2026/1731

22.7.2026

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2026/1731 AL COMISIEI

din 15 iulie 2026

de modificare a Regulamentelor de punere în aplicare (UE) 2024/2977, (UE) 2024/2979, (UE) 2024/2980 și (UE) 2024/2982 în ceea ce privește standardele și specificațiile aplicabile

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE ([1]), în special articolul 5a alineatul (23),

întrucât:

(1) Pentru a asigura cel mai înalt nivel de armonizare între statele membre în ceea ce privește dezvoltarea portofelelor europene pentru identitatea digitală, specificațiile tehnice aferente portofelelor se întemeiază pe activitatea desfășurată pe baza Recomandării (UE) 2021/946 a Comisiei ([2]) și în special pe arhitectura și pe cadrul de referință. Întrucât arhitectura și cadrul de referință au evoluat semnificativ de la Regulamentele de punere în aplicare (UE) 2024/2977 ([3]), (UE) 2024/2979 ([4]), (UE) 2024/2980 ([5]) și (UE) 2024/2982 ([6]) ale Comisiei, respectivele regulamente de punere în aplicare ar trebui modificate acum pentru a le alinia la noile standarde, specificații și proceduri.

În conformitate cu obiectivele Regulamentului (UE) nr. 910/2014, au fost selectate o serie de standarde pentru a îndeplini aceste cerințe specifice. Aceste standarde ar trebui să reflecte practicile consacrate și să fie recunoscute pe scară largă în sectoarele relevante. De exemplu, întrucât formatul W3C VCDM este utilizat ca format de referință pentru atestate, în special în sectorul educațional, portofelele europene pentru identitatea digitală ar trebui, de asemenea, să sprijine acest format în momentul în care noile profiluri vor fi disponibile în formatul W3C VCDM. Dacă este necesar, aceste standarde ar trebui adaptate sau completate pentru a asigura securitatea și credibilitatea portofelelor europene pentru identitatea digitală, facilitând în același timp interoperabilitatea transfrontalieră și funcționarea eficace a pieței interne.

(2) Pentru orice utilizare a portofelului care necesită prezentarea portretului utilizatorului portofelului, soluțiile pentru portofel trebuie să sprijine funcționalitatea de divulgare selectivă, iar divulgarea trebuie să se afle sub controlul deplin al utilizatorului. Pentru a proteja capacitatea de a decide cu privire la divulgare, precum și portretul împotriva unei cereri neintenționate sau neautorizate de divulgare, proiectarea arhitecturală a portofelelor europene pentru identitatea digitală ar trebui să prevadă mecanisme de avertizare și înregistrarea tuturor tranzacțiilor legate de utilizarea portretului. Pentru a se asigura că utilizatorul portofelului are cunoștință de schimbul de date biometrice, avertismentele ar trebui să indice faptul că cererea implică schimbul de date biometrice și să solicite în mod specific

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

([2]) Recomandarea (UE) 2021/946 a Comisiei din 3 iunie 2021 privind un set de instrumente comun al Uniunii pentru o abordare coordonată în direcția unui cadru european al identității digitale (JO L 210, 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Regulamentul de punere în aplicare (UE) 2024/2977 al Comisiei din 28 noiembrie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește datele de identificare personală și atestatele electronice ale atributelor emise portofelelor europene pentru identitatea digitală (JO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([4]) Regulamentul de punere în aplicare (UE) 2024/2979 al Comisiei din 28 noiembrie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește integritatea și funcționalitățile de bază ale portofelelor europene pentru identitatea digitală (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([5]) Regulamentul de punere în aplicare (UE) 2024/2980 al Comisiei din 28 noiembrie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește notificările transmise Comisiei referitoare la ecosistemul portofelelor europene pentru identitatea digitală (JO L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

([6]) Regulamentul de punere în aplicare (UE) 2024/2982 al Comisiei din 28 noiembrie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește protocoalele și interfețele care vor fi suportate de cadrul pentru identitatea digitală europeană (JO L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

utilizatorului să confirme divulgarea. În cazul în care un beneficiar prelucrează portretul în scopul identificării unice a unei persoane fizice sau al confirmării identității declarate a persoanei respective, se aplică articolele 6 și 9 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([7]), precum și toate celelalte cerințe ale regulamentului respectiv, inclusiv faptul că prelucrarea portretului de către beneficiari ar trebui să se limiteze la ceea ce este necesar pentru utilizarea preconizată. Utilizarea preconizată ar trebui comunicată utilizatorului portofelului, împreună cu cererea de divulgare, într-un limbaj clar și inteligibil. Pentru a ține seama în mod corespunzător de sensibilitatea datelor biometrice, utilizatorul portofelului ar trebui să confirme în mod explicit și specific divulgarea portretului. Tăcerea sau căsuțele bifate în prealabil nu ar trebui considerate drept o confirmare din partea utilizatorului portofelului. Confirmarea explicită a utilizatorului portofelului ar trebui să fie o garanție tehnică și să nu ofere, în sine, un temei juridic pentru prelucrare. Astfel cum se prevede la articolul 9 alineatul (4) din Regulamentul (UE) 2016/679, statele membre pot menține sau introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea de date genetice, date biometrice sau date privind sănătatea.

(3) Pentru a acorda statelor membre suficient timp să își adapteze procedurile naționale, portretul utilizatorului portofelului poate face parte din datele obligatorii de identificare personală ale persoanei fizice numai începând cu 11 august 2028. În cazul în care aceste imagini provin din documente de identitate existente, cum ar fi cărți de identitate sau pașapoarte, se aplică cerințele relevante prevăzute în Regulamentele (UE) 2025/1208 ([8]) sau, respectiv, (CE) nr. 2252/2004 ([9]) ale Consiliului.

(4) Conform Regulamentului (UE) nr. 910/2014, portofelele trebuie să poată să afișeze o marcă de încredere a portofelului UE pentru identitatea digitală, ca un indiciu verificabil, simplu și ușor de recunoscut al faptului că un portofel a fost furnizat în conformitate cu regulamentul menționat. Utilizarea unei astfel de mărci de încredere va sprijini funcționarea eficace a pieței interne, va garanta concurența loială și va proteja interesele consumatorilor. Pentru a se permite utilizarea unei astfel de mărci de încredere, ar trebui stabilite caracteristicile vizuale și tehnice ale acesteia.

(5) Astfel cum se prevede la articolul 12b din Regulamentul (UE) nr. 910/2014, controlorii de acces trebuie să le permită furnizorilor de portofele europene pentru identitatea digitală și emitenților de mijloace de identificare electronică notificate interoperabilitatea efectivă cu aceleași caracteristici ale sistemului de operare, ale hardware-ului sau ale software-ului și, în scopul interoperabilității, accesul la acestea. O astfel de interoperabilitate efectivă și un astfel de acces efectiv trebuie să fie furnizate gratuit și indiferent dacă respectivele caracteristici hardware sau software fac parte din sistemul de operare, sunt disponibile pentru controlorul de acces respectiv sau sunt utilizate de acesta atunci când furnizează astfel de servicii. Întrucât toate soluțiile pentru portofel ar trebui să sprijine un set comun de protocoale și interfețe pentru a asigura utilizabilitatea, securitatea și interoperabilitatea în toate statele membre, controlorii de acces ar trebui să activeze caracteristicile sistemului de operare, ale hardware-ului sau ale software-ului necesare pentru punerea în aplicare a protocoalelor și a interfețelor prevăzute în anexa XII la prezentul regulament. În acest context, în fluxurile online între dispozitive, atât pentru verificarea proximității fizice, cât și pentru transferul de date între cele două dispozitive, controlorii de acces ar trebui să prefere un canal local de comunicare, astfel cum este activat în versiunea 2.3 a specificației CTAP ([10]) (*Client To Authenticator Protocol*), în locul utilizării serviciilor de tuneluri hibride ale protocolului CTAP.

(6) Pentru a acorda statelor membre, furnizorilor de certificate de înregistrare ale beneficiarilor portofelelor și furnizorilor de portofele suficient timp astfel încât să permită unităților de portofel să autentifice și să valideze certificatele de înregistrare ale beneficiarilor portofelelor, această cerință ar trebui să se aplice numai de la 11 august 2028.

(7) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului și, după caz, Directiva 2002/58/CE a Parlamentului European și a Consiliului ([11]) se aplică tuturor activităților de prelucrare a datelor cu caracter personal efectuate în temeiul prezentului regulament.

([7]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Regulamentul (UE) 2025/1208 al Consiliului din 12 iunie 2025 privind consolidarea securității cărților de identitate ale cetățenilor Uniunii și a documentelor de ședere eliberate cetățenilor Uniunii și membrilor de familie ai acestora care își exercită dreptul la liberă circulație (JO L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Regulamentul (CE) nr. 2252/2004 al Consiliului din 13 decembrie 2004 privind standardele referitoare la elementele de securitate și datele biometrice cuprinse în pașapoartele și documentele de călătorie eliberate de statele membre (JO L 385, 29.12.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Fido Alliance a propus standardul *Client to Authenticator Protocol* (CTAP), 26 februarie 2026.

([11]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([12]) și a emis un aviz la 17 aprilie 2026 ([13]).

