2026/1731

22.7.2026

REGULAMENTO DE EXECUÇÃO (UE) 2026/1731 DA COMISSÃO

de 15 de julho de 2026

que altera os Regulamentos de Execução (UE) 2024/2977, (UE) 2024/2979, (UE) 2024/2980 e (UE) 2024/2982 no respeitante às normas e especificações aplicáveis

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) A fim de assegurar o mais elevado nível de harmonização entre os Estados-Membros para o desenvolvimento das carteiras europeias de identidade digital, as especificações técnicas das carteiras baseiam-se nos trabalhos realizados nos termos da Recomendação (UE) 2021/946 da Comissão ([2]) e, em especial, na arquitetura e no regime de referência. Uma vez que ambos evoluíram significativamente desde a adoção dos Regulamentos de Execução (UE) 2024/2977 ([3]), (UE) 2024/2979 ([4]), (UE) 2024/2980 ([5]) e (UE) 2024/2982 ([6]) da Comissão, estes deverão agora ser alterados de forma a estarem alinhados com as novas normas, especificações e procedimentos.

Em conformidade com os objetivos do Regulamento (UE) n.º 910/2014, foram selecionadas várias normas para cumprir estes requisitos específicos. Estas normas deverão refletir as práticas estabelecidas e ser amplamente reconhecidas nos setores pertinentes. Por exemplo, uma vez que o formato W3C VCDM é utilizado como formato de referência para certificados, em especial no setor da educação, as carteiras europeias de identidade digital deverão também suportar este formato quando estiverem disponíveis os novos perfis no formato W3C VCDM. Sempre que necessário, estas normas deverão ser adaptadas ou complementadas de modo a assegurar a segurança e a fiabilidade das carteiras europeias de identidade digital, facilitando simultaneamente a interoperabilidade transfronteiriça e o bom funcionamento do mercado interno.

(2) Para qualquer utilização da carteira que exija a apresentação do retrato do utente da carteira, as soluções de carteiras têm de suportar a funcionalidade de divulgação seletiva, sob o pleno controlo do utente. A fim de preservar a capacidade de decidir sobre a divulgação e de proteger o retrato contra pedidos de divulgação não intencionais ou não autorizados, a conceção arquitetural das carteiras europeias de identidade digital deverá prever mecanismos de alerta e o registo de todas as transações relacionadas com a utilização do retrato. De modo a assegurar que o utente da carteira tem conhecimento da partilha de dados biométricos, os alertas deverão indicar que o pedido implica a

([1]) JO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

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

([3]) 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).

([4]) 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).

([5]) 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).

([6]) 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).

partilha de dados biométricos e exigir especificamente a confirmação da divulgação por parte do utente. Sempre que um utilizador trate o retrato para efeitos de identificação inequívoca de uma pessoa singular ou para confirmar a identidade declarada dessa pessoa, aplicam-se os artigos 6.º e 9.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([7]), bem como todos os outros requisitos desse regulamento, nomeadamente que o tratamento do retrato pelos utilizadores se deverá limitar ao necessário para a utilização prevista. A utilização prevista deverá ser comunicada ao utente da carteira, juntamente com o pedido de divulgação, em linguagem clara e compreensível. A fim de ter devidamente em conta a sensibilidade dos dados biométricos, o utente da carteira deverá confirmar de forma explícita e específica a divulgação do retrato. A ausência de resposta ou casas previamente assinaladas não deverão ser consideradas como uma confirmação do utente de carteira. A confirmação explícita do utente da carteira deverá ser uma salvaguarda técnica e não constituir, por si só, um fundamento jurídico para o tratamento. Tal como referido no artigo 9.º, n.º 4, do Regulamento (UE) 2016/679, os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.

(3) Para dar aos Estados-Membros tempo suficiente para adaptarem os seus procedimentos nacionais, o retrato do utente de carteira pode fazer parte dos dados de identificação pessoal obrigatórios para a pessoa singular apenas a partir de 11 de agosto de 2028. Sempre que estas imagens forem obtidas a partir de documentos de identidade existentes, como bilhetes de identidade ou passaportes, aplicam-se os requisitos pertinentes estabelecidos nos Regulamentos (UE) 2025/1208 ([8]) ou (CE) n.º 2252/2004 ([9]) do Conselho, respetivamente.

(4) O Regulamento (UE) n.º 910/2014 exige que as carteiras sejam capazes de exibir uma marca de confiança «UE» para a carteira de identidade digital como indicação verificável, simples e reconhecível de que uma carteira foi fornecida em conformidade com o regulamento. A utilização dessa marca de confiança apoiará o funcionamento eficaz do mercado interno, garantirá uma concorrência leal e protegerá os interesses dos consumidores. A fim de permitir a sua utilização, deverão ser definidas as respetivas características visuais e técnicas.

(5) Tal como estabelecido no artigo 12.º-B do Regulamento (UE) n.º 910/2014, os controladores de acesso devem permitir aos fornecedores de carteiras europeias de identidade digital e aos emitentes de meios de identificação eletrónica notificados uma interoperabilidade efetiva com as funcionalidades do mesmo sistema operativo, *hardware* ou *software* e, para efeitos de interoperabilidade, o acesso aos mesmos. Essa interoperabilidade e esse acesso efetivos devem ser prestados a título gratuito e independentemente de essas funcionalidades de *hardware* ou de *software* fazerem parte do sistema operativo, estarem disponíveis ou serem utilizadas por esse controlador de acesso na prestação desses serviços. Uma vez que todas as soluções de carteiras deverão apoiar um conjunto comum de protocolos e interfaces para assegurarem a facilidade de utilização, a segurança e a interoperabilidade em todos os Estados-Membros, os controladores de acesso deverão permitir as funcionalidades do sistema operativo, do *hardware* ou do *software* necessárias para aplicar os protocolos e as interfaces estabelecidos no anexo XII do presente regulamento. Neste contexto, nos fluxos entre dispositivos em linha, tanto para a verificação de proximidade física como para a transferência de dados entre os dois dispositivos, os controladores de acesso deverão privilegiar a utilização de um canal de comunicação local, tal como previsto pela versão 2.3 da especificação do protocolo cliente a autenticador (CTAP) ([10]), à utilização de serviços de túnel CTAP híbrido.

(6) A fim de dar aos Estados-Membros, aos fornecedores de certificados de registo de utilizadores de carteiras e aos fornecedores de carteiras tempo suficiente para permitir que as unidades de carteira autentiquem e validem os certificados de registo de utilizadores de carteiras, este requisito só deverá ser aplicável a partir de 11 de agosto de 2028.

(7) O Regulamento (UE) 2016/679 e, se for caso disso, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([11]) aplicam-se a todas as atividades de tratamento de dados pessoais ao abrigo do presente regulamento.

([7]) 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).

([8]) Regulamento (UE) 2025/1208 do Conselho, de 12 de junho de 2025, que visa reforçar a segurança dos bilhetes de identidade dos cidadãos da União e dos títulos de residência emitidos aos cidadãos da União e seus familiares que exercem o direito à livre circulação (JO L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Regulamento (CE) n.º 2252/2004 do Conselho, de 13 de dezembro de 2004, que estabelece normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros (JO L 385 de 29.12.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Norma proposta pela Fido Alliance, *Client to Authenticator Protocol (CTAP)*, 26 de fevereiro de 2026.

([11]) 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).

(8) 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 ([12]) e emitiu parecer em 17 de abril de 2026 ([13]).

(9) As medidas previstas no presente regulamento estão em conformidade com o parecer do comité instituído pelo artigo 48.º do Regulamento (UE) n.º 910/2014,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Alterações do Regulamento de Execução (UE) 2024/2977

O Regulamento de Execução (UE) 2024/2977 é alterado do seguinte modo:

1) É inserido o seguinte artigo 3.º-A:

«*Artigo 3.º-A*

Proteção do retrato

1. Para além dos requisitos de informação nos termos do Regulamento (UE) 2016/679, os fornecedores de carteiras devem assegurar que as soluções de carteiras que fornecem emitem alertas aos utentes das carteiras sempre que os utilizadores solicitem a divulgação do retrato, indicando que o pedido envolve a partilha de dados biométricos e exige a confirmação da divulgação seletiva do retrato.

2. Para a aplicação da divulgação seletiva do retrato a um utilizador de carteira, os fornecedores de carteiras devem assegurar que as soluções de carteiras exigem que o utente da carteira confirme de forma explícita e específica a apresentação do retrato.

3. O retrato não pode ser conservado pelos utilizadores de carteiras, a menos que o seu tratamento seja necessário para efeito de identificação e autenticação em conformidade com o direito da União em matéria de proteção de dados ou sempre que tal esteja previsto no direito da União ou no direito nacional, em conformidade com o direito da União em matéria de proteção de dados. O retrato não pode ser transferido para países terceiros ou organizações internacionais, a menos que o direito da União em matéria de proteção de dados o permita.»;

2) No artigo 4.º, o n.º 1 passa a ter a seguinte redação:

«1. Os certificados eletrónicos de atributos emitidos para unidades de carteira devem cumprir, pelo menos, uma das normas estabelecidas no anexo II do Regulamento de Execução (UE) 2024/2979.»;

3) No artigo 5.º, o n.º 4, alínea b), passa a ter a seguinte redação:

«b) Se o certificado de unidade de carteira da unidade de carteira para o qual foram emitidos os dados de identificação pessoal tiver sido revogado;»;

4) O anexo é substituído pelo texto que consta do anexo I do presente regulamento.

([12]) 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).

([13]) *EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980* | Autoridade Europeia para a Proteção de Dados.

Artigo 2.º

Alterações do Regulamento de Execução (UE) 2024/2979

O Regulamento de Execução (UE) 2024/2979 é alterado do seguinte modo:

1) No artigo 3.º, é suprimido o n.º 2;

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

«a) Realizam operações criptográficas de carteira que envolvam ativos críticos armazenados num dispositivo criptográfico seguro de carteiras e que não são necessários para a autenticação do utente da carteira apenas nos casos em que essas aplicações tenham autenticado com êxito os utentes das carteiras;»;

3) É inserido o seguinte artigo 5.º-A:

«*Artigo 5.º-A*

Mecanismos criptográficos

Os fornecedores de carteiras devem, para efeitos do artigo 4.º, n.º 2, utilizar apenas os mecanismos criptográficos referidos no anexo I-A.»;

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

a) O n.º 1 passa a ter a seguinte redação:

«1. Os fornecedores de carteiras devem emitir certificados de unidades de carteira para cada unidade de carteira. Os utilizadores de carteiras devem apor uma assinatura ou um selo nos certificados de unidade de carteira de forma a que as assinaturas ou selos possam ser validados por meio de um certificado incluído numa lista em conformidade com a secção 2, ponto 1), alínea h), do anexo II do Regulamento de Execução (UE) 2024/2980.»;

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

«2. Os fornecedores de carteiras devem assegurar que os certificados de unidades de carteira a que se refere o n.º 1 estão em conformidade com as especificações técnicas estabelecidas no anexo I-B.»;

c) No n.º 3, a alínea b) passa a ter a seguinte redação:

«b) Disponibilizar mecanismos seguros de identificação e autenticação aos utentes das carteiras que sejam independentes das unidades de carteira;»;

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

«b) O nome, os dados de contacto e o identificador único do utilizador de carteira correspondente e do Estado-Membro de estabelecimento desse utilizador;»;

6) No artigo 10.º, o n.º 1 passa a ter a seguinte redação:

«1. Os fornecedores de carteiras devem assegurar que as unidades de carteira que disponibilizam são capazes de processar os certificados eletrónicos de atributos emitidos em conformidade com as especificações técnicas aplicáveis às políticas comuns de divulgação incorporadas estabelecidas no anexo III.»;

7) O artigo 12.º é alterado do seguinte modo:

a) No n.º 2, a alínea c) passa a ter a seguinte redação:

«c) Criar assinaturas ou selos em conformidade, pelo menos, com o formato obrigatório de assinatura ou selo referido no anexo IV;»;

b) O n.º 3 passa a ter a seguinte redação:

«3. As aplicações de criação de assinaturas podem ser integradas em instâncias de carteiras ou ser externas às mesmas.»;

c) É inserido o seguinte número:

«4. As aplicações de criação de assinaturas utilizadas pelas unidades de carteira devem suportar, pelo menos, a interface de programação de aplicações referida no anexo IV.»;

8) No artigo 14.º, é suprimido o n.º 1;

9) É inserido o seguinte artigo 14.º-A:

«*Artigo 14.º-A*

Marca de confiança "UE" para a carteira de identidade digital

1. Os fornecedores de carteiras devem assegurar que as unidades de carteira exibem a marca de confiança "UE" para a carteira de identidade digital. A marca de confiança "UE" para a carteira de identidade digital deve ser apresentada no formato constante dos anexos VI e VII.

2. Os fornecedores de carteiras devem assegurar que as unidades de carteira autorizam o acesso dos utentes das carteiras a informações que lhes permitam verificar o estado de certificação da solução de carteira. Para o efeito, devem garantir que, após o registo de uma solução de carteira, as unidades de carteira correspondentes incluem os URL fornecidos pela Comissão Europeia para essa verificação. Devem igualmente garantir que as respetivas unidades de carteira têm acesso aos dados da marca de confiança "UE" para a carteira de identidade digital que estão em conformidade com as especificações técnicas estabelecidas no anexo VIII.

3. As cores de referência da marca de confiança "UE" para a carteira de identidade digital são o Pantone n.º 661 e o n.º 116, ou azul (100 % ciano + 67 % magenta + 0 % amarelo + 40 % preto) e amarelo (0 % ciano + 20 % magenta + 100 % amarelo + 0 % preto) quando é utilizada quadricromia; quando são usadas cores RGB, as cores de referência são azul (0 vermelho + 51 verde + 153 azul) e amarelo (255 vermelho + 204 verde + 0 azul).

4. A marca de confiança "UE" para a carteira de identidade digital pode ser usada em preto e branco, conforme estabelecida no anexo VII, apenas quando a utilização de cor não é viável.

