAS EUROPEIAS DE IDENTIDADE DIGITAL

Artigo 8.º

Formatos para dados de identificação pessoal e certificados eletrónicos de atributos

Os fornecedores de carteiras devem assegurar que as soluções de carteiras permitem a utilização de dados de identificação pessoal e de certificados eletrónicos de atributos emitidos em conformidade com a lista de normas estabelecida no anexo II.

Artigo 9.º

Registos de transações

1. Independentemente de uma transação ser ou não concluída com êxito, as instâncias de carteiras devem registar todas as transações com utilizadores de carteiras e outras unidades de carteira, incluindo a aposição de assinaturas e selos eletrónicos.

2. As informações registadas devem conter, pelo menos:

a) A hora e data da transação;

b) O nome, os dados de contacto e o identificador único do utilizador de carteira correspondente e do Estado-Membro de estabelecimento desse utilizador ou, no caso de outras unidades de carteira, informações pertinentes do certificado de unidade de carteira;

c) O tipo ou tipos de dados solicitados e apresentados na transação;

d) No caso de transações não concluídas, a razão dessa não conclusão.

3. Os fornecedores de carteiras devem assegurar a integridade, a autenticidade e a confidencialidade das informações registadas.

4. As instâncias de carteiras devem registar as comunicações enviadas pelo utente da carteira às autoridades de proteção de dados através da sua unidade de carteira.

5. O fornecedor de carteiras deve ter acesso aos registos a que se referem os n.os 1 e 2, sempre que tal seja necessário para a prestação de serviços de carteira, com base no consentimento prévio explícito do utente da carteira.

6. Os registos a que se referem os n.os 1 e 2 devem permanecer acessíveis enquanto tal for exigido pelo direito da União ou pelo direito nacional.

7. Os fornecedores de carteiras devem permitir que os utentes das carteiras exportem as informações registadas a que se refere o n.º 2.

Artigo 10.º

Divulgação incorporada

1. Os fornecedores de carteiras devem assegurar que as unidades de carteira que disponibilizam são capazes de processar os certificados eletrónicos de atributos com as políticas comuns de divulgação incorporadas estabelecidas no anexo III.

2. As instâncias de carteiras devem ser capazes de processar e apresentar as políticas de divulgação incorporadas a que se refere o n.º 1, em conjugação com os dados recebidos do utilizador de carteira requerente.

3. As instâncias de carteiras devem verificar se o utilizador de carteira cumpre os requisitos da política de divulgação incorporada e informar o utente da carteira do resultado.

Artigo 11.º

Assinaturas e selos eletrónicos qualificados

1. Os fornecedores de carteiras devem assegurar que os utentes das carteiras podem receber certificados qualificados para assinaturas ou selos eletrónicos qualificados associados a dispositivos locais, externos ou remotos, em relação às instâncias de carteiras, de criação de assinaturas ou selos qualificados.

2. Os fornecedores de carteiras devem assegurar que as soluções de carteiras são capazes de interagir de forma segura com um dos seguintes tipos de dispositivos de criação de assinaturas ou selos qualificados: dispositivos locais, externos ou geridos à distância de criação de assinaturas ou selos qualificados para efeitos da utilização dos certificados qualificados a que se refere o n.º 1.

3. Os fornecedores de carteiras devem assegurar que os utentes das carteiras que sejam pessoas singulares tenham, pelo menos para fins não profissionais, acesso gratuito a aplicações de criação de assinaturas que permitam a criação gratuita de assinaturas eletrónicas qualificadas utilizando os certificados a que se refere o n.º 1.

Artigo 12.º

Aplicações de criação de assinaturas

1. As aplicações de criação de assinaturas utilizadas pelas unidades de carteira podem ser disponibilizadas por fornecedores de carteiras, por prestadores de serviços de confiança ou por utilizadores de carteiras.

2. As aplicações de criação de assinaturas devem dispor das seguintes funções:

a) Apor uma assinatura ou um selo nos dados facultados pelos utentes das carteiras;

b) Apor uma assinatura ou um selo nos dados facultados pelo utilizador;

c) Criar assinaturas ou selos em conformidade, pelo menos, com os formatos obrigatórios referidos no anexo IV;

d) Informar os utentes das carteiras sobre o resultado do processo de criação de assinaturas ou selos.

3. As aplicações de criação de assinaturas podem ser integradas em instâncias de carteiras ou ser externas às mesmas. Caso as aplicações de criação de assinaturas recorram a dispositivos qualificados de criação de assinaturas à distância e estejam integradas em instâncias de carteiras, devem suportar a interface de programação de aplicações a que se refere o anexo IV.