(9) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului instituit prin articolul 48 din Regulamentul (UE) nr. 910/2014,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Modificări ale Regulamentului de punere în aplicare (UE) 2024/2977

Regulamentul de punere în aplicare (UE) 2024/2977 se modifică după cum urmează:

1. Se introduce următorul articol 3a:

„*Articolul 3a*

Protecția portretului

(1) Pe lângă cerințele de informare prevăzute în Regulamentul (UE) 2016/679, furnizorii de portofele se asigură că soluțiile pentru portofel pe care le oferă emit avertismente utilizatorilor portofelelor în cazul în care beneficiarii portofelelor solicită divulgarea portretului, indicând că cererea implică schimbul de date biometrice și necesită o confirmare pentru divulgarea selectivă a portretului.

(2) Pentru punerea în aplicare a divulgării selective a portretului către un beneficiar al portofelului, furnizorii de portofele se asigură că soluțiile pentru portofel impun utilizatorului portofelului să confirme în mod explicit și specific prezentarea portretului.

(3) Portretul nu se păstrează de către beneficiarii portofelelor, cu excepția cazului în care prelucrarea sa este necesară în scopul identificării și al autentificării în conformitate cu dreptul Uniunii privind protecția datelor sau în cazul în care acest lucru este prevăzut de dreptul Uniunii sau de dreptul intern, cu respectarea dreptului Uniunii privind protecția datelor. Portretul nu se transferă către țări terțe sau organizații internaționale, cu excepția cazului în care acest lucru este permis de legislația Uniunii privind protecția datelor.”

2. La articolul 4, alineatul (1) se înlocuiește cu următorul text:

„(1) Atestatele electronice ale atributelor emise unităților de portofel trebuie să respecte cel puțin unul dintre standardele prevăzute în anexa II la Regulamentul de punere în aplicare (UE) 2024/2979.”

3. La articolul 5, la alineatul (4), litera (b) se înlocuiește cu următorul text:

„(b) în cazul în care atestatul unității de portofel al unității de portofel către care au fost emise datele de identificare personală a fost revocat;”.

4. Anexa se înlocuiește cu textul prevăzut în anexa I la prezentul regulament.

([12]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) Observațiile formale ale AEPD cu privire la Proiectul de regulament de punere în aplicare în ceea ce privește standardele și specificațiile aplicabile și de rectificare a Regulamentului de punere în aplicare (UE) 2024/2980 |Autoritatea Europeană pentru Protecția Datelor.

Articolul 2

Modificări ale Regulamentului de punere în aplicare (UE) 2024/2979

Regulamentul de punere în aplicare (UE) 2024/2979 se modifică după cum urmează:

1. La articolul 3, alineatul (2) se elimină.

2. La articolul 5 alineatul (1), litera (a) se înlocuiește cu următorul text:

„(a) efectuează operațiuni criptografice pentru portofel care implică active critice stocate într-un dispozitiv criptografic securizat pentru portofel și care nu sunt solicitate pentru autentificarea utilizatorului portofelului numai în cazurile în care aplicațiile respective i-au autentificat cu succes pe utilizatorii portofelelor;”.

3. Se introduce următorul articol 5a:

„*Articolul 5a*

Mecanisme criptografice

În sensul articolului 4 alineatul (2), furnizorii de portofele utilizează numai mecanismele criptografice menționate în anexa Ia.”

4. Articolul 6 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) Furnizorii de portofele emit atestate ale unităților de portofel pentru fiecare unitate de portofel. Furnizorii de portofele semnează sau sigilează atestatele unității de portofel astfel încât semnăturile sau sigiliile să poată fi validate prin intermediul unui certificat enumerat în conformitate cu secțiunea 2 punctul 1 litera (h) din anexa II la Regulamentul de punere în aplicare (UE) 2024/2980.”;

(b) alineatul (2) se înlocuiește cu următorul text:

„(2) Furnizorii de portofele se asigură că atestatele unităților de portofel menționate la alineatul (1) respectă specificațiile tehnice prevăzute în anexa Ib.”;

(c) la alineatul (3), litera (b) se înlocuiește cu următorul text:

„(b) furnizează mecanisme securizate de identificare și autentificare pentru utilizatorii portofelelor care sunt independente de unitățile de portofel.”

5. La articolul 9 alineatul (2), litera (b) se înlocuiește cu următorul text:

„(b) numele, datele de contact și identificatorul unic al beneficiarului portofelului corespunzător și statul membru în care este stabilit beneficiarul portofelului;”.

6. La articolul 10, alineatul (1) se înlocuiește cu următorul text:

„(1) Furnizorii de portofele se asigură că atestatele electronice ale atributelor emise în conformitate cu specificațiile tehnice aplicabile pentru politicile comune de divulgare încorporate prevăzute în anexa III pot fi prelucrate de unitățile de portofel pe care le furnizează aceștia.”

7. Articolul 12 se modifică după cum urmează:

(a) la alineatul (2), litera (c) se înlocuiește cu următorul text:

„(c) creează semnături sau sigilii în conformitate cel puțin cu formatul obligatoriu de semnătură sau sigiliu menționat în anexa IV;”;

(b) alineatul (3) se înlocuiește cu următorul text:

„(3) Aplicațiile de creare a semnăturii pot să fie integrate în instanțele portofelelor sau să fie externe acestora.”;

(c) se introduce următorul alineat:

„(4) Aplicațiile de creare a semnăturii utilizate de unitățile de portofel trebuie să suporte cel puțin interfața de programare a aplicațiilor menționată în anexa IV.”

8. La articolul 14, alineatul (1) se elimină.

9. Se introduce următorul articol 14a:

„*Articolul 14a*

Marca de încredere a portofelului UE pentru identitatea digitală

(1) Furnizorii de portofele se asigură că unitățile de portofel afișează marca de încredere a portofelului UE pentru identitatea digitală. Marca de încredere a portofelului UE pentru identitatea digitală are formatul prevăzut în anexele VI și VII.

(2) Furnizorii de portofele se asigură că unitățile de portofel le permit utilizatorilor portofelelor să acceseze informații cu ajutorul cărora să poată verifica statutul certificării aferent soluției pentru portofel. În acest scop, furnizorii de portofele se asigură că, în urma înregistrării unei soluții pentru portofel, unitățile de portofel corespunzătoare includ URL-urile furnizate de Comisia Europeană pentru o astfel de verificare. Furnizorii de portofele se asigură că unitățile lor de portofel au acces la datele privind marca de încredere a portofelului UE pentru identitatea digitală care respectă specificațiile tehnice prevăzute în anexa VIII.

(3) Culorile de referință pentru marca de încredere a portofelului UE pentru identitatea digitală sunt Pantone nr. 661 și 116 sau albastru (100 % cyan + 67 % magenta + 0 % galben + 40 % negru) și galben (0 % cyan + 20 % magenta + 100 % galben + 0 % negru), atunci când se utilizează tetracromia; atunci când se utilizează culorile modelului cromatic RGB (roșu-verde-albastru), culorile de referință sunt albastru (0 roșu + 51 verde + 153 albastru) și galben (255 roșu + 204 verde + 0 albastru).

(4) Marca de încredere a portofelului UE pentru identitatea digitală poate fi utilizată în alb și negru, astfel cum se prevede în anexa VII, numai în cazul în care utilizarea culorilor nu este posibilă.

(5) În cazul în care marca de încredere a portofelului UE pentru identitatea digitală este utilizată pe un fond închis, aceasta poate fi utilizată în format negativ, folosind aceeași culoare de fond. În cazul în care marca de încredere a portofelului UE pentru identitatea digitală este utilizată în culori pe un fond colorat care îngreunează vizualizarea acesteia, se poate folosi o linie exterioară delimitativă în jurul mărcii de încredere a portofelului UE pentru identitatea digitală pentru a îmbunătăți contrastul cu culorile de fond.

(6) Marca de încredere a portofelului UE pentru identitatea digitală are o dimensiune minimă de 64 × 85 de pixeli la 150 dpi.

(7) Furnizorii de portofele se asigură că marca de încredere a portofelului UE pentru identitatea digitală este utilizată într-un mod care să permită indicarea clară a unității de portofel la care se referă marca de încredere a portofelului UE pentru identitatea digitală. Marca de încredere a portofelului UE pentru identitatea digitală poate fi asociată cu elemente grafice sau textuale care să indice în mod clar unitatea de portofel pentru care este utilizată, cu condiția ca acestea să nu modifice nici nivelul său de recunoaștere ca marcă de încredere a portofelului UE pentru identitatea digitală, nici asocierea cu lista portofelelor europene pentru identitatea digitală certificate menționată la articolul 5d din Regulamentul (UE) nr. 910/2014.

(8) În cazul în care furnizorii de portofele au revocat un atestat al unității de portofel, aceștia se asigură că marca de încredere a portofelului UE pentru identitatea digitală nu mai este afișată de unitatea de portofel corespunzătoare.”