5. Se a marca de confiança "UE" para a carteira de identidade digital for colocada num fundo de cor escura, é possível recorrer ao formato negativo utilizando a mesma cor de fundo. Da mesma forma, se a marca de confiança "UE" para a carteira de identidade digital for utilizada a cores ou com um fundo colorido que dificulte a sua visibilidade, pode ser delimitada por uma linha exterior à sua volta, a fim de melhorar o contraste com as cores de fundo.

6. A marca de confiança "UE" para a carteira de identidade digital deve ter uma dimensão mínima de 64 × 85 píxeis a 150 DPI.

7. Os fornecedores de carteiras devem assegurar que a marca de confiança "UE" para a carteira de identidade digital é utilizada de forma a permitir a indicação clara da unidade de carteira a que diz respeito. A marca de confiança "UE" para a carteira de identidade digital pode ser associada a elementos gráficos ou textuais que indiquem claramente a unidade de carteira para a qual é utilizada, desde que não alterem o seu reconhecimento como marca de confiança "UE" para a carteira de identidade digital nem a associação com a lista de carteiras europeias de identidade digital certificadas a que se refere o artigo 5.º-D do Regulamento (UE) n.º 910/2014.

8. Caso os fornecedores de carteiras tenham revogado um certificado de unidade de carteira, devem assegurar que a marca de confiança "UE" para a carteira de identidade digital deixa de ser exibida pela unidade de carteira correspondente.»;

10) São aditados os anexos I-A e I-B, tal como estabelecidos nos anexos II e III do presente regulamento;

11) O anexo II é substituído pelo anexo IV do presente regulamento;

12) O anexo III é substituído pelo anexo V do presente regulamento;

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

14) O anexo V é suprimido;

15) O texto que consta do anexo VII do presente regulamento é inserido como anexo VI;

16) O texto que consta do anexo VIII do presente regulamento é inserido como anexo VII;

17) O texto que consta do anexo IX do presente regulamento é inserido como anexo VIII.

Artigo 3.º

Alterações do Regulamento de Execução (UE) 2024/2980

O Regulamento de Execução (UE) 2024/2980 é alterado do seguinte modo:

1) No artigo 5.º, o n.º 2 passa a ter a seguinte redação:

«2. Se for caso disso, a Comissão elabora, mantém e publica uma lista que inclui as informações notificadas pelos Estados-Membros sobre os fornecedores de carteiras, os fornecedores de dados de identificação pessoal, os fornecedores de certificados de acesso de utilizadores de carteiras e os fornecedores de certificados de registo de utilizadores de carteiras, conforme referido no anexo II, secções 2, 3, 4 e 5.».

2) O anexo II do Regulamento de Execução (UE) 2024/2980 é alterado em conformidade com o anexo X do presente regulamento.

Artigo 4.º

Alterações do Regulamento de Execução (UE) 2024/2982

O Regulamento de Execução (UE) 2024/2982 é alterado do seguinte modo:

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

«2) A apresentação de atributos de dados de identificação pessoal e certificados eletrónicos de atributos aos utilizadores de carteiras;»;

2) O artigo 3.º é alterado do seguinte modo:

a) O ponto 1) passa a ter a seguinte redação:

«1) Autenticam e validam os certificados de acesso de utilizadores de carteiras caso interajam com utilizadores de carteiras sem delegar a execução destes processos no navegador de um sistema operativo ou noutra aplicação intermediária;»;

b) O ponto 2) é suprimido;

c) O ponto 3) passa a ter a seguinte redação:

«3) Autenticam e validam os pedidos apresentados utilizando certificados de acesso de utilizadores de carteiras;»;

d) O ponto 4) passa a ter a seguinte redação:

«4) Autenticam e validam o certificado de registo de utilizador de carteira;»;

e) O ponto 5) passa a ter a seguinte redação:

«5) Apresentam aos utentes das carteiras as informações contidas nos certificados de acesso de utilizadores de carteiras;»;

f) O ponto 8) é suprimido;

g) O ponto 9) passa a ter a seguinte redação:

«9) Não apresentam quaisquer atributos solicitados a utilizadores de carteiras até que estejam concluídas as seguintes etapas:

a) Verificação de que as políticas de divulgação incorporadas foram processadas na unidade de carteira em conformidade com o artigo 10.º do Regulamento de Execução (UE) 2024/2979;

b) Verificação de que os utentes das carteiras aprovaram parcial ou integralmente a apresentação.»;

3) No artigo 4.º, o n.º 1 passa a ter a seguinte redação:

«1. Os fornecedores de carteiras devem assegurar que as soluções de carteiras suportam os protocolos e interfaces estabelecidos no anexo I para a emissão de dados de identificação pessoal e certificados eletrónicos de atributos para unidades de carteira.»;

4) O artigo 5.º é alterado do seguinte modo:

a) Os n.ºs 1 e 2 passam a ter a seguinte redação:

«1. Os fornecedores de carteiras asseguram que as soluções de carteiras suportam protocolos e interfaces para a apresentação de atributos a utilizadores de carteiras, à distância e, se for caso disso, em situação de proximidade, nos termos das especificações técnicas estabelecidas no anexo II.

2. Os fornecedores de carteiras devem assegurar que, a pedido dos utentes, as unidades de carteira respondem aos pedidos devidamente autenticados e validados dos utilizadores de carteiras a que se refere o artigo 3.º, nos termos das especificações técnicas estabelecidas no anexo II.»;

b) É suprimido o n.º 5;

5) O artigo 8.º passa a ter a seguinte redação:

«*Artigo 8.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 artigo 3, ponto 4), é aplicável a partir de 11 de agosto de 2028.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.»;

6) O anexo é suprimido;

7) O texto que consta do anexo XI do presente regulamento é aditado como anexo I;

8) O texto que consta do anexo XII do presente regulamento é aditado como anexo II.

Artigo 5.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 15 de julho de 2026.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO I

«ANEXO

Especificações técnicas para os dados de identificação pessoal a que se refere o artigo 3.º, n.º 3

(1) Secção 1: Conjunto de dados de identificação de pessoas singulares

Quadro 1

Dados de identificação pessoal obrigatórios para pessoas singulares para divulgação seletiva

Identificador dos dados	Definição
`family_name`	Apelido(s) atual(ais) do utente a quem os dados de identificação pessoal se referem.
`given_name`	Nome(s) próprio(s) atual(ais), incluindo outro(s) nome(s) próprio(s), se for caso disso, do utente a quem os dados de identificação pessoal se referem.
`birth_date`	Dia, mês e ano de nascimento do utente a quem os dados de identificação pessoal se referem.
`birth_place`	O país, indicado por meio do código alpha-2, tal como especificado na norma ISO 3166-1, ou o Estado, província, distrito ou zona local ou o município, cidade, vila ou aldeia de nascimento do utente a quem os dados de identificação pessoal se referem.
`nationality`	Um ou mais códigos de país alpha-2, conforme especificado na norma ISO 3166-1, que representam a nacionalidade do utente a quem os dados de identificação pessoal se referem.
`portrait`	Exceto quando o utente opta explicitamente por não a incluir, se for caso disso, a imagem facial do utente a quem os dados de identificação pessoal se referem, em conformidade com os requisitos de qualidade para um tipo de imagem frontal completa, conforme estabelecido pela norma ISO/IEC 39794-5 ou, para retrocompatibilidade, pela norma ISO/IEC 19794-5, cláusulas 8.2, 8.3 e 8.4, fornecida como dados de imagem codificados sem os cabeçalhos ou blocos, conforme especificado pela norma ISO/IEC 19794-5, cláusula 5, com exceção dos próprios dados da imagem (JPEG), é aplicável a partir de 11 de agosto de 2028.

— Os Estados-Membros podem prever que o utente tenha a opção de recusar a inserção do retrato nos dados de identificação pessoal.

— Os Estados-Membros devem assegurar que a divulgação seletiva é aplicável a cada identificador de dados, incluindo o retrato.

— Quando a data de nascimento da pessoa singular não é conhecida, os Estados-Membros devem escolher valores adequados que estejam em conformidade com as especificações estabelecidas nas secções 4.1 ou 4.2 (conforme adequado) do presente anexo.

— Quando a nacionalidade da pessoa singular é desconhecida, os Estados-Membros devem utilizar o valor "QU".

— Quando a pessoa singular não possui uma nacionalidade, os Estados-Membros devem utilizar o valor "QS".

— Quando o utente opta por não incluir o retrato, os Estados-Membros devem deixar o valor vazio.

Quadro 2

Dados de identificação pessoal facultativos para pessoas singulares para divulgação seletiva

Identificador dos dados	Definição
`resident_address`	O endereço completo do local de residência ou contacto atual do utente a quem os dados de identificação pessoal se referem (rua, número da porta, cidade, etc.).
`resident_country`	O país de residência atual do utente a quem os dados de identificação pessoal se referem, indicado por meio do código de país alpha-2, conforme especificado na norma ISO 3166-1.
`resident_state`	O Estado, a província, o distrito ou a zona local de residência atual do utente a quem os dados de identificação pessoal se referem.
`resident_city`	O município, a cidade, a vila ou a aldeia de residência atual do utente a quem os dados de identificação pessoal se referem.
`resident_postal_code`	O código postal do local de residência atual do utente a quem os dados de identificação pessoal se referem.
`resident_street`	O nome da rua de residência atual do utente a quem os dados de identificação pessoal se referem, incluindo o número da porta e qualquer afixo ou sufixo.
`personal_administrative_-number`	Um valor atribuído ao utente a quem os dados de identificação pessoal se referem que é único entre todos os números administrativos pessoais emitidos pelo fornecedor de dados de identificação pessoal. Caso os Estados-Membros optem por incluir este atributo, devem descrever nos seus sistemas de identificação eletrónica, ao abrigo dos quais os dados de identificação pessoal são emitidos, a política que aplicam aos valores deste atributo, incluindo, se for caso disso, condições específicas para o tratamento deste valor.
`family_name_birth`	Apelido(s) do utente a quem os dados de identificação pessoal se referem no momento do nascimento.
`given_name_birth`	Nome(s) próprio(s), incluindo outro(s) nome(s) próprio(s), do utente a quem os dados de identificação pessoal se referem no momento do nascimento.
`sex`	O valor deve ser um dos seguintes: 0 = desconhecido; 1 = masculino; 2 = feminino; 3 = outro; 4 = intersexual; 5 = diverso; 6 = fluido; 9 = não aplicável; Para os valores 0, 1, 2 e 9, aplica-se a norma ISO/IEC 5218.
`email_address`	Endereço de correio eletrónico do utente a quem os dados de identificação pessoal se referem [tal como especificado no RFC 5322 ([1])].

Identificador dos dados	Definição
`mobile_phone_number`	Número de telemóvel do utente a quem os dados de identificação pessoal se referem, começando pelo símbolo "+" como prefixo internacional e o código do país, seguido apenas de números.

([1]) P. Resnick, Ed., "Internet Message Format", RFC 5322, outubro de 2008.

(2) Secção 2: Conjunto de dados de identificação de pessoas coletivas

Quadro 3

Dados de identificação pessoal obrigatórios para pessoas coletivas

Identificador dos dados
Denominação oficial atual
Um identificador único atribuído pelo Estado-Membro de expedição, conforme com as especificações técnicas para efeitos de identificação transfronteiriça e tão persistente quanto possível no tempo.

— Caso um identificador de dados da pessoa não seja conhecido ou não possa ser emitido como parte do conjunto de dados de identificação pessoal, os Estados-Membros devem, em vez disso, utilizar o valor de um atributo adequado à situação.

Quadro 4

Dados de identificação pessoal facultativos para pessoas coletivas

Identificador dos dados
Endereço atual
Número IVA
Número de identificação fiscal
Identificador único europeu a que se refere a Diretiva (UE) 2017/1132 do Parlamento Europeu e do Conselho ([1])
Identificador de entidade jurídica (LEI) a que se refere o Regulamento de Execução (UE) 2022/1860 da Comissão ([2])
Número de registo de operador económico (EORI) a que se refere o Regulamento de Execução (UE) n.º 1352/2013 da Comissão ([3])
Número de imposto especial de consumo previsto no artigo 2.º, ponto 12), do Regulamento (UE) n.º 389/2012 do Conselho ([4])

([1]) Diretiva (UE) 2017/1132 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, relativa a determinados aspetos do direito das sociedades (JO L 169 de 30.6.2017, p.46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Regulamento de Execução (UE) 2022/1860 da Comissão de 10 de junho de 2022 que estabelece normas técnicas de execução relativamente à aplicação do Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho no que diz respeito aos padrões, formatos, periodicidade, métodos e mecanismos de comunicação de informações (JO L 262 de 7.10.2022, p.68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Regulamento de Execução (UE) n.º 1352/2013 da Comissão, de 4 de dezembro de 2013 , que estabelece os formulários previstos no Regulamento (UE) n.º 608/2013 do Parlamento Europeu e do Conselho relativo à intervenção das autoridades aduaneiras para assegurar o cumprimento da legislação sobre os direitos de propriedade intelectual (JO L 341 de 18.12.2013, p.10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Regulamento (UE) n.º 389/2012 do Conselho, de 2 de maio de 2012 , relativo à cooperação administrativa no domínio dos impostos especiais de consumo e que revoga o Regulamento (CE) n.º 2073/2004 (JO L 121 de 8.5.2012, p.1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

(3) Secção 3: Conjunto de metadados sobre os dados de identificação pessoal

Quadro 5

Metadados sobre os dados de identificação pessoal

Identificador dos dados	Definição	Presença
`issuing_authority`	Nome da autoridade administrativa que emitiu os dados de identificação pessoal ou o código de país alpha-2 de acordo com a norma ISO 3166 do respetivo Estado-Membro, caso não exista uma autoridade distinta habilitada a emitir dados de identificação pessoal.	Obrigatória
`issuing_country`	Código de país alpha-2, conforme especificado na norma ISO 3166-1, do país ou território do fornecedor dos dados de identificação pessoal.	Obrigatória
`expiry_date`	Data (e, se possível, hora) de expiração do período de validade administrativa dos dados de identificação pessoal.	Facultativa
`document_number`	Um número para os dados de identificação pessoal, atribuído pelo fornecedor de dados de identificação pessoal.	Facultativa
`issuing_jurisdiction`	Código de subdivisão do país da jurisdição que emitiu os dados de identificação pessoal, conforme especificado na norma ISO 3166-2:2020, cláusula 8. A primeira parte do código deve ser igual ao valor do país emissor.	Facultativa
`issuance_date`	Data (e, se possível, hora) de início do período de validade administrativa dos dados de identificação pessoal.	Facultativa

(4) Secção 4: Codificação dos atributos dos dados de identificação de pessoas singulares

— Os dados de identificação de pessoas singulares devem ser emitidos em conformidade com as normas estabelecidas no anexo II do Regulamento de Execução (UE) 2024/2979, cláusulas 5 (formato SD-JWT VC) e 6 (formato ISO/IEC-mdoc), aplicáveis aos certificados eletrónicos de atributos. As cláusulas 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 e 6.2.5 não são aplicáveis.