Artigo 13.º

Exportação e portabilidade dos dados

As unidades de carteira devem, sempre que tal seja tecnicamente viável e exceto em casos que envolvam ativos críticos, permitir a exportação e a portabilidade seguras dos dados pessoais do utente da carteira, a fim de possibilitar a migração do utente da carteira para uma unidade de carteira de outra solução de carteira, conforme estabelecido no Regulamento de Execução (UE) 2015/1502.

Artigo 14.º

Pseudónimos

1. As unidades de carteira devem permitir a geração de pseudónimos para os utentes das carteiras, em conformidade com as especificações técnicas estabelecidas no anexo V.

2. As unidades de carteira devem permitir a geração, a pedido de um utilizador de carteira, de um pseudónimo específico e único para esse utilizador de carteira e facultar esse pseudónimo ao utilizador de carteira, seja de forma autónoma seja em combinação com quaisquer dados de identificação pessoal ou certificados eletrónicos de atributos solicitados por esse utilizador.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Artigo 15.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

LISTA DAS NORMAS REFERIDAS NO ARTIGO 5.º

— SAM.01, *Secured Applications for Mobile* [Requisitos para suportar *applets* de terceiros em eSIM e eSE via SAM], v1.1, 2023, GSMA;

— GPC_GUI_ 217, *SAM Configuration* [Especificações técnicas para a implementação de SAM], v1.0, abril de 2024, GlobalPlatform;

— GPC_SPE_0 34, *Card Specification* [Especificações técnicas para cartões inteligentes], v2.3.1, março de 2018, GlobalPlatform;

— GPC_SPE_0 07, *Confidential Card Content Management – Amendment A*, v1.2, julho de 2019, GlobalPlatform;

— GPC_SPE_0 13, *Secure Channel Protocol 03 – Amendment D*, v1.2, abril de 2020, GlobalPlatform;

— GPC_SPE_0 93, *Secure Channel Protocol 11 – Amendment F*, v1.4, março de 2024, GlobalPlatform;

— GPD_SPE_0 75, *Open Mobile API (OMAPI) Specification* [IPA para que as aplicações móveis acedam a elementos seguros nos dispositivos do utente], v3.3, agosto de 2018, GlobalPlatform.

ANEXO II

LISTA DAS NORMAS REFERIDAS NO ARTIGO 8.º

— ISO/IEC.18013-5:2021;

— *Verifiable Credentials Data Model 1.1.*, recomendação do W3C, 3 de março de 2022.

ANEXO III

LISTA DAS POLÍTICAS COMUNS DE DIVULGAÇÃO INCORPORADAS A QUE SE REFERE O ARTIGO 10.º

1. «Nenhuma política» indica que não é aplicável nenhuma política aos certificados eletrónicos de atributos.
2. «Política "reservado a utilizadores autorizados"» indica que os utentes de carteiras só podem divulgar certificados eletrónicos de atributos a utilizadores autenticados que estejam explicitamente enumerados nas políticas de divulgação.
3. «Raiz específica de confiança» indica que os utentes das carteiras só devem divulgar o certificado eletrónico de atributos específico aos utilizadores de carteiras autenticados com certificados de acesso de utilizadores de carteiras derivados de uma raiz específica (ou lista de raízes específicas) ou de um ou vários certificados intermédios.

ANEXO IV

FORMATOS DAS ASSINATURAS E DOS SELOS A QUE SE REFERE O ARTIGO 12.º

1. Formato obrigatório das assinaturas ou dos selos:

   a) PAdES (*PDF Advanced Electronic Signature*), conforme especificado na norma ETSI EN 319 142-1 V1.1.1 (abril de 2016), *Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures*.

2. Lista de formatos facultativos das assinaturas ou dos selos:

   a) XAdES, conforme especificado na norma ETSI EN 319 132-1 V1.2.1 (fevereiro de 2022), *Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures (XAdES)*, para assinaturas no formato XML;

   b) JAdES, conforme especificado na norma ETSI TS 119 182-1 V1.2.1 (julho de 2024), *Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures*, para assinaturas no formato JSON;

   c) CAdES (*CMS Advanced Electronic Signature*), conforme especificado na norma ETSI EN 319 122-1 V1.3.1 (junho de 2023), *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures*, para assinaturas no formato CMS;

   d) ASiC (*Associated Signature Container*), conforme especificado na norma ETSI EN 319 162-1 V1.1.1 (abril de 2016), *Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers* e ETSI EN 319 162-2 V1.1.1 (abril de 2016) *Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers*, para assinaturas de contentores.

3. Interface de programação de aplicações:

   — Especificação do Cloud Signature Consortium (CSC), v2.0 (20 de abril de 2023).

ANEXO V

ESPECIFICAÇÕES TÉCNICAS PARA A GERAÇÃO DE PSEUDÓNIMOS A QUE SE REFERE O ARTIGO 14.º

Especificações técnicas:

— Web*Authn*, recomendação do W3C, 8 de abril de 2021, nível 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.