10. Se adaugă anexele Ia și Ib, astfel cum se prevede în anexa II și în anexa III la prezentul regulament.

11. Anexa II se înlocuiește cu anexa IV la prezentul regulament.

12. Anexa III se înlocuiește cu anexa V la prezentul regulament.

13. Anexa IV se modifică în conformitate cu anexa VI la prezentul regulament.

14. Anexa V se elimină.

15. Textul din anexa VII la prezentul regulament se inserează ca anexa VI.

16. Textul din anexa VIII la prezentul regulament se inserează ca anexa VII.

17. Textul din anexa IX la prezentul regulament se inserează ca anexa VIII.

Articolul 3

Modificări ale Regulamentului de punere în aplicare (UE) 2024/2980

Regulamentul de punere în aplicare (UE) 2024/2980 se modifică după cum urmează:

1. La articolul 5, alineatul (2) se înlocuiește cu următorul text:

„(2) După caz, Comisia întocmește, actualizează și publică o listă care cuprinde informațiile notificate de statele membre cu privire la furnizorii de portofele, furnizorii de date de identificare personală, furnizorii de certificate de acces pentru beneficiarii portofelelor și furnizorii de certificate de înregistrare ale beneficiarilor portofelelor, astfel cum sunt menționate în anexa II secțiunile 2, 3, 4 și 5."

2. Anexa II la Regulamentul de punere în aplicare (UE) 2024/2980 se modifică în conformitate cu anexa X la prezentul regulament.

Articolul 4

Modificări ale Regulamentului de punere în aplicare (UE) 2024/2982

Regulamentul de punere în aplicare (UE) 2024/2982 se modifică după cum urmează:

1. La articolul 1, punctul 2 se înlocuiește cu următorul text:

„2. prezentarea atributelor datelor de identificare personală și a atestatelor electronice ale atributelor către beneficiarii portofelului;".

2. Articolul 3 se modifică după cum urmează:

(a) punctul 1 se înlocuiește cu următorul text:

„1. autentifică și validează certificatele de acces pentru beneficiarii portofelelor în cazul în care interacționează cu beneficiarii portofelelor fără a delega executarea acestor procese unui browser al sistemului de operare sau unei alte aplicații intermediare;";

(b) punctul 2 se elimină;

(c) punctul 3 se înlocuiește cu următorul text:

„3. autentifică și validează cererile adresate prin utilizarea certificatelor de acces pentru beneficiarii portofelului;";

(d) punctul 4 se înlocuiește cu următorul text:

„4. autentifică și validează certificatul de înregistrare al beneficiarului portofelului;";

(e) punctul 5 se înlocuiește cu următorul text:

„5. afișează pentru utilizatorii portofelului informațiile conținute în certificatele de acces pentru beneficiarii portofelului;";

(f) punctul 8 se elimină;

(g) punctul 9 se înlocuiește cu următorul text:

„9. nu prezintă niciun atribut solicitat beneficiarilor portofelului până când nu sunt finalizate următoarele etape:

(a) verificarea prelucrării politicilor încorporate de divulgare a informațiilor în cadrul unității de portofel în conformitate cu articolul 10 din Regulamentul de punere în aplicare (UE) 2024/2979;

(b) verificarea aprobării parțiale sau integrale a prezentării de către utilizatorii portofelelor."

3. La articolul 4, alineatul (1) se înlocuiește cu următorul text:

„(1) Furnizorii de portofele se asigură că soluțiile pentru portofel suportă protocoalele și interfețele prevăzute în anexa I pentru emiterea de date de identificare personală și de atestate electronice ale atributelor către unitățile de portofel."

4. Articolul 5 se modifică după cum urmează:

   (a) alineatele (1) și (2) se înlocuiesc cu următorul text:

   „(1) Furnizorii de portofele se asigură că soluțiile pentru portofel suportă protocoalele și interfețele pentru prezentarea atributelor către beneficiarii portofelului, la distanță și, după caz, în proximitate, în conformitate cu specificațiile tehnice prevăzute în anexa II.

   (2) Furnizorii de portofele se asigură că, la cererea utilizatorilor, unitățile de portofel răspund cererilor autentificate și validate cu succes din partea beneficiarilor portofelului menționate la articolul 3, în conformitate cu specificațiile tehnice prevăzute în anexa II.”;

   (b) alineatul (5) se elimină.

5. Articolul 8 se înlocuiește cu următorul text:

„*Articolul 8*

Intrare în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Articolul 3 alineatul (4) se aplică începând cu 11 august 2028.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.”

6. Anexa se elimină.

7. Textul din anexa XI la prezentul regulament se adaugă ca anexa I.

8. Textul din anexa XII la prezentul regulament se adaugă ca anexa II.

Articolul 5

Intrare în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 15 iulie 2026.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

„ANEXĂ

Specificații tehnice pentru datele de identificare personală menționate la articolul 3 alineatul (3)

1. Secțiunea 1: Set de date de identificare a persoanelor fizice

Tabelul 1

Date de identificare personală obligatorii pentru persoanele fizice în vederea divulgării selective

Identificator al datelor	Definiție
`family_name`	Numele actual al utilizatorului la care se referă datele de identificare personală.
`given_name`	Prenumele actual, inclusiv al doilea prenume, al(e) utilizatorului la care se referă datele de identificare personală.
`birth_date`	Ziua, luna și anul în care s-a născut utilizatorul la care se referă datele de identificare personală.
`birth_place`	Țara, sub forma unui cod de țară alfa-2, astfel cum este indicat în standardul ISO 3166-1, sau statul, provincia, districtul sau regiunea ori municipalitatea, orașul sau satul în care s-a născut utilizatorul la care se referă datele de identificare personală.
`nationality`	Unul sau mai multe coduri de țară alfa-2, astfel cum sunt indicate în standardul ISO 3166-1, reprezentând cetățenia utilizatorului la care se referă datele de identificare personală.
`portrait`	Cu excepția situației în care utilizatorul optează în mod explicit să nu includă portretul, după caz, imaginea facială a utilizatorului la care se referă datele de identificare personală, conformă cu cerințele de calitate pentru un tip de imagine frontală completă, astfel cum se prevede în standardul ISO/IEC 39794-5, sau, în ceea ce privește compatibilitatea inversă, în clauzele 8.2, 8.3 și 8.4 din standardul ISO/IEC 19794-5, furnizată sub formă de date codificate ale imaginii fără antetele sau blocurile specificate în clauza 5 din standardul ISO/IEC 19794-5, cu excepția datelor imaginii în sine (în format JPEG), se aplică după 11 august 2028.

— Statele membre pot prevedea ca utilizatorul să aibă opțiunea de a refuza introducerea portretului în datele de identificare personală.

— Statele membre se asigură că divulgarea selectivă se aplică fiecărui identificator de date, inclusiv portretului.

— În cazul în care data nașterii persoanei fizice nu este cunoscută, statele membre aleg valori adecvate care respectă specificațiile stabilite în secțiunile 4.1 sau 4.2 (după caz) din prezenta anexă.

— În cazul în care cetățenia persoanei fizice este necunoscută, statele membre utilizează valoarea «QU».

— În cazul în care persoana fizică nu deține cetățenia niciunei țări, statele membre utilizează valoarea «QS».

— În cazul în care utilizatorul optează să nu includă portretul, statele membre setează valoarea ca fiind necompletată.

Tabelul 2

Date de identificare personală opționale pentru persoanele fizice în vederea divulgării selective

Identificator al datelor	Definiție
`resident_address`	Adresa completă a locului în care utilizatorul la care se referă datele de identificare personală își are în prezent reședința sau la care poate fi contactat (numele străzii, numărul locuinței, orașul etc.).
`resident_country`	Țara în care își are în prezent reședința utilizatorul la care se referă datele de identificare personală, sub forma unui cod de țară alfa-2, astfel cum este indicat în standardul ISO 3166-1.
`resident_state`	Statul, provincia, districtul sau regiunea în care își are în prezent reședința utilizatorul la care se referă datele de identificare personală.
`resident_city`	Municipalitatea, orașul sau satul în care își are în prezent reședința utilizatorul la care se referă datele de identificare personală.
`resident_postal_code`	Codul poștal al localității în care își are în prezent reședința utilizatorul la care se referă datele de identificare personală.
`resident_street`	Numele străzii pe care își are în prezent reședința utilizatorul la care se referă datele de identificare personală, inclusiv numărul locuinței și orice afix sau sufix al acesteia.
`personal_administrative_-number`	O valoare atribuită utilizatorului la care se referă datele de identificare personală, care este unică între toate numerele administrative personale emise de furnizorul de date de identificare personală. În cazul în care aleg să includă acest atribut, statele membre trebuie să descrie în sistemele lor de identificare electronică în cadrul cărora sunt emise datele de identificare personală politica pe care o aplică în ceea ce privește valorile acestui atribut, inclusiv, după caz, condițiile specifice pentru prelucrarea acestei valori.
`family_name_birth`	Numele utilizatorului la care se referă datele de identificare personală la naștere.
`given_name_birth`	Prenumele, inclusiv al doilea prenume, al(e) utilizatorului la care se referă datele de identificare personală la naștere.
`sex`	Valorile corespund uneia dintre următoarele variante: 0 = necunoscut; 1 = bărbătesc; 2 = femeiesc; 3 = altul; 4 = intersexual; 5 = divers; 6 = deschis; 9 = nu se aplică. Pentru valorile 0, 1, 2 și 9 se aplică standardul ISO/IEC 5218.
`email_address`	Adresa de e-mail a utilizatorului la care se referă datele de identificare personală [în conformitate cu RFC 5322 ([1])].