— A codificação dos dados de identificação de pessoas singulares deve cumprir as especificações técnicas constantes das secções 4.1 e 4.2 do presente anexo.

4.1 Codificação dos dados de identificação de pessoas singulares em formato ISO/IEC-mdoc

— O tipo de certificado dos dados de identificação pessoal em formato ISO/IEC mdoc deve ser "eu.europa.ec.eudi.pid.1". O identificador do espaço de nomes dos atributos dos dados de identificação pessoal estabelecido no presente anexo deve ser "eu.europa.ec.eudi.pid.1".

— Quando os dados de identificação pessoal incluem dados cujos identificadores de dados não constam do presente anexo, esses dados devem ser definidos num espaço de nomes de dados de identificação pessoal nacional que utilize o formato geral eu.europa.ec.eudi.pid.[código de país ISO 3166-1 alpha-2 ou código de região ISO 3166-2] seguido de um ponto e de um número de versão facultativos.

— Quando é utilizado o espaço de nomes nacional, o seu sistema, incluindo todos os identificadores de dados, as respetivas definições, presença e formatos de codificação, devem ser publicados em conformidade com o artigo 8.º do Regulamento de Execução (UE) 2025/1569 da Comissão ([1]).

— Os dados de identificação pessoal e os respetivos metadados estabelecidos nas secções 1 e 3 do presente anexo devem ser incluídos nos elementos de dados de identificação pessoal na aceção das especificações do formato ISO/IEC mdoc.

— O membro deviceKey do membro deviceKeyInfo da instância do tipo MobileSecurityObject deve conter uma chave pública.

— Essa chave pública deve corresponder a uma chave privada armazenada no dispositivo criptográfico seguro de carteiras ("WSCD") do utente da carteira.

— O cabeçalho protegido da assinatura digital CB-AdES que assina dados de identificação pessoal em formato ISO/IEC-mdoc deve conter os parâmetros de cabeçalho x5u e x5t, ambos especificados no RFC 9360 ([2]).

— O algoritmo de resumo utilizado no parâmetro de cabeçalho x5t deve ser SHA-256.

— Os requisitos de codificação dos dados de identificação pessoal em formato ISO/IEC-mdoc estão estabelecidos no quadro 6.

Quadro 6

Requisitos de codificação dos dados de identificação pessoal em formato ISO/IEC-mdoc

Identificador dos dados	Identificador do atributo	Formato de codificação
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Regulamento de Execução (UE) 2025/1569 da Comissão, de 29 de julho de 2025, que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante aos certificados eletrónicos qualificados de atributos e aos certificados eletrónicos de atributos fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome (JO L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, "CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates" (https://datatracker.ietf.org/doc/rfc9360/).

Identificador dos dados	Identificador do atributo	Formato de codificação
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate ou full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate ou full-date

— A notação do formato de codificação dos atributos especificados no quadro 6 deve utilizar os tipos de representação especificados no RFC 8610 ([3]), com os seguintes requisitos adicionais:

(a) As tstr devem ser codificadas em UTF-8;

(b) As tstr devem ser compatíveis com toda a gama Unicode;

(c) As tstr devem ter o comprimento máximo de 150 carateres;

(d) Deve ser codificada uma data, conforme especificado no RFC 8943 ([4]);

(e) Um atributo full-date deve ser interpretado como #6.1004(tstr), em que a tag 1004 se encontra especificada no RFC 8943;

(f) Um atributo tdate deve conter uma cadeia data-hora, tal como especificado no RFC 3339 ([5]);

(g) Um atributo full-date deve conter uma cadeia full-date, tal como especificado no RFC 3339, em conformidade com o RFC 8943;

(h) Salvo indicação em contrário, a representação de uma data nos atributos:

— não utilizará frações de segundos,

— não utilizará um desvio local em relação ao tempo universal coordenado e a compensação horária especificada no RFC 3339 deve ser definida como "Z";

(i) Um número inteiro com os tipos principais 0 e 1 deve ser o mais pequeno possível, conforme especificado no RFC 8949 ([6]), secção 4.2;

(j) Um place_of_birth deve conter pelo menos um dos seguintes pares chave-valor: "country", "region" ou "locality";

(k) A expressão do comprimento numa bstr, tstr, arranjo (*array*) ou mapa deve ser a mais pequena possível, tal como especificado no RFC 8949, secção 4.2;

([3]) C. Vigano e H. Birkholz, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, junho de 2019.
([4]) M. Jones, A. Nadalin e J. Richter, "Concise Binary Object Representation (CBOR) Tags for Date", RFC 8943, novembro de 2020.
([5]) G. Klyne e C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, julho de 2002.
([6]) C. Bormann e P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 8949, dezembro de 2020.

(l) O atributo nationality deve ser codificado como um arranjo de códigos de país alpha-2, tal como especificado na norma ISO 3166-1. Quando for utilizada a notação CDDL, conforme especificada no RFC 8610, a codificação deste atributo deve ser:

— nationalities = [+ CountryCode],

— CountryCode = tstr; código de país alpha-2 especificado na norma ISO 3166-1,

— quando um utente de carteira a quem os dados de identificação pessoal se referem tem várias nacionalidades e o fornecedor de dados de identificação pessoal certificar essas várias nacionalidades, este fornecedor pode incluir todas as nacionalidades nos dados de identificação pessoal,

— o atributo place_of_birth deve ser codificado como um tipo place_of_birth. Quando for utilizada a notação CDDL, conforme especificada no RFC 8610, a codificação deste atributo deve ser:

place_of_birth =

{

? 'country' : tstr ; um único código de país alpha-2, conforme especificado na norma ISO 3166-1

? 'region': tstr ; o nome de um estado, província, distrito ou zona local

? 'locality': tstr ; o nome de um município, cidade, vila ou aldeia

}.

4.2 Requisitos de codificação de dados de identificação pessoal em formato SD-JWT VC

— Os dados de identificação pessoal e os respetivos metadados especificados nesta secção devem ser incluídos nos dados de identificação pessoal enquanto declarações na aceção das especificações do formato SD-JWT VC.

— Todas as declarações dos dados de identificação pessoal emitidos, referidos no travessão anterior, devem ser seletivamente divulgadas de forma individual, exceto as declarações definidas como não seletivamente divulgáveis em formato SD-JWT VC.

— O quadro 7 especifica a codificação de nomes de declarações que são nomes públicos.

— O quadro 8 especifica a codificação dos nomes de declarações que são específicas dos dados de identificação pessoal.

— Uma cadeia JSON utilizada nos dados de identificação pessoal codificada em SD-JWT VC deve ser codificada em UTF-8 e ser compatível com toda a gama Unicode, salvo indicação explícita em contrário no quadro 8 abaixo ou nas referências nele contidas.

— As declarações JWT nbf e exp, tal como definidas no RFC 7519 ([7]) devem ser utilizadas para expressar o período de validade técnica dos dados de identificação pessoal, em conformidade com o formato SD-JWT VC.

([7]) J. Jones *et al.*, "JSON Web Token (JWT)", RFC 7519, maio de 2015.

— Os dados de identificação pessoal devem incorporar a declaração cnf tal como definido no RFC 7800 ([8]), que deve ser uma chave pública gerada a partir de uma chave privada armazenada no WSCD da unidade de carteira dos utentes.

— O cabeçalho protegido da assinatura digital que assina dados de identificação pessoal em formato SD-JWT VC deve conter os parâmetros de cabeçalho x5u e x5t#S256, ambos especificados no RFC 7515 ([9]).

Quadro 7

Requisitos de codificação dos dados de identificação pessoal em formato SD-JWT VC utilizando nomes públicos

Identificador dos dados	Identificador do atributo	Formato de codificação
`family_name`	`family_name`	cadeia
`given_name`	`given_name`	cadeia
`birth_date`	`birthdate`	cadeia, ISO 8601-1, formato AAAA--MM-DD
`birth_place`	`place_of_birth`	estrutura JSON
`nationality`	`nationalities`	arranjo de cadeias
`resident_address`	`address.formatted`	cadeia
`resident_country`	`address.country`	cadeia
`resident_state`	`address.region`	cadeia
`resident_city`	`address.locality`	cadeia
`resident_postal_code`	`address.postal_code`	cadeia
`resident_street`	`address.street_address`	cadeia
`family_name_birth`	`birth_family_name`	cadeia
`given_name_birth`	`birth_given_name`	cadeia
`email_address`	`email`	cadeia
`mobile_phone_number`	`phone_number`	cadeia
`portrait`	`picture`	cadeia; URL dos dados que contém um retrato com codificação base64 em formato JPEG

([8]) M. Jones *et al.*, "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)", RFC 7800, abril de 2016.
([9]) M. Jones *et al.*, "JSON Web Signature (JWS)", RFC 7515, maio de 2015.

Quadro 8

Requisitos de codificação dos dados de identificação pessoal em formato SD-JWT VC utilizando nomes privados

Identificador dos dados	Identificador do atributo	Formato de codificação
`expiry_date`	`date_of_expiry`	cadeia, ISO 8601-1, formato AAAA--MM-DD
`issuance_date`	`date_of_issuance`	cadeia, ISO 8601-1, formato AAAA--MM-DD
`personal_administrative_-number`	`personal_administrati-ve_number`	cadeia
`sex`	`sex`	número
`issuing_authority`	`issuing_authority`	cadeia
`issuing_country`	`issuing_country`	cadeia
`document_number`	`document_number`	cadeia
`issuing_jurisdiction`	`issuing_jurisdiction`	cadeia

— O tipo de base dos dados de identificação pessoal deve ser "urn:eudi:pid:1", incluído na declaração vct. Todos os dados de identificação pessoal devem utilizar tipos no espaço de nomes "urn:eudi:pid:".

— Quando os dados de identificação pessoal incluem atributos não especificados no presente anexo, esses atributos devem ser definidos dentro de um tipo nacional.

— Quando é utilizado o tipo nacional, o seu sistema, incluindo todos os identificadores de dados, as respetivas definições, presenças e formatos de codificação, deve ser definido num sistema publicado em conformidade com o artigo 8.º do Regulamento de Execução (UE) 2025/1569.

(5) Secção 5: Dados relativos à infraestrutura de confiança

A lista de fornecedores de dados de identificação pessoal disponibilizada pela Comissão em conformidade com o Regulamento de Execução (UE) 2024/2980 deve permitir a autenticação de dados de identificação pessoal.».

ANEXO II

«*ANEXO I-A*

Mecanismos criptográficos a que se refere o artigo 5.º-A

Grupo Europeu para a Certificação da Cibersegurança, subgrupo para a criptografia: "Agreed Cryptographic Mechanisms" (Mecanismos criptográficos acordados), documento publicado pela Agência da União Europeia para a Cibersegurança (ENISA) ([1]).».

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en?prefLang=pt.

ANEXO III

«ANEXO I-B

Especificações técnicas para os certificados de unidades de carteira a que se refere o artigo 6.º, n.º 2-A

(1) Um certificado de unidade de carteira deve incluir um ou mais certificados de instância de carteira e um ou mais certificados de chave.

(2) O certificado de instância de carteira e os certificados de chave devem cumprir os seguintes requisitos:

(a) Requisitos de formato

— FR-WIA-1: um certificado de instância de carteira deve ser um JSON Web Token (JWT), conforme especificado no RFC 7519 ([1]), que tenha sido assinado ou selado pelo fornecedor de carteiras através de uma assinatura JAdES básica B de caráter compacto.

— FR-WIA-1.1: um certificado de instância de carteira deve ser um certificado de carteira conforme especificado no apêndice E de "OpenID for Verifiable Credential Issuance v1.0" ([2]) (OID4VCI) e alargado conforme indicado, abaixo, em C-WIA-1 e C-WIA-2.

— FR-KA-1: um certificado de chave deve ser um JWT conforme especificado no RFC 7519, que tenha sido assinado ou selado pelo fornecedor de carteiras através de uma assinatura JAdES básica B de caráter compacto.

— FR_KA_1.1: um certificado de chave deve ser um certificado de chave conforme especificado no apêndice D da OID4VCI, alargado conforme especificado, abaixo, em C_KA-1 e C_KA-2;

(b) Requisitos de transporte

— TR-WIA-1: uma unidade de carteira deve utilizar um certificado de instância de carteira durante a emissão de dados de identificação pessoal, certificados eletrónicos qualificados ou não qualificados de atributos, ou certificados eletrónicos de atributos, fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome.

— TR-WIA-2: um fornecedor de carteiras deve verificar a integridade da instância de carteira e assinar ou selar o certificado de instância de carteira.

— TR-WIA-2.1: quando um fornecedor de carteiras emite um certificado de instância de carteira, a diferença entre a hora em que o fornecedor de carteiras verificou a integridade da instância de carteira e a hora que irá indicar no parâmetro de cabeçalho "exp" do certificado emitido deve ser inferior a 24 horas.

— TR-WIA-2.2: o fornecedor de carteiras deve assegurar que uma unidade de carteira contém os certificados de instância de carteira necessários para a emissão de dados de identificação pessoal e certificados eletrónicos de atributos.

— TR-WIA-3: durante a emissão, uma unidade de carteira deve enviar um certificado de instância de carteira ao servidor de autorização no pedido de autorização transmitido por envio seletivo (*pushed*) e no pedido de *token*, conforme especificado na OID4VCI.

— TR-WIA-3.1: uma unidade de carteira deve enviar o certificado de instância de carteira juntamente com uma prova de posse (PoP), conforme especificado no apêndice E da OID4VCI.

— TR-WIA-3.2: uma unidade de carteira deve enviar o mesmo certificado de instância de carteira para apenas um servidor de autorização.

([1]) RFC 7519: "JSON Web Token (JWT)", maio de 2015.
([2]) "OpenID for Verifiable Credential Issuance v1.0", https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: quando um fornecedor de carteiras utiliza a opção "per-issuer reuse" (reutilização por emitente) especificada, abaixo, em R_WIA_1, uma unidade de carteira pode enviar um certificado de instância de carteira para o mesmo servidor de autorização várias vezes.

— TR-WIA-3.2.2: quando um fornecedor de carteiras não utiliza a opção "per-issuer reuse", uma unidade de carteira deve utilizar um certificado de instância de carteira num só processo de emissão.

— TR-WIA-4: quando um servidor de autorização recebe um certificado de instância de carteira, deve verificar a assinatura do certificado de instância de carteira utilizando a chave pública no certificado de assinatura incluído no parâmetro "x5c" do cabeçalho JOSE do certificado de instância de carteira.

— TR-WIA-4.1: o servidor de autorização deve também verificar se este certificado de assinatura pode ser verificado com uma âncora de confiança na lista de fornecedores de carteiras referida no artigo 5.º do Regulamento de Execução (UE) 2024/2980, utilizando potencialmente certificados intermédios incluídos no parâmetro x5c.

— TR-WIA-4.2: o servidor de autorização deve verificar se o certificado de instância de carteira já expirou.

— TR-WIA-4.3: o servidor de autorização deve verificar a assinatura da PoP utilizando a chave pública existente na declaração "cnf".

— TR_KA-1: uma unidade de carteira deve utilizar um certificado de chave durante a emissão de dados de identificação pessoal e durante a emissão de certificados eletrónicos qualificados ou não qualificados de atributos associados a um dispositivo, ou certificados eletrónicos de atributos fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome.

— TR_KA-1.1: uma unidade de carteira não deve utilizar um certificado de chave durante a emissão de certificados eletrónicos qualificados ou não qualificados de atributos não associados a um dispositivo, ou certificados eletrónicos de atributos fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome.

— TR_KA-2: um fornecedor de carteiras deve fornecer uma unidade de carteira com diferentes certificados de chave para o WSCD da unidade de carteira e para cada um dos seus repositórios de chaves.

— TR_KA-2.1: o fornecedor de carteiras deve assinar ou selar um certificado de chave após verificar que as chaves certificadas no mesmo estão armazenadas no WSCD da unidade de carteira ou no repositório de chaves descrito no certificado de chave.

— TR_KA-2.2: um certificado de chave deve conter pelo menos uma chave pública certificada. O número de chaves no certificado de chave enviado a um emitente de credenciais não deve ultrapassar o tamanho máximo do lote especificado por esse emitente nos respetivos metadados de emitente de credenciais; consultar ETSI TS 119 472-3 ([3]), parâmetro "credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size".

— TR_KA-2.3: um fornecedor de carteiras deve incluir uma chave pública (correspondente a uma chave privada armazenada no WSCD ou repositório de chaves da unidade de carteira) num só certificado de chave.

— TR_KA-2.4: uma unidade de carteira deve utilizar um certificado de chave num só processo de emissão ou reemissão de credenciais.

— TR_KA-2.5: um fornecedor de carteiras deve assegurar que uma unidade de carteira possui os certificados de chave necessários para a emissão de dados de identificação pessoal e certificados eletrónicos de atributos associados a um dispositivo.

([3]) ETSI, "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles", ETSI TS 119 472-3, V1.1.1, março de 2026.

— TR_KA-3: quando necessário durante a emissão, uma unidade de carteira deve incluir um certificado de chave no campo "proofs" (provas) de um pedido de credenciais ao emitente de credenciais, conforme especificado na OID4VCI, numa prova do tipo "jwt" ou "attestation".

— TR_KA_3.1: quando uma unidade de carteira inclui um certificado de chave num elemento "jwt", deve assinar ou selar esse certificado utilizando a chave privada correspondente à chave pública no índice 0 do arranjo "attested_keys" no objeto "key_attestation".

— TR_KA-4: quando um emitente de credenciais emite credenciais associadas a um dispositivo, deve indicar no parâmetro "proof_types_supported" dos respetivos metadados de emitente de credenciais, conforme especificado na secção 12.2.4 da OID4VCI, que suporta tanto o tipo de prova "jwt" como "attestation" para certificados de chave que têm de incluir o objeto "key_attestations_required".

— TR_KA-4.1: quando um emitente de credenciais emite credenciais não associadas a um dispositivo, deve omitir os parâmetros "proof_types_supported" e "cryptographic_binding_methods_-supported" nos metadados de emitente de credenciais.

— TR_KA-5: quando um emitente de credenciais recebe um certificado de chave com um tipo de prova "jwt" ou "attestation", deve verificar a assinatura desse certificado utilizando a chave pública no certificado de assinatura incluído no parâmetro "x5c" do cabeçalho JOSE do certificado de chave e se este certificado de assinatura pode ser verificado com uma âncora de confiança na lista de fornecedores de carteiras referida no artigo 5.º do Regulamento de Execução (UE) 2024/2980, utilizando potencialmente certificados intermédios incluídos no parâmetro "x5c".

— TR_KA-6: quando um emitente de credenciais recebe um certificado de chave com um tipo de prova "jwt", deve verificar a assinatura do elemento "jwt" utilizando a chave no índice 0 do arranjo "attested_keys" no objeto "key_attestation" incluído no elemento "jwt".

— TR_KA-6.1: o emitente de credenciais deve verificar se o campo "nonce" do elemento "jwt" inclui um c_nonce válido do respetivo nonce_endpoint, conforme especificado na OID4VCI.

— TR_KA-7: quando um emitente de credenciais recebe um certificado de chave com um tipo de prova "attestation", deve verificar se o objeto "key_attestation" inclui um c_nonce válido do respetivo nonce_endpoint.

— TR_KA-8: um fornecedor de dados de identificação pessoal deve assegurar que esses dados estão associados a uma chave pública originária de um certificado de chave que mencione um WSCD;

(c) Requisitos de conteúdo

— C_WIA-1: um certificado de instância de carteira deve incluir o seguinte:

— a declaração "wallet_name" especificada no apêndice E da OID4VCI, onde o seu valor deve ser o identificador da solução de carteira que se encontra na lista de fornecedores de carteiras referida no artigo 5.º do Regulamento de Execução (UE) 2024/2980,

— uma declaração "wallet_version" ([4]), que deve ser uma cadeia cujo valor é a versão da solução de carteira,

— uma declaração "wallet_solution_certification_information", que deve ser um objeto JSON que contém informações sobre o organismo de avaliação da conformidade que certificou a solução de carteira, o número de certificação, conforme aplicável, e outros dados pertinentes sobre a certificação,

([4]) Esta declaração é definida neste regulamento de execução da Comissão e não faz parte da especificação da OID4VCI.

— uma declaração “client_status” com dois subcampos:

— “status”: uma referência à lista de estados, conforme especificado no apêndice E da OID4VCI, que representa o estado de revogação da instância de carteira. Consultar as informações pormenorizadas na secção (e) abaixo,

— “exp”: uma NumericDate, conforme especificado no RFC 7519, que define a hora até quando o fornecedor de carteiras irá manter o estado de revogação no índice da lista de estados indicado em “status”,

— a declaração “exp” especificada no apêndice E da OID4VCI.

— *NOTA*: a declaração “client_status.status” num certificado de instância de carteira representa o estado de revogação da instância de carteira e não o estado de revogação do próprio certificado. Tal como descrito, abaixo, em R_WIA-1, um fornecedor de carteiras pode optar por limitar o âmbito de cada certificado de instância de carteira a um servidor de autorização específico com base no facto de todos os certificados enviados a esse servidor conterem o mesmo valor de índice na entrada “client_status.status”.

— *NOTA*: o valor “idx” na declaração “status” pode ser utilizado como identificador único (por pares) da instância de carteira e da unidade de carteira.

— C_WIA-2: um certificado de instância de carteira deve também incluir a declaração “wallet_link” especificada no apêndice E da OID4VCI e o valor desta declaração deve ser um URI onde podem ser obtidas mais informações sobre a solução de carteira.

— C_WIA-3: um servidor de autorização não deve interpretar o parâmetro “exp” no nível superior de um certificado de instância de carteira como o final do período de manutenção da revogação da instância de carteira.

— *NOTA*: o parâmetro “exp” no nível superior de um certificado de instância de carteira indica a expiração do próprio certificado.

— C_KA-1: um certificado de chave deve incluir:

— As declarações “key_storage” e “user_authentication” especificadas no apêndice D da OID4VCI.

— Os atributos “key_storage” e “user_authentication” devem ter o valor “iso_18045_high” quando um certificado de chave menciona um WSCD.

— A declaração “certification” especificada no apêndice D da OID4VCI, contendo um URL onde é possível obter informações sobre a certificação alcançada pelo WSCD ou repositório de chaves, nomeadamente o sistema, como Common Criteria (Critérios Comuns) ou o GlobalPlatform, os requisitos avaliados, como o perfil de proteção aplicável, e o nível de avaliação.

— A partir destas informações, deve ser possível determinar se o armazenamento de chaves é um WSCD.

— Uma declaração “key_storage_status” com dois subcampos:

— “status”: uma referência à lista de estados, conforme especificado no apêndice D.1 da OID4VCI. O valor representa o estado da revogação do tipo de WSCD ou repositório de chaves utilizado para armazenar as chaves certificadas ou, na opção de índice per-key--attestation, o estado da revogação de um WSCD ou repositório de chaves de uma determinada unidade de carteira. Consultar, abaixo, R_KA_1 para obter informações sobre as opções de atribuição de índices disponíveis,

— “exp”: uma NumericDate, conforme especificado no RFC 7519, que define a hora até quando o fornecedor de carteiras irá manter o estado de revogação no índice da lista de estados indicado em “status”.

— A declaração “exp” especificada no apêndice D da OID4VCI.

— *NOTA* sobre o valor "idx" da declaração "key_storage_status.status" de um certificado de chave: quando o fornecedor de carteiras utiliza a opção "type-shared index" (consultar R_KA_1 abaixo), todos os certificados de chave para o mesmo tipo de WSCD ou repositório de chaves partilham o mesmo índice de lista de estados. Desta forma, o valor "idx" não é único por unidade de carteira. Pelo contrário, quando o fornecedor de carteiras utiliza a opção "per-key-attestation index", o valor "idx" é único para a unidade de carteira (ou único por pares por emitente de credenciais). Em todos os casos, contudo, um emitente de credenciais não deve utilizar o valor "idx" num certificado de chave como identificador de unidade de carteira, mas sim num certificado de instância de carteira.

— C_KA-2: quando um certificado de chave é enviado num tipo de prova "attestation", deve igualmente incluir um c_nonce válido, conforme especificado no Apêndice F.3 da OID4VCI.

— C_KA-3: um emitente de credenciais não deve interpretar o parâmetro "exp" no nível superior de um certificado de chave como o final do período de manutenção da revogação do WSCD ou repositório de chaves.

— *NOTA*: o parâmetro "exp" no nível superior de um certificado de chave indica a expiração do próprio certificado;

(d) Requisitos relativos ao ciclo de vida

— O presente anexo especifica os seguintes parâmetros de metadados do emitente de credenciais:

  — "preferred_client_status_period": OPTIONAL. Um número inteiro que especifica o período de manutenção do estado remanescente preferido do certificado de instância de carteira a ser apresentado pela unidade de carteira durante a emissão, em segundos. O período de manutenção do estado remanescente é definido como o valor de "client_status.exp" no certificado menos o tempo de receção do certificado,

  — "preferred_key_storage_status_period": OPTIONAL. Um número inteiro que especifica o período de manutenção do estado remanescente preferido do certificado de chave a ser apresentado pela unidade de carteira durante a emissão, em segundos. O período de manutenção do estado remanescente é definido como o valor "key_storage_status.exp" no certificado menos o tempo de receção do certificado.

— LC_WIA-1: um servidor de autorização pode comunicar as suas preferências para o período de manutenção do estado remanescente nos certificados de instância de carteira ao incluir o parâmetro de metadados "preferred_client_status_period" no respetivo ponto terminal dos metadados do emitente de credenciais, conforme especificado na secção 12.2.2 da OID4VCI.

  — LC_WIA-1.1: este campo deve ser colocado no nível superior dos metadados do emitente de credenciais.

— LC_WIA_2: um servidor de autorização não deve interpretar o parâmetro "exp" no nível superior de um certificado de instância de carteira como o final do período de manutenção da revogação da instância de carteira.

— LC_WIA_3: quando um fornecedor de carteiras assina ou sela um certificado de instância de carteira, deve manter o estado de revogação da instância de carteira relevante até o "wallet_instance_status.exp" indicado nesse certificado passar.

— LC_KA-1: quando é necessário um certificado de chave, um emitente de credenciais pode comunicar as suas preferências para o período de manutenção do estado remanescente nos certificados de chave ao incluir o parâmetro de metadados "preferred_key_storage_status_period" especificado acima no respetivo ponto terminal dos metadados do emitente de credenciais, conforme especificado na secção 12.2.2 da OID4VCI.