Identificator al datelor	Definiție
`mobile_phone_number`	Numărul de telefon mobil al utilizatorului la care se referă datele de identificare personală, începând cu simbolul „+” ca prefix internațional și codul de țară, urmat numai de cifre.

([1]) P. Resnick, Ed., «Internet Message Format» (Formatul mesajelor transmise pe internet), RFC 5322, octombrie 2008.

2. Secțiunea 2: Set de date de identificare a persoanelor juridice

Tabelul 3

Date de identificare personală obligatorii pentru persoanele juridice

Identificator al datelor
denumirea oficială actuală
un identificator unic creat de către statul membru expeditor în conformitate cu specificațiile tehnice în scopul identificării transfrontaliere și care are o durată de viață cât mai lungă posibil

— În cazul în care un identificator de date nu este cunoscut pentru persoana respectivă sau nu poate fi emis în alt mod în cadrul setului de date de identificare personală, statele membre utilizează ca alternativă o valoare a atributului care corespunde situației.

Tabelul 4

Date de identificare personală opționale pentru persoanele juridice

Identificator al datelor
adresa actuală
codul de înregistrare în scopuri de TVA
codul de identificare fiscală
identificatorul unic european menționat în Directiva (UE) 2017/1132 a Parlamentului European și a Consiliului ([1])
identificatorul entității juridice (LEI) menționat în Regulamentul de punere în aplicare (UE) 2022/1860 al Comisiei ([2])
numărul de înregistrare și identificare a operatorilor economici (EORI) menționat în Regulamentul de punere în aplicare (UE) nr. 1352/2013 al Comisiei ([3])
codul de acciză prevăzut la articolul 2 punctul 12 din Regulamentul (UE) nr. 389/2012 al Consiliului ([4])

([1]) Directiva (UE) 2017/1132 a Parlamentului European și a Consiliului din 14 iunie 2017 privind anumite aspecte ale dreptului societăților comerciale (JO L 169, 30.6.2017, p. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Regulamentul de punere în aplicare (UE) 2022/1860 al Comisiei din 10 iunie 2022 de stabilire a standardelor tehnice de punere în aplicare pentru aplicarea Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului în ceea ce privește standardele, formatele, frecvența, metodele și modalitățile de raportare (JO L 262, 7.10.2022, p. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Regulamentul de punere în aplicare (UE) nr. 1352/2013 al Comisiei din 4 decembrie 2013 de stabilire a formularelor prevăzute de Regulamentul (UE) nr. 608/2013 al Parlamentului European și al Consiliului privind asigurarea respectării drepturilor de proprietate intelectuală de către autoritățile vamale (JO L 341, 18.12.2013, p. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Regulamentul (UE) nr. 389/2012 al Consiliului din 2 mai 2012 privind cooperarea administrativă în domeniul accizelor și de abrogare a Regulamentului (CE) nr. 2073/2004 (JO L 121, 8.5.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. Secțiunea 3: Set de metadate referitoare la datele de identificare personală

Tabelul 5

Metadate referitoare la datele de identificare personală

Identificator al datelor	Definiție	Prezență
`issuing_authority`	Numele autorității administrative care a emis datele de identificare personală sau codul de țară alfa-2 al statului membru conform standardului ISO 3166, dacă nu există o autoritate separată abilitată să emită date de identificare personală.	obligatorie
`issuing_country`	codul de țară alfa-2, astfel cum este indicat în standardul ISO 3166-1, al țării sau al teritoriului furnizorului de date de identificare personală.	obligatorie
`expiry_date`	Data (și, dacă este posibil, ora) la care va expira perioada de valabilitate administrativă a datelor de identificare personală.	opțională
`document_number`	Un număr pentru datele de identificare personală, atribuit de furnizorul de date de identificare personală.	opțională
`issuing_jurisdiction`	Codul de subdiviziune al țării al jurisdicției care a emis datele de identificare personală, astfel cum este indicat în standardul ISO 3166-2:2020, clauza 8. Prima parte a codului este aceeași cu valoarea pentru țara emitentă.	opțională
`issuance_date`	Data și, dacă este posibil, ora la care a început perioada de valabilitate administrativă a datelor de identificare personală.	opțională

4. Secțiunea 4: Codificarea atributelor datelor de identificare a persoanelor fizice

— Datele de identificare a persoanelor fizice se emit în conformitate cu standardele prevăzute în anexa II la Regulamentul de punere în aplicare (UE) 2024/2979, clauzele 5 (formatul SD-JWTVC) și 6 (formatul ISO/IEC-mdoc) aplicabile atestatelor electronice ale atributelor. Clauzele 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 și 6.2.5 nu se aplică.

— Codificarea datelor de identificare a persoanelor fizice respectă specificațiile tehnice din secțiunile 4.1 și 4.2 din prezenta anexă.

4.1. Codificarea datelor de identificare a persoanelor fizice în format ISO/IEC-mdoc

— Tipul de atestare pentru datele de identificare personală în format ISO/IEC-mdoc este «eu.europa.ec.eudi.pid.1». Identificatorul spațiului de nume pentru atributele datelor de identificare personală prevăzute în prezenta anexă este «eu.europa.ec.eudi.pid.1».

— În cazul în care datele de identificare personală includ date pentru care identificatorii de date nu sunt prevăzuți în prezenta anexă, datele respective sunt definite într-un spațiu de nume intern pentru date de identificare personală care utilizează formatul general eu.europa.ec.eudi.pid.[codul de țară ISO 3166-1 alfa-2 sau codul de regiune ISO 3166-2], urmat de un punct opțional și de un număr de versiune.

— În cazul în care se utilizează spațiul de nume intern, schema acestuia, inclusiv toți identificatorii de date, definițiile, prezența și formatele de codificare ale acestora, se publică în conformitate cu articolul 8 din Regulamentul de punere în aplicare (UE) 2025/1569 al Comisiei ([1]).

— Datele de identificare personală și metadatele acestora prevăzute în secțiunile 1 și 3 din prezenta anexă se includ în elementele de date de identificare personală în sensul specificațiilor privind formatul ISO/IEC-mdoc.

— Membrul deviceKey din cadrul membrului deviceKeyInfo al instanței de tipul MobileSecurityObject trebuie să conțină o cheie publică.

— Cheia publică respectivă corespunde unei chei private stocate în dispozitivul criptografic securizat pentru portofel («WSCD») al utilizatorului portofelului.

— Antetul protejat al semnăturii digitale CB-AdES care semnează datele de identificare personală în format ISO/IEC-mdoc conține parametrii antetului x5u și x5t, ambii specificați în RFC 9360 ([2]).

— Algoritmul digest utilizat în parametrul antetului x5t este SHA-256.

— Cerințele privind codificarea datelor de identificare personală în format ISO/IEC-mdoc sunt prevăzute în tabelul 6:

Tabelul 6

Cerințe privind codificarea datelor de identificare personală în format ISO/IEC-mdoc

Identificator al datelor	Identificator de atribute	Format de codificare
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]) Regulamentul de punere în aplicare (UE) 2025/1569 al Comisiei din 29 iulie 2025 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește atestatele electronice calificate ale atributelor și atestatele electronice ale atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism (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» [Semnarea și criptarea obiectelor CBOR (COSE): parametrii antetului pentru includerea și referențierea certificatele X.509] (https://datatracker.ietf.org/doc/rfc9360/).

Identificator al datelor	Identificator de atribute	Format de codificare
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate sau 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 sau full-date

— Notarea formatului de codificare al atributelor specificate în tabelul 6 utilizează tipurile de reprezentare prevăzute în RFC 8610 ([3]), cu următoarele cerințe suplimentare:

(a) un atribut tstr se codifică în UTF-8;

(b) un atribut tstr este compatibil cu întregul interval unicode;

(c) un atribut tstr are o lungime maximă de 150 de caractere;

(d) o dată se codifică astfel cum se specifică în RFC 8943 ([4]);

(e) o dată completă se interpretează ca #6.1004(tstr), unde tag 1004 este cea specificată în RFC 8943;

(f) un atribut tdate conține un șir dată-oră, astfel cum se specifică în RFC 3339 ([5]);

(g) un atribut full-date conține un șir full-date, astfel cum se specifică în RFC 3339, în conformitate cu RFC 8943;

(h) o reprezentare a unei date în atribute, cu excepția cazului în care se indică altfel:

— nu utilizează fracțiuni de secunde;

— nu utilizează o compensare locală din UTC, iar compensarea temporală specificată în RFC 3339 se setează la «Z»;

(i) un număr întreg cu tipurile majore 0 și 1 trebuie să fie cât mai mic posibil, astfel cum se specifică în RFC 8949 ([6]), secțiunea 4.2;

(j) un atribut place_of_birth conține cel puțin una dintre următoarele perechi de valori cheie: «country», «region» sau «locality»;

(k) exprimarea lungimii într-un atribut bstr, tstr, într-o serie sau într-o hartă trebuie să fie cât mai scurtă posibil, astfel cum se specifică în RFC 8949, secțiunea 4.2;

([3]) C. Vigano și H. Birkholz, «Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures» [Limbajul concis de definire a datelor (CDDL): o convenție de notare pentru exprimarea structurilor de date de reprezentare concisă a obiectelor binare (CBOR) și JSON], RFC 8610, iunie 2019.