  — LC_KA-1.1: este campo deve ser colocado no objeto "key_attestations_required", conforme especificado na secção 12.2.4 da OID4VCI.

— LC_KA-2: um fornecedor de carteiras deve escolher o período de validade técnica dos certificados de chave que emite.

— LC_KA-3: quando um fornecedor de carteiras assina ou sela um certificado de chave, deve manter o estado de revogação do WSCD ou repositório de chaves pertinente até o "key_storage_status.exp" indicado nesse certificado passar.

— LC_GEN-1: um fornecedor de carteiras deve assegurar que uma unidade de carteira pode sempre apresentar certificados de unidades de carteira e certificados de chave cujos "client_status.exp" e "key_storage_status.exp" (respetivamente) sejam pelo menos 31 dias no futuro no momento da apresentação a um servidor de autorização ou emitente de credenciais.

— *NOTA*: tal garante que os fornecedores de dados de identificação pessoal possam confiar no encadeamento de revogações sem serem forçados a emitir dados de identificação pessoal de curta duração.

— LC_GEN-2: um fornecedor de carteiras deve assegurar que uma unidade de carteira obtém os metadados de emitente de credenciais durante a emissão.

  — LC_GEN_2.1: se um campo "preferred_key_storage_status_period" for incluído nestes metadados, a unidade de carteira deve enviar um certificado de chave com ("key_storage_status.exp" − hora atual) − "preferred_key_storage_status_period" o mais curto possível, mas sem ser negativo. Se tal certificado de chave não estiver disponível para a unidade de carteira, esta deve obter um novo a partir do fornecedor de carteiras que cumpre o requisito "key_storage_status.exp" − hora atual ≥ "preferred_key_storage_status_period".

  — LC_GEN_2.2: se um campo "preferred_client_status_period" for incluído nestes metadados, a unidade de carteira deve enviar um certificado de instância de carteira com ("client_status.exp" − hora atual) − "preferred_client_status_period" o mais curto possível, mas sem ser negativo. Se tal certificado de instância de carteira não estiver disponível para a unidade de carteira, esta deve solicitar um novo a partir do fornecedor de carteiras que cumpre o requisito "client_status.exp" − hora atual ≥ "preferred_client_status_period".

— LC_GEN-3: o período de validade técnica dos dados de identificação pessoal deve terminar antes do "client_status.exp" do certificado de instância de carteira e do "key_storage_status.exp" do certificado de chave enviado ao fornecedor de dados de identificação pessoal durante o processo de emissão.

— LC_GEN-4: um fornecedor de dados de identificação pessoal com um período de validade técnica de mais de 24 horas deve verificar o estado de revogação do certificado de instância de carteira e do certificado de chave recebidos durante a emissão, pelo menos, a cada 24 horas durante o período de validade técnica dos dados de identificação pessoal. Caso um deles esteja revogado, o fornecedor deve revogar esses dados de identificação pessoal;

(e) Requisitos de revogação

— R_GEN-1: um fornecedor de carteiras deve utilizar listas de estados de *token* (especificadas na lista de estados de *token* do IETF) como mecanismo de revogação para certificados de chave e certificados de instância de carteira, conforme especificado nos apêndices D e E, respetivamente, da OID4VCI.

— *NOTA*: para aumentar a escalabilidade das suas listas de estados, um fornecedor de carteiras pode utilizar as seguintes otimizações:

  — dividir a lista de estados em vários grupos, caso os fornecedores de carteiras tenham um número considerável de utentes e certificados emitidos. Existem diversas estratégias de agrupamento, por exemplo baseadas num determinado tamanho ou período de tempo. Cabe a cada fornecedor de carteiras escolher a estratégia de agrupamento. Poderão ser tidos em conta fatores como o tamanho da lista de estados para descarregamento e a privacidade do utente,

  — possuir várias listas de estados,

  — comprimir uma lista de estados para reduzir o seu tamanho.

— R_WIA-1: um fornecedor de carteiras pode atribuir o mesmo valor à declaração "idx" na declaração "client_status.status" em todos os certificados de instância de carteira que uma determinada unidade de carteira apresenta ao mesmo servidor de autorização. Esta opção chama-se "per-issuer reuse". Se esta opção for utilizada:

  — R_WIA-1.1: a unidade de carteira deve manter o estado do valor do índice que utilizou para cada servidor de autorização com que interagiu anteriormente e solicitar um certificado de instância de carteira com o mesmo valor de índice quando voltar a interagir com esse servidor de autorização.

  — R_WIA-1.2: quando um fornecedor de carteiras recebe um pedido de certificado de instância de carteira com um valor de índice específico, deve verificar se a unidade de carteira que está a fazer o pedido já recebeu esse valor de índice anteriormente, antes de emitir um novo certificado com o mesmo valor de índice.

  — R_WIA-1.3: a unidade de carteira não deve reutilizar o mesmo valor de índice para interações com diferentes servidores de autorização.

— *NOTA*: se for utilizada a opção "per-issuer reuse", o fornecedor de carteiras poderá determinar com quantos servidores de autorização uma unidade de carteira já interagiu e a frequência com que interage com cada um.

— R_WIA-2: na respetiva política de confidencialidade, um fornecedor de carteiras deve indicar se utiliza a opção "per-issuer reuse" para revogação de instâncias de carteira.

— R_WIA-3: quando um fornecedor de carteiras não utiliza a opção "per-issuer reuse", deve atribuir um valor de índice novo e não associável a cada certificado de instância de carteira que emite.

— R_WIA-4: quando é necessário revogar uma unidade de carteira, o fornecedor de carteiras deve revogar os valores de índice na declaração "client_status.status" em todos os certificados de instância de carteira associados a essa unidade.

— R_WIA-5: um fornecedor de carteiras deve ter em conta a escala da sua implantação e a arquitetura subjacente ao determinar o tamanho das suas listas de estados dos certificados de instância de carteira, assegurando que têm a dimensão suficiente para impedir a correlação e proteger a privacidade dos utentes. No mínimo, uma lista de estados deve, sempre que possível, estar associada a pelo menos 10 000 certificados.

— R_KA_1: um fornecedor de carteiras deve escolher uma das seguintes opções de atribuição de índices para a declaração "key_storage_status.status" num certificado de chave:

  — opção 1, denominada "type-shared index", em que todos os certificados de chave que atestam chaves armazenadas no mesmo tipo de WSCD ou repositório de chaves contêm o mesmo valor de índice em "key_storage_status.status",

  — opção 2, denominada "per-key-attestion index", em que um certificado de chave que atesta chaves armazenadas num determinado WSCD ou repositório de chaves contém um valor de índice único (por pares) em "key_storage_status.status".

— *NOTA*: quando um fornecedor de carteiras utiliza a opção 1, uma única ação de revogação invalida todos os certificados de chave do tipo afetado em todas as unidades de carteira. Além disso, como todos os certificados de chave para o mesmo tipo de WSCD ou repositório de chaves partilham o mesmo índice de lista de estados, o número de entradas de uma lista de estados de certificado de chave reflete o número de tipos de WSCD ou repositório de chaves suportados pelo fornecedor de carteiras e não o número de unidades de carteira implantadas. Por este motivo, os aspetos relativos à proteção da privacidade que justificam o tamanho mínimo da lista de estados para listas de estados de instâncias de carteira não se aplicam a listas de estados de certificados de chave ao abrigo da opção 1, desde que existam unidades de carteira suficientes a utilizar o mesmo tipo de WSCD ou repositório de chaves.

— *NOTA*: quando um fornecedor de carteiras utiliza a opção 2, cada índice representa o estado de revogação do WSCD ou repositório de chaves específico certificado nesse certificado de chave.

— *NOTA*: quando um fornecedor de carteiras utiliza a opção 2, também é possível revogar a pedido do utente um WSCD ou repositório de chaves específico.

— R_KA-2: quando um fornecedor de carteiras utiliza a opção 2, pode opcionalmente utilizar a opção "per--issuer reuse" descrita em R_WIA-1. Se o fornecedor de carteiras utilizar esta opção, os requisitos de R_WIA-1 a R_WIA-3 aplicam-se *mutatis mutandis*.

— R_KA-3: quando um fornecedor de carteiras utiliza a opção 2, deve ter em conta a escala da sua implantação e a arquitetura subjacente ao determinar o tamanho das suas listas de estados dos certificados de chave, assegurando que têm a dimensão suficiente para impedir a correlação e proteger a privacidade dos utentes. No mínimo, uma lista de estados deve, sempre que possível, estar associada a pelo menos 10 000 certificados de chave.

— R_KA-4: quando um fornecedor de carteiras utiliza a opção 1 ("type-shared index"), deve apenas revogar uma entrada "key_storage_status.status" se o tipo de WSCD ou repositório de chaves tiver uma vulnerabilidade de segurança;

(f) Requisitos de algoritmos de assinatura

— SA-1: para a assinatura de certificados de instância de carteira, certificados de chave, provas de posse conexas e listas de estados de *token*, deve ser utilizado um dos seguintes algoritmos:

— ES256 (ECDSA com SHA-256 e P-256)

— ES384 (ECDSA com SHA-384 e P-384)

— ES512 (ECDSA com SHA-512 e P-521)

— SA-2: um fornecedor de carteiras deve escolher qual dos algoritmos referidos em SA-1 vai utilizar.

— SA-3: um servidor de autorização ou um emitente de credenciais (conforme especificado na OID4VCI) deve suportar todos os algoritmos referidos em SA-1.».

ANEXO IV

«ANEXO II

Lista das normas a que se refere o artigo 8.º

Aplicam-se as especificações técnicas enumeradas nas cláusulas 2 a 6 da norma ETSI TS 119 472-1 V1.2.1 (2026-02). Devem ser lidas com as seguintes adaptações:

(1) 2.1 *Normative references* [Referências normativas]

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures" [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 1: descrição geral e estruturas de dados comuns].

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers" [Assinaturas eletrónicas e infraestruturas de confiança (ESI); perfis de certificados; parte 6: requisitos de perfis de certificados para fornecedores de dados de identificação pessoal, carteiras, certificados eletrónicos de atributos, certificados eletrónicos qualificados de atributos e certificados eletrónicos de atributos de organismos do setor público].

— [25] Lista de estados de *token* do IETF, draft-ietf-oauth-status-list-20: "Token Status List" [Lista de estados de *token*], 20 de abril de 2026.

(2) 4.2.11.1 *General requirements* [Requisitos gerais]

— EAA-4.2.11.1-06: quando um elemento de estado é utilizado para dados de identificação pessoal, certificados eletrónicos qualificados de atributos ou certificados eletrónicos de atributos fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome, deve indicar apenas se o certificado está ou não revogado e não deve suportar outros valores de estado, nomeadamente a suspensão.

— EAA-4.2.11.1-06.1: quando um certificado é revogado, esta revogação é permanente.

(3) 4.2.13 *EAA short-lived* [Certificados eletrónicos de atributos de curta duração]

— EAA-4.2.13-03: quando são emitidos certificados eletrónicos de atributos de curta duração com um período de validade de 24 horas ou menos, a revogação não é necessária.

(4) 4.6.3 *Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA)* [Requisitos para certificados eletrónicos de atributos da UE emitidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome (PuB-EAA)]

— PuB-EAA-4.6.2-03: nulo e sem efeito.

— Pub-EAA-4.6.2-04: nulo e sem efeito.

— PuB-EAA-4.6.3-03: a assinatura digital PuB-EAA deve conter o certificado qualificado que a suporta.

— PuB-EAA-4.6.3-04: o certificado qualificado que suporta a assinatura digital PuB-EAA deve cumprir os requisitos da cláusula 8 da norma ETSI TS 119 412-6 v1.1.1 e deve conter o QcType qcStatement, conforme definido na norma ETSI EN 319 412-5 v2.5.1, com o valor id-etsi-qct-eidaspsbeaa definido da seguinte forma:

id-etsi-qct-eidaspsbeaa IDENTIFICADOR DE OBJETO ::= { id-etsi-eidas2-qct-extensions 3 } -- Certificado referido no artigo 45.º-F, n.º 1, alínea b), que suporta a assinatura eletrónica qualificada ou selo eletrónico qualificado do organismo do setor público referido no artigo 3.º, ponto 46), do Regulamento (UE) n.º 910/2014.

(5) 5.2.10.1 *General requirements* [Requisitos gerais]

— EAA-5.2.10.1-04: nulo e sem efeito.

— EAA-5.2.10.1-05: nulo e sem efeito.

— EAA-5.2.10.1-06: o membro "status" pode conter o membro "status_list", conforme especificado na cláusula 6.2 do IEFT draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: nulo e sem efeito.

— EAA-5.2.10.1-08: nulo e sem efeito.

— EAA-5.2.10.1-09: nulo e sem efeito.

— EAA-5.2.10.1-10: nulo e sem efeito.

— EAA-5.2.10.1-11: nulo e sem efeito.

— EAA-5.2.10.1-12: nulo e sem efeito.

(6) 6.2.10.1 *General requirements* [Requisitos gerais]

— EAA-6.2.10.1-01: quando um certificado eletrónico de atributos em conformidade com ISO/IEC mdoc utiliza o mecanismo da lista de estados de certificados conforme estabelecido em EAA-6.2.10.1-02.2 ou o mecanismo da lista de revogação de certificados conforme estabelecido em EAA-6.2.10.1-02.3, o respetivo objeto de segurança móvel (MSO) deve conter a estrutura do estado conforme estabelecido em EAA-6.2.10.1-17, que contém as informações de revogação do MSO.

— EAA-6.2.10.1-01.1: durante a implementação do mecanismo da lista de identificadores, o elemento de estado deve conter o elemento identifier_list conforme estabelecido em EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: durante a implementação do mecanismo da lista de estados, o elemento de estado deve conter o elemento status_list conforme estabelecido em EAA-6.2.10.1-13.

— *NOTA*:

  — A estrutura de estado contém uma referência a uma lista de revogação do MSO.

  — A lista de revogação do MSO é uma estrutura COSE_Sign1 que indica se um MSO específico está revogado ou não.

  — A estrutura de estado contém todas as informações necessárias para o utilizador de carteira determinar se a lista de revogação do MSO é autêntica.

— EAA-6.2.10.1-02: o fornecedor de dados de identificação pessoal, o fornecedor de certificados eletrónicos qualificados de atributos ou o fornecedor de certificados eletrónicos de atributos fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome deve utilizar um dos seguintes métodos de revogação de dados de identificação pessoal, certificados eletrónicos qualificados de atributos ou certificados eletrónicos de atributos fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome:

— EAA-6.2.10.1-02.1: quando emite certificados eletrónicos de atributos de curta duração com um período de validade igual ou inferior a 24 horas, a revogação não é exigida.

— EAA-6.2.10.1-02.2: utilizar um mecanismo da lista de estados de certificados para codificar as informações de revogação como lista de estados.

— EAA-6.2.10.1-02.2.1: o mecanismo da lista de estados revoga um MSO caso o bit da posição dos bits definida pelo emitente no MSO esteja definido como verdadeiro na lista de estados.

— EAA-6.2.10.1-02.2.2: o mecanismo da lista de estados está indicado na especificação da lista de estados de *token* (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: utilizar um mecanismo de lista de revogação de certificados para codificar as informações de revogação como lista de identificadores.

— EAA-6.2.10.1-02.3.1: o mecanismo da lista de identificadores revoga um MSO caso o identificador definido pelo emitente no MSO esteja presente na mesma lista.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 e EAA-6.2.10.1-11 especificam o mecanismo da lista de identificadores, com base nos requisitos da especificação da lista de estados de *token*, incluindo os pontos comuns entre o mecanismo da lista de estados e da lista de identificadores.

— EAA-6.2.10.1-03: quando o elemento de estado é utilizado para dados de identificação pessoal, certificados eletrónicos qualificados de atributos ou certificados eletrónicos de atributos fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome, deve ser utilizado exclusivamente o estado "revoked".

— EAA-6.2.10.1-03.1: para uma lista de estados, tal implica que apenas devem ser utilizados os valores "valid" e "invalid", conforme indicado na especificação da lista de estados de *token*.

— EAA-6.2.10.1-03.2: para a lista de identificadores, apenas os MSO revogados, em oposição a MSO temporariamente suspensos, devem ser colocados na lista de identificadores.

— EAA-6.2.10.1-04: quando um MSO é revogado, esta revogação é permanente.

— EAA-6.2.10.1-05: a verificação da lista de revogação do MSO é facultativa para o utilizador de carteira e, se for o caso, deve respeitar os requisitos de verificação indicados na especificação da lista de estados de token e a especificação da estrutura de estado estabelecida em EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: quando um utilizador de carteira necessita de verificar o estado de revogação de dados de identificação pessoal ou de certificados eletrónicos de atributos, deve suportar tanto o mecanismo da lista de estados de certificados como o mecanismo da lista de revogação de certificados, conforme estabelecido em EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: identifier_list e status_list do MSO podem conter o elemento do certificado.

— EAA-6.2.10.1-06.1: quando o elemento do certificado está presente, deve conter um certificado com a chave pública que assinou ou selou o certificado de nível superior no elemento x5chain da estrutura da lista de revogação do MSO.

— EAA-6.2.10.1-06.1.1: a instância de utilizador de carteira deve utilizar esse certificado como âncora de confiança para a verificação do elemento x5chain da estrutura da lista de revogação do MSO.

— EAA-6.2.10.1-06.2: quando o elemento do certificado não está presente, o certificado de nível superior do elemento x5chain da estrutura da lista de revogação do MSO deve ser assinado ou selado pelo certificado utilizado para assinar o certificado do elemento x5chain do MSO.

— EAA-6.2.10.1-06.2.1: a instância de utilizador de carteira deve utilizar esse certificado como âncora de confiança para a verificação do elemento x5chain da estrutura da lista de revogação do MSO.

— EAA-6.2.10.1-07: deve ser implementada uma lista de revogação do MSO em conformidade com a especificação da lista de estados de *token* como um *token* da lista de estados no formato CWT.

— EAA-6.2.10.1-08: para a lista de revogação do MSO do mecanismo da lista de estados e da lista de identificadores, aplicam-se os seguintes requisitos:

  — a declaração exp deve estar presente,

  — a declaração ttl pode estar presente,

  — a declaração aggregation_uri da declaração IdentifierList ou StatusList pode estar presente e o fornecedor de dados de identificação pessoal, de certificados eletrónicos qualificados de atributos ou de certificados

eletrónicos de atributos fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome pode utilizar a declaração aggregation_uri para indicar o suporte ao mecanismo de agregação, conforme indicado na especificação da lista de estados de *token*,

— o CWT deve ser um objeto COSE_Sign1 que utiliza um dos seguintes algoritmos de assinatura para o cálculo da assinatura:

(a) "ES256" (ECDSA com curva NIST P-256 e SHA-256);

(b) "ES384" (ECDSA com curva NIST P-384 e SHA-384);

(c) "ES512" (ECDSA com curva NIST P-521 e SHA-512);

(d) "ESB256" (ECDSA com curva brainpoolP256r1 e SHA-256);

(e) "ESB384" (ECDSA com curva brainpoolP384r1 e SHA-384);

(f) "ESB512" (ECDSA com curva brainpoolP512r1 e SHA-512),

— o CWT deve conter o elemento x5chain no cabeçalho protegido que contém o certificado ou cadeia de certificados para verificar a assinatura da lista de revogação do MSO,

— a utilização alargada da chave do identificador de objeto indicado na especificação da lista de estados de *token* pode ser usada no certificado de assinatura da lista de estados e da lista de identificadores e as instâncias de utilizador de carteira podem suportar a utilização alargada da chave de identificadores de objeto indicados na especificação da lista de estados de *token* e, para o identificador de objeto, o fornecedor de certificados eletrónicos qualificados de atributos ou o fornecedor de certificados eletrónicos de atributos fornecidos por um organismo do setor público ou em seu nome não deve tornar crítico o campo de utilização alargada da chave ao usar o OID de utilização alargada da chave indicado na especificação da lista de estados de *token*.

— EAA-6.2.10.1-09: em derrogação dos requisitos da especificação da lista de estados de *token*, aplicam-se os seguintes requisitos ao mecanismo da lista de identificadores:

— o valor da declaração "type" deve ser "application/identifierlist+cwt",

— a declaração StatusList não deve estar presente no conjunto de declarações CWT,

— a estrutura IdentifierList definida em EAA-6.2.10.1-11 deve estar presente como declaração no conjunto de declarações CWT que utiliza a chave 65530.

— EAA-6.2.10.1-10: a estrutura IdentifierList deve ser uma estrutura CBOR com a seguinte CDDL:

```
IdentifierList = {

    'identifiers': { * Identifier => IdentifierInfo },

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: quando o identificador da estrutura IdentifierList está presente, o MSO que contém o identificador no elemento de estado é revogado.

— EAA-6.2.10.1-10.2: a declaração Aggregation_uri é indicada na secção 9.2 da especificação da lista de estados de *token*.

— EAA-6.2.10.1-10.3: o tipo de conteúdo da lista de identificadores deve ser "application/identifierlist+cwt", conforme estabelecido nos requisitos indicados na secção 8.2 da especificação da lista de estados de *token*.

— EAA-6.2.10.1-11: aplicam-se os seguintes requisitos ao elemento identifier_list no MSO (consultar EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: o elemento identifier_list é uma estrutura CBOR com a seguinte CDDL:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: para impedir que o identificador seja utilizado como uma correlação entre apresentações, deve ser único por MSO.

— EAA-6.2.10.1-12: aplicam-se os seguintes requisitos à lista de estados:

  — EAA-6.2.10.1-12.1: o elemento de bits na estrutura StatusList deve ser definido como 1.

— EAA-6.2.10.1-13: aplicam-se os seguintes requisitos ao elemento status_list no MSO (consultar EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: o elemento status_list deve seguir os requisitos da estrutura StatusListInfo conforme indicado na especificação da lista de estados de *token* e o elemento de certificado facultativo definido em EAA-6.2.10.1-06 deve ser adicionado.

  — EAA-6.2.10.1-13.2: para impedir que o índice de estado seja uma correlação entre apresentações, a combinação de índice de estado e URI deve ser única por MSO.

— EAA-6.2.10.1-14: o fornecedor de carteiras deve utilizar o segundo (EAA-6.2.10.1-02.2) ou o terceiro (EAA-6.2.10.1-02.3) dos métodos especificados em EAA-6.2.10.1-02 para a revogação de um certificado de instância de carteira (WIA) e para a revogação de um certificado de chave (KA).

— EAA-6.2.10.1-15: o fornecedor de carteiras deve implementar os mecanismos de revogação de certificados especificados em EAA-6.2.10.1-02 na sua solução de carteira.

— EAA-6.2.10.1-16: o fornecedor de dados de identificação pessoal e o fornecedor de certificados eletrónicos de atributos devem suportar tanto o mecanismo da lista de estados de certificação como o mecanismo da lista de revogação de certificados especificados em EAA-6.2.10.1-02 para verificar o estado de revogação de um certificado de instância de carteira (WIA) e de um certificado de chave (KA).

— EAA-6.2.10.1-17: a estrutura de estado no MSO deve ser uma estrutura CBOR com a seguinte CDDL:

```
Status = {
? 'identifier_list' : IdentifierListInfo,
? 'status_list' : StatusListInfo,
* tstr => RFU
    }».
```

ANEXO V

«ANEXO III

Especificações técnicas a que se refere o artigo 10.º

— Especificações técnicas:

  — cláusula 4.2.5 da norma ETSI TS 119 472-3 V1.1.1 (2026-03).».

ANEXO VI

O anexo IV é alterado do seguinte modo:

(1) O ponto 1 passa a ter a seguinte redação:

«1. Formato obrigatório das assinaturas ou dos selos:

a) PAdES (*PDF Advanced Electronic Signature*), conforme especificado na norma ETSI EN 319 142-1 V1.2.1 (2024-01); "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures" [Assinaturas eletrónicas e infraestruturas (ESI); assinaturas digitais PAdES; parte 1: blocos de construção e assinaturas de base PAdES].»;

(2) O ponto 3 passa a ter a seguinte redação:

«3. Interface de programação de aplicações:
ETSI TS 119 432 v1.3.1 (2026-03), cláusulas 6.4.3, A.6, A.7 e A.8.».

ANEXO VII

«*ANEXO VI*

Marca de confiança "UE" para a carteira de identidade digital a cores



»

ANEXO VIII

«*ANEXO VII*

Marca de confiança "UE" para a carteira de identidade digital a preto e branco



»

ANEXO IX

«ANEXO VIII

Dados da marca de confiança "UE" para a carteira de identidade digital

Dados	Descrição	Codificação	Estado
TrustMarkResourceURL	URL dos elementos gráficos da marca de confiança "UE" para a carteira de identidade digital e dos recursos informativos do utente na interface do utente da carteira.	URL	Obrigatório
ListOfCertifiedWalletsURL	URL da lista pública de soluções de carteira certificadas na UE conforme estabelecido no Regulamento de Execução (UE) 2025/849 [1].	URL	Obrigatório
ListOfCertifiedWalletsQRCode	*QR Code* (código QR) com as informações de ListOfCertifiedWalletsURL.	ISO-8859-1 *Byte mode QR code*	Facultativo
WalletSolutionInfoPageURL	URL da página de informação da solução de carteira certificada na lista de páginas de soluções de carteira certificadas do URL ListOfCertifiedWalletsURL completado com um "?" e o identificador WalletSolutionID da solução de carteira.	URL	Obrigatório
WalletSolutionInfoPageQRCode	*QR Code* com as informações de WalletSolutionInfoPageURL.	ISO-8859-1 *Byte mode QR code*	Facultativo
WalletVerifierToolURL*	URL do ponto terminal da ferramenta de verificação de carteiras */.well-known/openid--credential-issuer* utilizado para obter os metadados do fornecedor de certificados.	URL	Facultativo».

[1] Regulamento de Execução (UE) 2025/849 da Comissão, de 6 de maio de 2025, que estabelece as regras de execução do Regulamento (UE) n.o 910/2014 do Parlamento Europeu e do Conselho no respeitante à apresentação à Comissão e ao grupo de cooperação de informações destinadas à lista de carteiras europeias de identidade digital certificadas (JO L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj)

ANEXO X

O anexo II é alterado do seguinte modo:

(1) No anexo II, secção 1, ponto 1), a alínea i) passa a ter a seguinte redação:

«i) Um ou vários certificados conformes com a norma ETSI EN 319 412-2 V2.4.1 (2025-06) ou com a norma ETSI EN 319 412-3 V1.3.1 (2023-09) que possam ser utilizados para verificar a assinatura ou o selo criado pelo responsável pelo registo nos dados do registo e relativamente aos quais os dados de identificação certificados incluam o nome do responsável pelo registo e, se for caso disso, o número de registo desse responsável, conforme previsto nas alíneas c) e d), respetivamente;»;

(2) No anexo II, secção 2, ponto 1), a alínea h) passa a ter a seguinte redação:

«h) Um ou vários certificados conformes com a norma ETSI EN 319 412-2 V2.4.1 (2025-06) ou com a norma ETSI EN 319 412-3 V1.3.1 (2023-09) que possam ser utilizados para autenticar e validar os certificados de unidades de carteira emitidos pelo fornecedor de carteiras e relativamente aos quais os dados de identificação certificados incluam o nome e, se for caso disso, o número de registo do fornecedor de carteiras, conforme previsto nas alíneas a) e b), respetivamente;»;

(3) No anexo II, secção 3, ponto 1), a alínea h) passa a ter a seguinte redação:

«h) Um ou vários certificados conformes com a norma ETSI EN 319 412-2 V2.4.1 (2025-06) ou com a norma ETSI EN 319 412-3 V1.3.1 (2023-09) que possam ser utilizados para verificar a assinatura ou o selo criado pelo fornecedor de dados de identificação pessoal nos dados de identificação pessoal que disponibiliza e relativamente aos quais os dados de identificação certificados incluam o nome e, se for caso disso, o número de registo do fornecedor de dados de identificação pessoal, conforme previsto nas alíneas a) e b), respetivamente.»;

(4) No anexo II, secção 4, ponto 1), a alínea g) passa a ter a seguinte redação:

«g) Um ou vários certificados conformes com a norma ETSI EN 319 412-2 V2.4.1 (2025-06) ou com a norma ETSI EN 319 412-3 V1.3.1 (2023-09) que possam ser utilizados para verificar a assinatura ou o selo criado pelo fornecedor de certificados de acesso de utilizadores de carteiras no certificado de acesso que disponibiliza aos utilizadores de carteiras, com, se for caso disso, as informações necessárias para distinguir os certificados de acesso de utilizadores de carteiras de outros certificados.»;

(5) No anexo II, é aditada a secção 5 com a seguinte redação:

«5. Notificações de informações sobre os fornecedores de certificados de registo de utilizadores de carteiras

1. Os Estados-Membros devem facultar à Comissão as seguintes informações sobre os fornecedores de certificados de registo de utilizadores de carteiras:

a) O nome do fornecedor de certificados de registo de utilizadores de carteiras;

b) Se for caso disso, um número de registo do fornecedor de certificados de registo de utilizadores de carteiras;

c) O Estado-Membro em que o fornecedor de certificados de registo de utilizadores de carteiras está estabelecido;

d) O endereço de correio eletrónico e o número de telefone de contacto do fornecedor de certificados de registo de utilizadores de carteiras, para questões relacionadas com os certificados de registo que disponibiliza aos utilizadores de carteiras;

e) Se for caso disso, o URL da página Web do fornecedor de certificados de registo de utilizadores de carteiras que contém informações adicionais sobre o fornecedor e os certificados de registo que disponibiliza aos utilizadores de carteiras;

f) O URL da página Web que contém as políticas, os termos e as condições aplicáveis ao fornecimento e à utilização dos certificados de registo que disponibiliza aos utilizadores de carteiras;

g) Um ou vários certificados conformes com a norma ETSI EN 319 412-2 V2.4.1 (2025-06) ou com a norma ETSI EN 319 412-3 V1.3.1 (2023-09) que possam ser utilizados para verificar a assinatura ou o selo criado pelo fornecedor de certificados de registo de utilizadores de carteiras nos certificados de registo que disponibiliza aos utilizadores de carteiras, com, se for caso disso, as informações necessárias para distinguir os certificados de registo de utilizadores de carteiras de outros certificados.

2. As informações referidas no ponto 1) devem ser facultadas por fornecedor de certificados de registo de utilizadores de carteiras.».

ANEXO XI

«ANEXO I

Protocolos e interfaces a que se refere o artigo 4.º

Aplica-se a especificação ETSI TS 119 472-3 V1.1.1 (2026-03) com as seguintes adaptações:

(1) 4.1 *General requirements* [Requisitos gerais]

— GEN-REQ-4.1-05: nulo e sem efeito.

— *NOTA*: nulo e sem efeito.

(2) 4.2.3 *Provision of registration certificates of PID/EAA Provider to EUDI Wallet* [Fornecimento de certificados de registo de fornecedor de dados de identificação pessoal/certificados eletrónicos de atributos à carteira europeia de identidade digital]

— ISS-MDATA-REG_CERT-4.2.3-04: um dos elementos do parâmetro do arranjo issuer_info deve conter o certificado de registo do fornecedor de PID/EAA.

— ISS-MDATA-REG_CERT-4.2.3-07: nulo e sem efeito.

— ISS-MDATA-REG_CERT-4.2.3-08: nulo e sem efeito.

— ISS-MDATA-REG_CERT-4.2.3-09: nulo e sem efeito.

— ISS-MDATA-REG_CERT-4.2.3-10: nulo e sem efeito.

— ISS-MDATA-REG_CERT-4.2.3-11: nulo e sem efeito.

— ISS-MDATA-REG_CERT-4.2.3-12: nulo e sem efeito.

— ISS-MDATA-REG_CERT-4.2.3-13: nulo e sem efeito.

(3) 4.2.4.2 *ARF pre-defined PID/EAA reuse policy* [Política de reutilização de dados de identificação pessoal/certificados eletrónicos de atributos predefinidos da arquitetura e do regime de referência]

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: quando o membro id tem o valor “arf_annex_ii” e o arranjo mapeado para a etiqueta “details” contém o valor “once_only” ou “per-relying-party”, o objeto JSON que contém este arranjo para a etiqueta “details” deve igualmente conter um número JSON mapeado para a etiqueta “reissue_trigger_unused”.

(4) O anexo A não é aplicável.».

ANEXO XII

«ANEXO II

Especificações técnicas a que se refere o artigo 5.º

Aplicam-se as especificações técnicas no anexo C da norma ISO/IEC 18013-7:2025.

Aplicam-se as especificações técnicas das cláusulas 4.1, 4.2, 5 e 6 da norma ETSI TS 119 472-2 V1.2.1 (2026-03), com as seguintes adaptações, incluindo a adição de uma nova cláusula 4.3:

(1) 1 *Scope* [Âmbito]

— O presente documento especifica dois perfis de protocolos para permitir que os utilizadores (RP) solicitem apresentações de certificados eletrónicos de atributos (EAAP) ou dados de identificação pessoal (PID) à carteira europeia de identidade digital e para permitir que esta envie as EAAP/os PID solicitados ao RP. Cada um dos perfis suporta dois mecanismos de transmissão, nomeadamente com e sem mediação por IPA, conforme apresentado abaixo:

(a) Um perfil baseia-se em:

— ISO/IEC 18013-5 [10] apenas para mecanismos de transmissão sem mediação por IPA, e

— Anexo C da norma ISO/IEC 18013-7 [16] para mecanismos de transmissão com mediação por IPA.

Este perfil, denominado ISO/IEC-mdoc, está definido na cláusula 5 do presente documento;

(b) Um perfil baseia-se em:

OpenID4VC-HAIP [11] para mecanismos de transmissão com e sem mediação por IPA, da seguinte forma:

— secções 5, 5.1, 5.3, 7 e 8 de [11] para transmissão via reencaminhamentos ou para o mecanismo de transmissão sem mediação por IPA, e

— secções 5, 5.2, 5.3, 7 e 8 de [11] para o mecanismo de transmissão com mediação por IPA.

Este perfil, denominado OpenID4VC-HAIP, está definido na cláusula 6 do presente documento.

(2) 2.1 *Normative references* [Referências normativas]

— [15] ISO 639: "Language code" (Código de língua).

— [16] ISO/IEC 18013-7:2025 "Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions" [Identificação pessoal — ISO — carta de condução conforme — parte 7: funções suplementares da carta de condução móvel (mDL)].

(3) 4.1 *EAAP implementation based on SD-JWT VC* [Implementação de EAAP baseada em SD-JWT VC]

— EAAP-SD-JWT VC-04: nulo e sem efeito.

(4) 4.2 *EAAP implementation based on ISO/IEC-mdoc* [Implementação de EAAP baseada em ISO/IEC-mdoc]

— EAAP-ISO/IEC-mdoc-01: nulo e sem efeito.

— Note2: nulo e sem efeito.

— EAAP-ISO/IEC-mdoc-02: nulo e sem efeito.

(5) 4.3 *EAAP implementation with mediating API* [Implementação de EAAP com mediação por IPA]

— EAAP-API-GEN-01: a carteira europeia de identidade digital deve suportar uma IPA de mediação compatível com ambos os protocolos definidos na cláusula 5.2 de [11] e no anexo C de [16].

— *NOTA*: quando o dispositivo onde a carteira europeia de identidade digital está instalada não suporta ambos os protocolos, este requisito não pode ser cumprido e é acionada uma não conformidade porque os sistemas operativos e navegadores subjacentes não implementaram as funcionalidades de interoperabilidade necessárias.

— EAAP-API-GEN-02: a carteira europeia de identidade digital deve suportar uma IPA de mediação pelo menos para tipos de PID e EAA registados no catálogo de sistemas, conforme definido no Regulamento de Execução (UE) 2025/1569, e pelo menos para todos os formatos definidos no anexo II do Regulamento de Execução (UE) 2024/2979.

— *NOTA 1*: quando o sistema operativo, navegador, IPA de mediação ou qualquer outra camada técnica subjacente fora do controlo da carteira europeia de identidade digital restringe, filtra, pré-seleciona ou limita de outra forma os formatos da credencial, e os tipos de PID e EAA registados no catálogo de sistemas, este requisito não pode ser cumprido. Quando tal restrição impede a carteira europeia de identidade digital de suportar um tipo ou formato de credencial registado, a não conformidade resultante é atribuível à incapacidade desses sistemas operativos, navegadores, IPA de mediação ou outras camadas técnicas subjacentes pertinentes fornecerem as funcionalidades de interoperabilidade necessárias.

(6) 4.4 *Wallet-relying party validation and overasking checks* [Validação do utilizador de carteira e verificações de pedido excessivo de dados]

— WRP-VALIDATION-01: a carteira europeia de identidade digital deve validar o certificado de registo de utilizadores de carteiras recebido no pedido antes de apresentar quaisquer PID ou certificados eletrónicos de atributos solicitados ao utente de carteira para aprovação.

— WRP-VALIDATION-02: quando a validação do certificado de registo de utilizadores de carteiras falha, incluindo quando o certificado está expirado, revogado, incorreto, não foi emitido por um fornecedor de confiança válido de certificados de registo de utilizadores de carteiras ou não pode ser verificado criptograficamente, a carteira europeia de identidade digital deve avisar o utente de carteira de que não foi possível validar o utilizador de carteira e de que não irá apresentar o pedido como devidamente validado. O utente de carteira deve aprovar explicitamente o pedido do utilizador de carteira. A ausência de resposta ou casas previamente assinaladas não são suficientes para obter aprovação explícita.

— WRP-VALIDATION-03: o fornecedor de carteiras deve determinar, com base na sua análise de risco e política de segurança, se e em que condições determinadas verificações de validação falhadas podem ser contornadas pelo utente de carteira.

— WRP-OVERASKING-01: a carteira europeia de identidade digital deve comparar os certificados e atributos pedidos pelo utilizador de carteiras com os certificados e atributos registados no certificado de registo de utilizadores de carteiras.

— WRP-OVERASKING-02: quando o utilizador de carteiras solicita PID ou certificados eletrónicos de atributos ou declarações que não estão abrangidos pelo certificado de registo de utilizadores de carteiras, a carteira europeia de identidade digital deve avisar claramente o utente de carteira antes de qualquer divulgação. Este aviso deve indicar que o utilizador de carteiras está a solicitar mais informações do que aquelas que estão registadas. O utente de carteira deve aprovar explicitamente o pedido do utilizador de carteira. A ausência de resposta ou casas previamente assinaladas não são suficientes para obter aprovação explícita.

— WRP-OVERASKING-03: com base na sua análise de risco, política de segurança e lei aplicável, o fornecedor de carteiras deve determinar se o utente de carteira pode continuar apesar desse aviso, se apenas o subconjunto de dados solicitados abrangidos pelo certificado de registo pode ser divulgado ou se o pedido deve ser rejeitado.

(7) 5.1 *Introduction* [Introdução]

— A cláusula 5 e respetivas subcláusulas definem um perfil para um protocolo que permite a um RP solicitar EAAP ou PID à carteira europeia de identidade digital, e que permite que esta envie as EAAP/os PID solicitados ao RP que está a utilizar um mecanismo de transmissão sem mediação por IPA, baseado na norma ISO/IEC 18013-5 [10], ou um mecanismo de transmissão com mediação por IPA, baseado no anexo C da norma ISO/IEC 18013-7 [16], para transferir as estruturas de dados definidas na norma ISO/IEC 18013-5 [10] devidamente encapsuladas.

— O restante conteúdo da cláusula 5 está organizado da seguinte forma:

  — a cláusula 5.2 define os requisitos de suporte do perfil e dos mecanismos de transmissão por parte dos RP e da carteira europeia de identidade digital,

  — a cláusula 5.3 especifica os requisitos especificamente aplicáveis ao mecanismo de transmissão sem mediação por IPA,

  — a cláusula 5.4 e respetivas subcláusulas especificam os requisitos especificamente aplicáveis ao mecanismo de transmissão com mediação por IPA.

(8) 5.2 *Requirements on EUDI Wallet and RP support* [Requisitos de suporte da carteira europeia de identidade digital e do RP]

— ISO/IEC 18013-SUPPORT-01: as unidades de carteira, fornecedores de PID, fornecedores de certificados, fornecedores de carteiras e utilizadores não suportam a recuperação do servidor, conforme especificado na norma ISO/IEC 18013-5 [10] para solicitar e apresentar atributos de certificados ou PID.

— ISO/IEC 18013-SUPPORT-02: a carteira europeia de identidade digital deve cumprir os requisitos definidos nas cláusulas 5.3 e 5.4 do presente documento.

— ISO/IEC 18013-SUPPORT-04: um utilizador deve implementar o perfil definido na cláusula 5.4 do presente documento.

(9) 5.3.2 *ISO/IEC-mdoc EAAP Request contents* [Conteúdo do pedido de EAAP do ISO/IEC-mdoc]

— ISO/IEC 18013-5-REQ-04: os pedidos dos dispositivo enviados às carteiras europeias de identidade digital devem conter o par chave-valor "requestInfo" especificado na cláusula 8.3.2.1.2.1 de [10]. O valor deste par deve ser do tipo RequestInfo.

— ISO/IEC 18013-5-REQ-05: o tipo RequestInfo deve corresponder à definição CDDL apresentada abaixo.