([4]) M. Jones, A. Nadalin și J. Richter, «Concise Binary Object Representation (CBOR) Tags for Date» [Etichete de reprezentare concisă a obiectelor binare (CBOR) pentru dată], RFC 8943, noiembrie 2020.

([5]) G. Klyne și C. Newman, «Date and Time on the Internet: Timestamps» (Data și ora pe internet: mărci temporale), RFC 3339, iulie 2002.

([6]) C. Bormann și P. Hoffman, «Concise Binary Object Representation (CBOR)» (Reprezentare concisă a obiectelor binare), RFC 8949, decembrie 2020.

(l) atributul naționalitate se codifică ca o serie de coduri de țară alfa-2, astfel cum se specifică în ISO 3166-1. În cazul în care se utilizează notația CDDL specificată în RFC 8610, codificarea acestui atribut este:

— nationalities = [+ CountryCode];

— CountryCode = tstr; codul țării alfa-2 specificat în ISO 3166-1;

— în cazul în care un utilizator al portofelului la care se referă datele de identificare personală are mai multe cetățenii, iar furnizorul de date de identificare personală atestă aceste cetățenii multiple, furnizorul de date de identificare personală poate include toate cetățeniile în datele de identificare personală;

— atributul place_of_birth se codifică drept tip place_of_birth. În cazul în care se utilizează notația CDDL specificată în RFC 8610, codificarea acestui atribut este:

place_of_birth =

{

? «country»: tstr ; un singur cod al țării alfa-2 specificat în ISO 3166-1

? «region»: tstr ; numele unui stat, al unei provincii, al unui district sau al unei zone locale

? «locality»: tstr ; numele unei localități, al unui oraș, al unui oraș sau al unui sat

}

4.2. Cerințe privind codificarea datelor de identificare personală în format SD-JWT VC

— Datele de identificare personală și metadatele acestora specificate în prezenta secțiune se includ în datele de identificare personală ca afirmații în sensul specificațiilor privind formatul SD-jwt VC.

— Toate afirmațiile din datele de identificare personală emise, menționate la liniuța anterioară, trebuie să poată fi divulgate în mod selectiv în mod individual, cu excepția acelor afirmații definite ca nedivulgabile în mod selectiv în format SD-jwt VC.

— Tabelul 7 specifică codificarea numelor de afirmații care sunt denumiri publice.

— Tabelul 8 specifică codificarea numelor de afirmații care sunt specifice datelor de identificare personală.

— Un șir JSON utilizat în datele de identificare personală codificate în SD-JWT VC trebuie să fie codificat în UTF-8 și trebuie să fie compatibil cu întregul interval de caractere Unicode, cu excepția cazului în care se specifică altfel în mod explicit în tabelul 8 de mai jos sau în trimiterile la acesta.

— Afirmațiile jwt nbf și exp, astfel cum sunt definite în RFC 7519 ([7]), se utilizează pentru a exprima perioada de valabilitate tehnică a datelor de identificare personală care respectă formatul SD-JWT VC.

([7]) J. Jones, et al., «JSON Web Token (JWT)» [Tokenul web JSON (JWT)], RFC 7519, mai 2015.

— Datele de identificare personală includ afirmația cnf, astfel cum este definită în RFC 7800 ([8]), care este o cheie publică generată de o cheie privată stocată în WSCD-ul unității de portofel a utilizatorilor portofelului.

— Antetul protejat al semnăturii digitale care semnează datele de identificare personală în format SD-JWT VC trebuie să conțină parametrii de antet x5u și x5t#S256 specificați în RFC 7515 ([9]).

Tabelul 7

Cerințe privind codificarea datelor de identificare personală în format SD-JWT VC utilizând nume publice

Identificator al datelor	Identificator de atribute	Format de codificare
`family_name`	`family_name`	șir de caractere
`given_name`	`given_name`	șir de caractere
`birth_date`	`birthdate`	șir, ISO 8601-1, format AAAA-LL-ZZ
`birth_place`	`place_of_birth`	structura JSON
`nationality`	`nationalities`	serie de șiruri
`resident_address`	`address.formatted`	șir de caractere
`resident_country`	`address.country`	șir de caractere
`resident_state`	`address.region`	șir de caractere
`resident_city`	`address.locality`	șir de caractere
`resident_postal_code`	`address.postal_code`	șir de caractere
`resident_street`	`address.street_address`	șir de caractere
`family_name_birth`	`birth_family_name`	șir de caractere
`given_name_birth`	`birth_given_name`	șir de caractere
`email_address`	`email`	șir de caractere
`mobile_phone_number`	`phone_number`	șir de caractere
`portrait`	`picture`	șir de caractere; date URL conținând un portret codificat base64 în format JPEG

([8]) M. Jones, et al., «Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)» (Semantica cheii reprezentând dovada deținerii pentru tokenurile web JSON), RFC 7800, aprilie 2016.
([9]) M. Jones, et al., «JSON Web Signature (JWS)» [Semnătura web JSON (JWS)], RFC 7515, mai 2015.

Tabelul 8

Cerințe privind codificarea datelor de identificare personală în format SD-JWT VC utilizând nume private

Identificator al datelor	Identificator de atribute	Format de codificare
`expiry_date`	`date_of_expiry`	șir, ISO 8601-1, format AAAA-LL-ZZ
`issuance_date`	`date_of_issuance`	șir, ISO 8601-1, format AAAA-LL-ZZ
`personal_administrative_number`	`personal_administrative_number`	șir de caractere
`sex`	`sex`	număr
`issuing_authority`	`issuing_authority`	șir de caractere
`issuing_country`	`issuing_country`	șir de caractere
`document_number`	`document_number`	șir de caractere
`issuing_jurisdiction`	`issuing_jurisdiction`	șir de caractere

— Tipul de bază al datelor de identificare personală este «urn:eudi:pid:1», inclus în afirmația vct. Toate datele de identificare personală utilizează tipuri în spațiul de nume «urn:eudi:pid:».

— În cazul în care datele de identificare personală includ atribute care nu sunt specificate în prezenta anexă, aceste atribute sunt definite în cadrul unui tip intern.

— În cazul în care se utilizează tipul intern, sistemul acestuia, inclusiv toți identificatorii de date, definițiile acestora, prezența și formatele de codificare se definesc în cadrul unui sistem care este publicat în conformitate cu articolul 8 din Regulamentul de punere în aplicare (UE) 2025/1569.

5. Secțiunea 5: Detalii privind infrastructura de încredere

Lista furnizorilor de date de identificare personală pusă la dispoziție de Comisie în conformitate cu Regulamentul de punere în aplicare (UE) 2024/2980 permite autentificarea datelor de identificare personală.”

ANEXA II

„ANEXA Ia

Mecanismele criptografice menționate la articolul 5a

Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia: «Mecanisme criptografice convenite», publicat de Agenția Uniunii Europene pentru Securitate Cibernetică («ENISA») ([1]).”

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

ANEXA III

„ANEXA Ib

Specificații tehnice pentru atestatele unităților de portofel menționate la articolul 6 alineatul (2a)

1. Un atestat al unității de portofel cuprinde unul sau mai multe atestate ale instanței portofelului și unul sau mai multe atestate ale cheii.

2. Atestatul instanței portofelului și atestatele cheilor îndeplinesc următoarele cerințe:

   (a) Cerințe privind formatul

   — FR-WIA-1: un atestat al instanței portofelului este un token web JSON (JWT), astfel cum se specifică în RFC 7519 ([1]), semnat sau sigilat de furnizorul de portofel prin intermediul semnăturii B de referință compacte JAdES.

   — FR-WIA-1.1: un atestat al instanței portofelului este un atestat al portofelului, astfel cum se specifică în apendicele E la specificațiile OpenID pentru emiterea de acreditări verificabile v1.0 ([2]) («OID4VCI») și se extinde astfel cum se specifică la C-WIA-1 și C-WIA-2 de mai jos.

   — FR-KA-1: un atestat al cheii este un JWT, astfel cum se specifică în RFC 7519, semnat sau sigilat de furnizorul de portofel prin intermediul semnăturii B de referință compacte JAdES.

   — FR_KA_1.1: un atestat al cheii este un atestat al cheii, astfel cum se specifică în apendicele D la OID4VCI, prelungit astfel cum se specifică în C_KA-1 și C_KA-2 mai jos.

   (b) Cerințe privind transportul

   — TR-WIA-1: o unitate de portofel utilizează un atestat al instanței portofelului în timpul emiterii datelor de identificare personală, a atestatelor electronice calificate sau necalificate ale atributelor sau a atestatelor electronice ale atributelor furnizate de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism.

   — TR-WIA-2: un furnizor de portofel verifică integritatea instanței portofelului și semnează sau sigilează atestatul instanței portofelului.

   — TR-WIA-2.1: în cazul în care un furnizor de portofel emite un atestat al instanței portofelului, diferența dintre momentul în care furnizorul de portofel a verificat integritatea instanței portofelului și momentul pe care îl va indica în parametrul antetului «exp» al atestatului instanței portofelului emis este mai mică de 24 de ore.