```
RequestInfo = {

    'euWrprc': bstr ; contém um certificado de registo (ver requisitos abaixo)

}
```

— ISO/IEC 18013-5-REQ-06: o membro requestInfo referido deve conter um membro com a etiqueta "euWrprc".

— ISO/IEC 18013-5-REQ-07: o valor de "euWrprc" deve ser um certificado de registo com codificação CBOR.

— ISO/IEC 18013-5-REQ-08: nulo e sem efeito.

— NOTA 3: nulo e sem efeito.

— ISO/IEC 18013-5-REQ-09: nulo e sem efeito.

— ISO/IEC 18013-5-REQ-10: nulo e sem efeito.

— ISO/IEC 18013-5-REQ-11: nulo e sem efeito.

(10) 5.3.3 *ISO/IEC-mdoc EAAP Response profile* [Perfil de resposta de EAAP ISO/IEC-mdoc]

— A presente cláusula define os requisitos para o tipo de mensagem DeviceResponse, comum aos dois tipos de mecanismo de transmissão (com e sem mediação por IPA).

— *NOTA 1*: quando é utilizado um mecanismo sem mediação por IPA baseado na norma ISO/IEC 18013-5 [10], uma resposta EAAP é exatamente uma instância de DeviceResponse, conforme descrita na presente cláusula. Quando é utilizado um mecanismo com mediação por IPA baseado no anexo C da norma ISO/IEC 18013-7 [16], a instância DeviceRequest é encapsulada conforme especificado no anexo C de [16].

— ISO/IEC 18013-5-RESP-02: o fornecedor de dados de identificação pessoal e de certificados eletrónicos de atributos não deve incluir quaisquer elementos de dados no mapa KeyAuthorizations do objeto de segurança móvel dos dados de identificação pessoal e dos certificados eletrónicos de atributos que emite, exceto para elementos de dados fornecidos pelo utilizador de carteira nos dados transacionais do pedido mdoc a ser assinado ou selado pela unidade de carteira com recurso à chave privada dos dados de identificação pessoal ou certificados eletrónicos de atributos.

— *NOTA 2*: por conseguinte, as unidades de carteira não podem apresentar quaisquer elementos de dados assinados por um dispositivo a utilizadores de carteiras, exceto para assinar dados que o utilizador de carteira tenha fornecido, por exemplo para uma autenticação segura de utentes.

— *NOTA 3*: a norma ISO/IEC 18013-5:2021 não especifica como os utilizadores de carteiras podem incluir dados transacionais num pedido mdoc. A inclusão destes dados num pedido mdoc deve ocorrer com a adição de especificações técnicas.

— ISO/IEC 18013-5-RESP-03: os fornecedores de dados de identificação pessoal não devem permitir que a chave privada dos dados de identificação pessoal assine elementos de dados que são fornecidos pelo utilizador de carteira nos dados transacionais do pedido mdoc.

(11) 5.4 *Requirements for API mediated mechanism* [Requisitos do mecanismo com mediação por IPA]

5.4.1 *ISO/IEC 18013-7-related requirements* [Requisitos relacionados com a norma ISO/IEC 18013-7]

A presente cláusula define os requisitos para o mecanismo de transmissão com mediação por IPA relacionados com os requisitos definidos no anexo C de [16].

— ISO/IEC 18013-7-API-01: o perfil que apoia as apresentações com mediação por IPA deve cumprir os requisitos do anexo C da norma ISO/IEC 18013-7 [16], conforme descrito mais pormenorizadamente nas cláusulas 5.3 e 5.4 do presente documento.

— ISO/IEC 18013-7-API-02: todos os requisitos obrigatórios definidos no anexo C de [16] são aplicáveis conforme descrito mais pormenorizadamente nas cláusulas 5.3 e 5.4 do presente documento.

— ISO/IEC 18013-7-API-03: todos os requisitos facultativos definidos no anexo C de [16] permanecem facultativos salvo indicação em contrário no presente documento.

(12) 5.4.2 *Additional requirements* [Requisitos adicionais]

— A presente cláusula especifica os requisitos adicionais para o mecanismo de transmissão com mediação por IPA.

— ISO/IEC 18013-ADD-API-01: por defeito, a carteira europeia de identidade digital deve divulgar a presença de todos os tipos de certificados eletrónicos de atributos armazenados na IPA de mediação que opera em conformidade com o anexo C de [16], mas não deve divulgar os atributos e os respetivos valores nesses certificados eletrónicos de atributos.

— *NOTA 1*: a restrição relativa ao valor dos atributos aplica-se mesmo que essa divulgação possa melhorar os serviços fornecidos pelo sistema operativo à carteira europeia de identidade digital, por exemplo, a seleção de certificados no contexto da IPA de mediação.

— Existem considerações relacionadas com sistemas operativos e navegadores que estão fora do controlo dos responsáveis pela execução e que podem ser tidas em conta conforme indicado nas seguintes notas 2 a 4:

— *NOTA 2*: o navegador e/ou sistema operativo podem processar um pedido de apresentação de um utilizador que suporte o anexo C de [16] para pesquisar EAA disponíveis, impedir fraudes que tenham o utente como alvo ou para fins de resolução de problemas.

— *NOTA 3*: espera-se que um pedido de apresentação de um utilizador que suporte o anexo C de [16] seja processado pelo navegador e/ou sistema operativo para fins de segurança do utente.

— *NOTA 4*: espera-se que um pedido de apresentação de um utilizador que suporte o anexo C de [16] não seja processado pelo navegador e/ou sistema operativo para fins de análise do mercado (incluindo como objetivo secundário) ou para fins internos do navegador e/ou do sistema operativo.

— ISO/IEC 18013-ADD-API-02: quando, a pedido do utente, uma carteira europeia de identidade digital apaga PID ou EAA anteriormente divulgados à IPA de mediação que opera em conformidade com o anexo C de [16], deve indicar que já não armazena esses PID ou EAA à IPA de mediação.

— ISO/IEC 18013-ADD-API-03: se o utente desinstalar a sua carteira europeia de identidade digital, esta deve indicar à IPA de mediação que opera em conformidade com o anexo C de [16] que já não armazena quaisquer PID ou EAA anteriormente divulgados.

— ISO/IEC 18013-ADD-API-04: a carteira europeia de identidade digital deve disponibilizar uma definição de utente global que desative a divulgação de EAA armazenados através de uma IPA de mediação que opera conforme especificado na norma ISO/IEC 18013-ADD-API-01. Quando esta definição está desativada, a carteira não deve anunciar ou responder a pedidos de apresentação ou emissão mediados por IPA.

— ISO/IEC 18013-ADD-API-05: as carteiras europeias de identidade digital devem verificar nos fluxos entre dispositivos, utilizando a IPA de mediação, se o dispositivo em interação está fisicamente próximo da carteira europeia de identidade digital, recorrendo a um canal de comunicação local seguro, direto e mediado pelo utente, como um tecnologia de comunicação sem fios de curto alcance, para efetuar a verificação de proximidade física.

— *NOTA*: o CTAP 2.3 permite a utilização do *Bluetooth* de baixo consumo (BLE) para realizar a verificação de proximidade física e, quando implementado por ambos os dispositivos, permite igualmente o transporte dos dados entre os dispositivos por meio de tecnologias de transmissão de curto alcance. A execução da verificação de proximidade física e da transferência de dados entre os dois dispositivos utilizando um canal de comunicação local por via do CTAP 2.3 deve ser a opção privilegiada pelos sistemas operativos, navegadores, IPA de mediação ou qualquer outra camada técnica subjacentes fora do controlo da carteira europeia de identidade digital em detrimento da utilização de serviços de túnel CTAP híbrido.

(13) 6.2 *Requirements on EUDI Wallet and RP support* [Requisitos de suporte da carteira europeia de identidade digital e do RP]

— OIDFVP-HAIP-SUPPORT-02: a carteira europeia de identidade digital deve cumprir os requisitos especificados na cláusula 6.5 do presente anexo.

— OIDFVP-HAIP-SUPPORT-03: a carteira europeia de identidade digital não deve suportar o mecanismo baseado em reencaminhamentos especificado na cláusula 6.4 para fluxos de apresentação entre dispositivos.

— *NOTA 3*: a utilização deste mecanismo é vulnerável a ataques como de fixação de sessão. A mitigação destes ataques cabe aos utilizadores. A implementação deste mecanismo não deve desencadear uma não conformidade.

— OIDFVP-HAIP-SUPPORT-05: um RP deve cumprir os requisitos especificados na cláusula 6.5 do presente anexo.

— *NOTA 5*: nulo e sem efeito.

(14) 6.3.1 *General requirements* [Requisitos gerais]

— OIDFVP-HAIP-GEN-01: aplicam-se todos os requisitos obrigatórios especificados nas cláusulas 5, 5.3, 7 e 8 de HAIP [11].

— *NOTA 1*: a "secção 5 de HAIP [11]" refere-se apenas aos requisitos diretamente indicados sob o título da secção 5. Tal não inclui as secções 5.1, 5.2 e 5.3.

— OIDFVP-HAIP-GEN-03: se o presente anexo modificar um requisito da especificação OpenID4VC-HAIP [11], prevalece o requisito modificado especificado no presente anexo.

— *NOTA 2*: tal permitirá, por exemplo, tornar obrigatório um requisito facultativo da OpenID4VC-HAIP [11] ou alargar requisitos obrigatórios.

— OIDFVP-HAIP-GEN-04: quando o formato do certificado solicitado está em conformidade com [10], os RP e as carteiras europeias de identidade digital devem cumprir os requisitos do perfil "ISO mdocs" na secção 6 de [11].

— *NOTA 3*: por razões de clareza: o "perfil ISO mdocs" de HAIP implica que os RP e as carteiras europeias de identidade tenham de cumprir os requisitos aplicáveis de [7] Anexo B.2.

— OIDFVP-HAIP-GEN-05: quando o formato do certificado solicitado está em conformidade com [2], os RP e as carteiras europeias de identidade digital devem cumprir os requisitos do perfil "IETF SD-JWT VCs" na secção 6 de [11].

— *NOTA 4*: por razões de clareza: o "perfil IETF SD-JWT VCs" implica que os RP e as carteiras europeias de identidade tenham de cumprir os requisitos do anexo B.3 de [7], bem como os requisitos da secção 6.1 de [11].

(15) 6.3.2.1 *General requirements* [Requisitos gerais]

— OIDFVP-HAIP-COMMON-REQ-01: nulo e sem efeito.

(16) 6.3.2.2 *Requirements for the Request Object* [Requisitos para o objeto do pedido]

— OIDFVP-HAIP-COMMON-REQ-RO-02: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-03: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-04: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-05: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-06: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-07: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-08: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-09: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-10: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-11: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-12: nulo e sem efeito.

— *Nota 2*: nulo e sem efeito.

— OIDFVP-HAIP-COMMON-REQ-RO-13: um dos elementos do parâmetro verifier_info deve conter o certificado de registo.

— OIDFVP-HAIP-COMMON-REQ-RO-23: o certificado de entidade final referido na secção 5.9.3 de OpenID4VP para utilização com x509_hash Client Identifier Prefix deve ser um certificado de acesso do RP, conforme especificado na norma ETSI TS 119 475 [14].

(17) 6.3.3 *Authorization Response (EAAP response) profile* [Perfil de resposta de autorização (resposta de EAAP)]

— OIDFVP-HAIP-COMMON-RESP-01: nulo e sem efeito.

(18) 6.4.1 *General requirements* [Requisitos gerais]

— OIDFVP-HAIP-REDIRECTS-04: nulo e sem efeito.

— *NOTA*: nulo e sem efeito.

(19) 6.5.2 *Additional requirements* [Requisitos adicionais]

— OIDFVP-HAIP-ADD-API-01: por defeito, a carteira europeia de identidade digital deve divulgar a presença de todos os tipos de EAA armazenados na IPA de mediação que opera em conformidade com a cláusula 5.2 de [11], mas não deve divulgar os atributos e os respetivos valores nesses EAA.

— OIDFVP-HAIP-ADD-API-04: se a carteira europeia de identidade digital suportar uma IPA de mediação que opera conforme especificado em OIDFVP-HAIP-ADD-API-01, deve disponibilizar uma definição de utente global que desative a divulgação de EAA armazenados através da IPA de mediação. Quando esta definição está configurada para desativar a divulgação, a carteira deve subsequentemente permitir que o utente selecione os certificados individuais a divulgar à IPA de mediação.

— OIDFVP-HAIP-ADD-API-05: as carteiras europeias de identidade digital devem verificar nos fluxos entre dispositivos, utilizando a IPA de mediação, se o dispositivo em interação está fisicamente próximo da carteira europeia de identidade digital, recorrendo a um canal de comunicação local seguro, direto e mediado pelo utente, como um tecnologia de comunicação sem fios de curto alcance, para efetuar a verificação de proximidade física.

— *NOTA 5*: o CTAP 2.3 permite a utilização do BLE para realizar a verificação de proximidade física e, quando implementado por ambos os dispositivos, permite igualmente o transporte dos dados entre os dispositivos por meio de tecnologias de transmissão de curto alcance. A execução da verificação de proximidade física e da transferência de dados entre os dois dispositivos utilizando um canal de comunicação local por via do CTAP 2.3 deve ser a opção privilegiada pelos sistemas operativos, navegadores, IPA de mediação ou qualquer outra camada técnica subjacentes fora do controlo da carteira europeia de identidade digital em detrimento da utilização de serviços de túnel CTAP híbrido.

(20) 6.5.3 *Specific requirements when requesting ISO/IEC 18013-5 EAAP* [Requisitos específicos para pedidos de EAAP em conformidade com a ISO/IEC 18013-5]

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: todos os requisitos especificados neste documento que são aplicáveis às estruturas de pedido do dispositivo e resposta do dispositivo constantes da norma ISO/IEC 18013-5 aplicam-se igualmente quando a carteira europeia de identidade digital recebe um pedido de apresentação ISO/IEC mdoc através de um mecanismo com transmissão por IPA indicado na cláusula C.1 de [16].».