   — TR-WIA-2.2: furnizorul de portofel se asigură că o unitate de portofel conține atestate ale instanței portofelului necesare pentru emiterea datelor de identificare personale și atestate electronice ale atributelor.

   — TR-WIA-3: în timpul emiterii, o unitate de portofel trimite către serverul de autorizare un atestat al instanței portofelului în cererea de autorizare împinsă și în solicitarea de token, astfel cum se specifică în OID4VCI.

   — TR-WIA-3.1: o unitate de portofel trimite atestatul instanței portofelului împreună cu o dovadă a deținerii («PoP»), astfel cum se specifică în apendicele E la OID4VCI.

   — TR-WIA-3.2: o unitate de portofel trimite același atestat al instanței portofelului unui singur server de autorizare.

([1]) RFC 7519: «*JSON Web Token (JWT)*» [Tokenul web JSON (JWT)], mai 2015.
([2]) OpenID pentru emiterea de acreditări verificabile v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: în cazul în care un furnizor de portofel utilizează opțiunea «per-issuer reuse» specificată în R_WIA_1 de mai jos, o unitate de portofel poate trimite de mai multe ori un atestat al instanței portofelului aceluiași server de autorizare.

— TR-WIA-3.2.2: în cazul în care un furnizor de portofel nu utilizează opțiunea «per-issuer reuse», o unitate de portofel utilizează un atestat al instanței portofelului în cel mult un proces de emitere.

— TR-WIA-4: în cazul în care un server de autorizare primește un atestat al instanței portofelului, acesta verifică semnătura atestatului instanței portofelului utilizând cheia publică din certificatul pentru semnare inclus în parametrul «x5c» din antetul JOSE al atestatului instanței portofelului.

— TR-WIA-4.1: serverul de autorizare verifică, de asemenea, dacă acest certificat de semnătură poate fi verificat cu o ancoră de încredere pe lista furnizorilor de portofele menționată la articolul 5 din Regulamentul de punere în aplicare (UE) 2024/2980, eventual utilizând certificatele intermediare incluse în parametrul x5c.

— TR-WIA-4.2: serverul de autorizare verifică dacă atestatul instanței portofelului nu a expirat.

— TR-WIA-4.3: serverul de autorizare verifică semnătura PoP cu cheia publică prezentă în afirmația «cnf».

— TR_KA-1: o unitate de portofel utilizează un atestat al cheii în timpul emiterii datelor de identificare personală și în timpul emiterii atestatelor electronice calificate sau necalificate ale atributelor legate de un dispozitiv sau a atestatelor electronice ale atributelor furnizate de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism.

— TR_KA-1.1: o unitate de portofel nu utilizează un atestat al cheii în timpul emiterii atestatelor electronice calificate sau necalificate ale atributelor nelegate de un dispozitiv sau a atestatelor electronice ale atributelor furnizate de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism.

— TR_KA-2: un furnizor de portofel furnizează unei unități de portofel diferite atestate ale cheilor pentru WSCD-ul unității de portofel și pentru fiecare dintre depozitele sale de chei.

— TR_KA-2.1: furnizorul de portofel semnează sau sigilează un atestat al cheii, după ce a verificat dacă cheile atestate în atestatul cheii sunt stocate în WSCD-ul unității de portofel sau al depozitului de chei descris în atestatul cheii.

— TR_KA-2.2: un atestat al cheii conține cel puțin o cheie publică atestată. Numărul de chei din atestatul cheii trimis unui emitent de acreditări nu ar trebui să depășească dimensiunea maximă a lotului specificată de emitentul de acreditări respectiv în metadatele sale privind emitentul de acreditări; a se vedea ETSI TS 119 472-3 ([3]), parametrul «credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size.

— TR_KA-2.3: un furnizor de portofel include o cheie publică (care corespunde unei chei private stocate în WSCD sau în depozitul de chei al unității de portofel) în cel mult un atestat al cheii.

— TR_KA-2.4: o unitate de portofel utilizează un atestat cu cheie în cel mult un proces de emitere sau de reemitere a acreditărilor.

— TR_KA-2.5: furnizorul de portofel se asigură că o unitate de portofel deține atestate ale cheilor necesare pentru emiterea datelor de identificare personală și atestate electronice ale atributelor legate de un dispozitiv.

([3]) ETSI, «Semnături electronice și infrastructuri (ESI); Semnături digitale în format JAdES; Partea 3: Niveluri JAdES și profiluri de referință», ETSI TS 119 472-3, V1.1.1, martie 2026.

— TR_KA-3: dacă este necesar în timpul emiterii, o unitate de portofel include un atestat al cheii în câmpul «proofs» al unei solicitări de acreditare adresate emitentului de acreditări, astfel cum se specifică în OID4VCI, într-o dovadă de tipul «jwt» sau de tipul «attestation».

— TR_KA_3.1: în cazul în care o unitate de portofel include un atestat al cheii într-un element «jwt», aceasta semnează sau sigilează atestatul cheii utilizând cheia privată corespunzătoare cheii publice de la indexul 0 al seriei «attested_key» din cadrul obiectului «key_atattestation».

— TR_KA-4: în cazul în care un emitent de acreditări emite acreditări legate de un dispozitiv, acesta indică în parametrul «proof_types_supported» din metadatele acreditărilor emitentului său, astfel cum se specifică în secțiunea 12.2.4 din OID4VCI, că acceptă atât tipul de dovadă «jwt», cât și tipul de dovadă «attestation» pentru atestatele cheilor care trebuie să includă obiectul «key_attestations_required».

— TR_KA-4.1: în cazul în care un emitent de acreditări emite acreditări nelegate de un dispozitiv, acesta omite parametrii «proof_types_supported» și «cryptographic_binding_metods_supported» din metadatele emitentului de acreditări.

— TR_KA-5: în cazul în care un emitent de acreditări primește un atestat al cheii într-un tip de dovadă «jwt» sau «attestation», acesta verifică semnătura atestatului cheii în cheia publică din certificatul de semnătură inclus în parametrul «x5c» din antetul JOSE al atestatului cheii și dacă acest certificat de semnătură are o ancoră de încredere pe lista pentru furnizorii de portofele menționată la articolul 5 din Regulamentul de punere în aplicare (UE) 2024/2980, eventual utilizând certificate intermediare incluse în parametrul «x5c».

— TR_KA-6: în cazul în care un emitent de acreditări primește un atestat cheie de tip «jwt», acesta verifică semnătura elementului «jwt» al cheii de la indexul 0 al seriei «attested_key» din cadrul obiectului «key_atattestation» inclus în elementul «jwt».

— TR_KA-6.1: emitentul acreditării verifică dacă în câmpul «nonce» al elementului «jwt» este inclus un parametru c_nonce valabil din nonce_endpoint corespunzător, astfel cum se specifică în OID4VCI.

— TR_KA-7: în cazul în care un emitent de acreditări primește un atestat al cheii într-un tip de dovadă «attestation», acesta trebuie să verifice dacă obiectul «key_attestation» include o valoare c_nonce valabilă provenind de la parametrul nonce_endpoint.

— TR_KA-8: un furnizor de date de identificare personală se asigură că datele de identificare personală sunt legate de o cheie publică care provine dintr-un atestat al cheii care menționează un WSCD.

(c) Cerințe privind conținutul

— C_WIA-1: un atestat al instanței portofelului include următoarele:

— afirmația „wallet_name” menționată în apendicele E la OID4VCI, unde valoarea sa reprezintă identificatorul soluției pentru portofel care poate fi găsit pe lista furnizorilor de portofele prevăzută la articolul 5 din Regulamentul de punere în aplicare (UE) 2024/2980.

— afirmație de tip «wallet_version» ([4]), care este un șir a cărui valoare este versiunea soluției pentru portofel.

— afirmație «wallet_solution_certification_information», care este un obiect JSON ce conține informații despre organismul de evaluare a conformității care a certificat soluția pentru portofel, numărul de certificare, după caz, și alte detalii relevante în ceea ce privește certificarea.

([4]) Această afirmație este definită în prezentul registru comun de date de identitate, deoarece nu face parte din specificația OID4VCI.

— afirmație «client_status», care conține două subcâmpuri:

— «status»: o referință la lista de statute, astfel cum se specifică în apendicele E la OID4VCI, care reprezintă statutul de revocare al instanței portofelului. Pentru detalii, a se vedea secțiunea (e) de mai jos;

— «exp»: «NumericDate», astfel cum se specifică în RFC 7519, care definește momentul până la care furnizorul de portofel va menține statutul de revocare la indexul listei de statute menționat în «status».

— afirmația «exp» specificată în apendicele E la OID4VCI.

— *NOTĂ*: afirmația «client_status.status» dintr-un atestat al instanței portofelului reprezintă statutul revocării instanței portofelului, nu statutul revocării atestatului în sine. Astfel cum se descrie în R_WIA-1 de mai jos, un furnizor de portofel poate decide să extindă domeniul de aplicare al fiecărui atestat al instanței portofelului la un server de autorizare specific pe baza faptului că toate atestatele trimise serverului respectiv conțin aceeași valoare de index la intrarea «client_status.status».

— *NOTĂ*: valoarea «idx» din afirmația «status» poate fi utilizată ca identificator unic (în pereche) al instanței portofelului și al unității de portofel.

— C_WIA-2: un atestat al instanței portofelului ar trebui să includă, de asemenea, afirmația «wallet_link» specificată în apendicele E la OID4VCI, iar valoarea acestei afirmații trebuie să fie o adresă URI unde se pot obține informații suplimentare cu privire la soluția pentru portofel.

— C_WIA-3: un server de autorizare nu interpretează parametrul «exp» din nivelul superior al unui atestat al instanței portofelului ca fiind sfârșitul perioadei de menținere a revocării instanței portofelului.

— *NOTĂ*: parametrul «exp» din nivelul superior al atestatului instanței portofelului indică momentul în care expiră atestatul în sine.

— C_KA-1: un atestat al cheii include:

— afirmațiile «key_storage» și «user_authentication» specificate în apendicele D la OID4VCI.

— Atributele «key_storage» și «user_authentication» au valoarea «iso_18045_high» în cazul în care un atestat al cheii menționează un WSCD;

— afirmația «certification» specificată în apendicele D la OID4VCI, care conține un URL prin care se pot obține informații cu privire la certificarea obținută de WSCD sau de depozitul de chei, cum ar fi, cu titlu indicativ, sisteme precum Common Criteria sau GlobalPlatform, cerințele evaluate precum profilul de protecție aplicabil și nivelul de evaluare.

— Pe baza acestor informații se poate stabili dacă depozitul de chei este un WSCD.

— afirmație «key_storage_status», care conține două subcâmpuri:

— «status»: o referință a listei de statute, astfel cum se specifică în apendicele D.1 la OID4VCI. Valoarea reprezintă fie statutul de revocare al WSCD-ului sau al tipului de depozit de chei utilizat pentru stocarea cheilor atestate, fie – în cadrul opțiunii de index per-key-attestation – statutul de revocare al WSCD-ului sau al depozitului de chei al unei unități de portofel individuale. A se vedea R_KA_1 de mai jos pentru opțiunile disponibile de atribuire a indexului;

— «exp»: «NumericDate», astfel cum se specifică în RFC 7519, care definește momentul până la care furnizorul de portofel va menține statutul de revocare la indexul listei de statute menționat în «status».

— afirmația «exp» specificată în apendicele D la OID4VCI.

— *NOTĂ* privind valoarea «idx» din afirmația «key_storage_status.status» dintr-un atestat al cheii: în cazul în care furnizorul de portofel utilizează opțiunea «type-shared index» (a se vedea R_KA_1 de mai jos), toate atestatele cheilor pentru același tip de WSCD sau depozit de chei au același index al listei de statute. Prin urmare, valoarea «idx» nu este unică pentru fiecare unitate de portofel în parte. Dimpotrivă, în cazul în care furnizorul de portofel utilizează opțiunea «per-key-attestation index», valoarea «idx» este unică pentru unitatea de portofel (sau unică în pereche pentru fiecare emitent de acreditări). Cu toate acestea, în toate cazurile, un emitent de acreditări nu utilizează valoarea «idx» într-un atestat al cheii ca identificator al unității de portofel, ci, în schimb, utilizează valoarea «idx» într-un atestat al instanței portofelului.

— C_KA-2: în cazul în care un atestat al cheii este trimis într-un tip de dovadă «attestation», acesta trebuie să includă, de asemenea, o valoare «c_nonce» valabilă, astfel cum se specifică în apendicele F.3 la OID4VCI.

— C_KA-3: un emitent de acreditări nu interpretează parametrul «exp» de la nivelul superior al unui atestat al cheii ca fiind sfârșitul perioadei de menținere a revocării WSCD-ului sau a depozitului de chei.

— *NOTĂ*: parametrul «exp» din nivelul superior al unui atestat al cheii indică momentul în care expiră atestatul cheii în sine.

(d) Cerințe privind ciclul de viață

— Prezenta anexă specifică următorii parametri ai metadatelor emitentului acreditării:

— «preferred_client_status_period»: OPTIONAL. Un număr întreg care indică perioada preferată rămasă de menținere a statutului atestatului instanței portofelului care trebuie prezentată de unitatea de portofel în timpul emiterii, în secunde. Perioada rămasă de menținere a statutului este definită ca valoarea «client_status.exp» din atestat, din care se scade ora primirii atestatului.

— «preferred_key_storage_status_period»: OPTIONAL. Un număr întreg care indică perioada preferată rămasă de menținere a statutului atestatului cheii care trebuie prezentată de unitatea de portofel în timpul emiterii, în secunde. Perioada rămasă de menținere a statutului este definită ca valoarea «key_storage_status.exp» din atestat, din care se scade ora primirii atestatului.

— LC_WIA-1: un server de autorizare își poate comunica preferințele pentru perioada rămasă de menținere a statutului în atestatele instanțelor portofelului prin includerea parametrului de metadate «preferred_client_status_period» în punctul final al metadatelor emitentului acreditării, astfel cum se specifică în secțiunea 12.2.2 din OID4VCI.

— LC_WIA-1.1: acest câmp se plasează la nivelul superior al metadatelor emitentului acreditării.

— LC_WIA_2: un server de autorizare nu interpretează parametrul «exp» din nivelul superior al unui atestat al instanței portofelului ca fiind sfârșitul perioadei de menținere a revocării instanței portofelului.

— LC_WIA_3: în cazul în care un furnizor de portofel semnează sau sigilează un atestat al instanței portofelului, acesta menține statutul de revocare al instanței relevante a portofelului până la expirarea valorii «wallet_instance_status.exp» indicate în atestatul respectiv al instanței portofelului.

— LC_KA-1: în cazul în care este necesar un atestat al cheii, un emitent de acreditări își poate comunica preferințele pentru perioada rămasă de menținere a statutului la atestările cheilor prin includerea parametrului de metadate «preferred_key_storage_status_period» specificat mai sus în punctul final al metadatelor emitentului de acreditări, astfel cum se specifică în secțiunea 12.2.2 din OID4VCI.

— LC_KA-1.1: acest câmp se introduce în obiectul «key_attestations_required», astfel cum se specifică în secțiunea 12.2.4 din OID4VCI.

— LC_KA-2: un furnizor de portofel alege perioada de valabilitate tehnică a atestatelor cheilor pe care le emite.

— LC_KA-3: în cazul în care un furnizor de portofel semnează sau sigilează un atestat al cheii, acesta menține statutul de revocare al WSCD-ului relevant sau al depozitului de chei până când «key_storage_status.exp» indicat în atestatul cheii respective a trecut.

— LC_GEN-1: un furnizor de portofel se asigură că o unitate de portofel poate prezenta întotdeauna atestate ale unității de portofel și atestate ale cheilor pentru care «client_status.exp» și (respectiv) «key_storage_status.exp» sunt la cel puțin 31 de zile în viitor la momentul prezentării către un server de autorizare sau către un emitent de acreditări.

— *NOTĂ*: acest lucru garantează că furnizorii de date de identificare personală se pot baza pe înlănțuirea revocărilor fără a fi obligați să emită date de identificare personală cu durată scurtă de viață.

— LC_GEN-2: un furnizor de portofel se asigură că o unitate de portofel obține metadatele emitentului acreditării în timpul emiterii.

  — LC_GEN_2.1: în cazul în care în aceste metadate este inclus un câmp «preferred_key_storage_status_period», unitatea de portofel trimite un atestat al cheii cu valoarea («key_storage_status.exp» – ora curentă) – «preferred_key_storage_status_period» cât mai mică posibil, dar nu negativă. În cazul în care unitatea de portofel nu dispune de un astfel de atestat al cheii, aceasta obține un nou atestat al cheii de la furnizorul de portofel care îndeplinește condiția «key_storage_status.exp» – ora curentă ≥ «preferred_key_storage_status_period».

  — LC_GEN_2.2: în cazul în care în aceste metadate este inclus un câmp «preferred_client_status_period», unitatea de portofel trimite un atestat instanței portofelului cu valoarea («client_status.exp» – ora curentă) – «preferred_client_status_period» cât mai mică posibil, dar nu negativă. În cazul în care unitatea de portofel nu dispune de un astfel de atestat al instanței portofelului, aceasta solicită furnizorului de portofel un nou atestat al instanței portofelului care îndeplinește condiția «client_status.exp» – ora curentă ≥ «preferred_client_status_period».

— LC_GEN-3: perioada de valabilitate tehnică a datelor de identificare personală se încheie atât înainte de termenul «client_status.exp» al atestatului instanței portofelului, cât și înainte de termenul «key_storage_status.exp» al atestatului cheii trimis furnizorului de date de identificare personală în procesul de emitere.

— LC_GEN-4: un furnizor de date de identificare personală cu o perioadă de valabilitate tehnică de peste 24 de ore verifică statutul de revocare atât al atestatului instanței portofelului, cât și al atestatului cheii primit în timpul emiterii cel puțin o dată la 24 de ore, în cursul perioadei de valabilitate tehnică a datelor de identificare personală. În cazul în care oricare dintre aceste statute este revocat, furnizorul revocă datele de identificare personală.

(e) Cerințe privind revocarea

— R_GEN-1: un furnizor de portofel utilizează liste de statute ale tokenului (specificate în lista de statute ale tokenului IETF) ca mecanism de revocare atât pentru atestatele cheii, cât și pentru atestatele instanței portofelului, astfel cum se specifică în apendicele D și, respectiv, E la OID4VCI.

— *NOTĂ*: pentru a îmbunătăți scalabilitatea listelor sale de statute, un furnizor de portofel poate utiliza următoarele optimizări:

  — Împărțirea listei de statute în mai multe blocuri, în cazul în care furnizorii de portofele au un număr considerabil de utilizatori și au emis atestate. Există numeroase strategii de împărțire în blocuri, de exemplu, bazate pe o dimensiune fixă sau pe o anumită perioadă de timp. Strategia de împărțire în blocuri este lăsată la latitudinea furnizorului de portofel. Printre considerente se numără dimensiunea unei liste de statute pentru descărcare și confidențialitatea utilizatorului.

  — Deținerea mai multor liste de statute.

  — Comprimarea unei liste de statute pentru a-i reduce dimensiunea.

— R_WIA-1: un furnizor de portofel poate atribui aceeași valoare afirmației «idx» din afirmația «client_status.status» din toate atestatele instanței portofelului pe care o anumită unitate de portofel le prezintă aceluiași server de autorizare. Aceasta se numește opțiunea «per-issuer reuse». Dacă se utilizează această opțiune:

  — R_WIA-1.1: unitatea de portofel menține statutul utilizat de valoarea indexului pentru fiecare server de autorizare cu care a interacționat anterior și solicită un atestat al instanței portofelului care să conțină aceeași valoare a indexului atunci când interacționează din nou cu același server de autorizare.

  — R_WIA-1.2: în cazul în care un furnizor de portofel primește o solicitare de atestat al instanței portofelului care conține o valoare specifică a indexului, acesta verifică dacă unitatea de portofel solicitantă a primit anterior respectiva valoare a indexului, înainte de a emite un nou atestat al instanței portofelului cu respectiva valoare a indexului.

  — R_WIA-1.3: unitatea de portofel nu trebuie să reutilizeze aceeași valoare a indexului pentru interacțiunile cu servere de autorizare diferite.

— *NOTĂ*: în cazul în care se utilizează opțiunea «per-issuer reuse», furnizorul de portofel va fi în măsură să stabilească cu câte servere de autorizare a interacționat o unitate de portofel și cât de des interacționează cu fiecare dintre acestea.

— R_WIA-2: în politica sa de confidențialitate, un furnizor de portofel documentează dacă utilizează opțiunea «per-issuer reuse» pentru revocarea instanței portofelului.

— R_WIA-3: în cazul în care un furnizor de portofel nu utilizează opțiunea «per-issuer reuse», furnizorul de portofel atribuie o valoare de index nouă, care nu poate fi legată cu altele, fiecărui atestat al instanței portofelului pe care îl emite.

— R_WIA-4: în cazul în care o unitate de portofel trebuie revocată, furnizorul de portofel revocă valorile indexului din afirmația «client_status.status» din toate atestatele instanței portofelului asociate cu respectiva unitate de portofel.

— R_WIA-5: un furnizor de portofel ține seama de amploarea implementării sale și de arhitectura subiacentă atunci când stabilește dimensiunea listelor sale de statute ale atestatului instanței portofelului, asigurându-se că acestea sunt suficient de mari pentru a preveni corelarea și a proteja viața privată a utilizatorilor. Atunci când este posibil, o listă de statute trebuie să se refere la cel puțin 10 000 de atestări.

— R_KA_1: un furnizor de portofel trebuie să aleagă una dintre următoarele opțiuni de atribuire a indexului pentru afirmația «key_storage_status.status» într-un atestat al cheii:

  — Opțiunea 1, denumită «type-shared index», în care toate atestatele cheilor care atestă cheile stocate în același tip de WSCD sau în același depozit de chei conțin aceeași valoare a indexului în «key_storage_status.status».

  — Opțiunea 2, denumită «per-key-attestion index», în care un atestat al cheii care atestă cheile stocate într-un WSCD individual sau într-un depozit de chei conține o valoare unică (în pereche) a indexului în «key_storage_status.status».

— *NOTĂ*: în cazul în care un furnizor de portofel utilizează opțiunea 1, o singură acțiune de revocare invalidează toate atestatele cheilor ale tipului afectat în toate unitățile de portofel. În plus, deoarece toate atestatele cheilor pentru același tip de WSCD sau de depozit de chei au un index unic al listei de statute, numărul de intrări dintr-o listă de statute a atestatelor cheii reflectă numărul de WSCD-uri sau de tipuri de depozite de chei acceptate de furnizorul de portofel, nu numărul de unități de portofel instalate. Prin urmare, considerentele de confidențialitate care justifică dimensiunea minimă a listei de statute pentru listele de statute ale instanțelor portofelului nu se aplică listelor de statute ale atestatelor cheilor din cadrul opțiunii 1, cu condiția să existe suficient de multe unități de portofel care utilizează același tip de WSCD sau de depozit de chei.

— *NOTĂ*: în cazul în care un furnizor de portofel utilizează opțiunea 2, fiecare index reprezintă starea de revocare a respectivului WSCD sau a respectivului depozit de chei atestat în atestatul cheii respective.

— *NOTĂ*: în cazul în care un furnizor de portofel utilizează opțiunea 2, un anumit WSCD sau un depozit de chei poate fi, de asemenea, revocat la cererea utilizatorului.

— R_KA-2: în cazul în care un furnizor de portofel utilizează opțiunea 2, furnizorul de portofel poate utiliza facultativ opțiunea «per-issuer reuse» descrisă în R_WIA-1. În cazul în care furnizorul de portofel utilizează această opțiune, cerințele R_WIA-1 – R_WIA-3 se aplică *mutatis mutandis*.

— R_KA-3: în cazul în care un furnizor de portofel utilizează opțiunea 2, furnizorul de portofel ține seama de amploarea implementării sale și de arhitectura subiacentă atunci când stabilește dimensiunea listelor sale de statute ale atestatului cheii, asigurându-se că acestea sunt suficient de mari pentru a preveni corelarea și a proteja viața privată a utilizatorilor. Atunci când este posibil, o listă de statute se referă cel puțin la 10 000 de atestate ale cheii.

— R_KA-4: în cazul în care un furnizor de portofel utilizează opțiunea 1 (index partajat în funcție de tip), furnizorul de portofel revocă o intrare «key_storage_status.status» numai dacă tipul de WSCD sau de depozit de chei are o vulnerabilitate în materie de securitate.

(f) Cerințe privind algoritmii de semnătură

— SA-1: Pentru semnarea atestatelor instanței portofelului, a atestatelor cheilor, a listelor aferente de dovadă a posesiei și de statute ale tokenului, se utilizează unul dintre următorii algoritmi:

— ES256 (ECDSA cu SHA-256 și P-256)

— ES384 (ECDSA cu SHA-384 și P-384)

— ES512 (ECDSA cu SHA-512 și P-521)

— SA-2: Un furnizor de portofel alege algoritmii menționați în SA-1 pe care îi va utiliza.

— SA-3: un server de autorizare sau un emitent de acreditări (astfel cum se specifică în OID4VCI) trebuie să fie compatibil cu toți algoritmii menționați în SA-1.”

ANEXA IV

„ANEXA II

Lista standardelor menționate la articolul 8

Se aplică specificațiile tehnice prevăzute la clauzele 2-6 din ETSI TS 119 472-1 V1.2.1 (2026-02). Acestea se citesc cu următoarele adaptări:

1. 2.1 Normative references

— [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» [Semnături electronice și infrastructuri (ESI); Profiluri de certificat; Partea 1: Prezentare generală și structuri comune de date].

— [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» [Semnăturile electronice și infrastructurile de încredere (ESI); Profiluri de certificat; Partea 6: Cerințe privind profilul certificatului pentru furnizorii de servicii de date de identificare personală, portofel, atestate electronice ale atributelor, atestate electronice calificate ale atributelor și prestatori de servicii de asigurare a încrederii calificați].

— [25] Lista de statute ale tokenului IETF (TSL), draft-ietf-oauth-status-list-20: «Token Status List» (Lista de statute ale tokenului), 20 aprilie 2026.

2. 4.2.11.1 General requirements

— EAA-4.2.11.1-06: atunci când se utilizează un element de statut pentru datele de identificare personală, atestatele electronice calificate ale atributelor sau atestatele electronice ale atributelor furnizate de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism, acesta indică numai dacă atestatul este revocat sau nu și nu acceptă nicio altă valoare a statutului, cum ar fi suspendarea.

— EAA-4.2.11.1-06.1: în cazul în care un atestat este revocat, revocarea sa este permanentă.

3. 4.2.13 EAA short-lived

— EAA-4.2.13-03: în cazul în care se emit atestate electronice cu durată scurtă de viață ale atributelor cu o perioadă de valabilitate de cel mult 24 de ore, revocarea nu este necesară.

4. 4.6.3 Cerințe pentru atestatul electronic al atributelor european, emis de un organism public responsabil de o sursă autentică (PuB-EAA) sau în numele unui astfel de organism

— PuB-EAA-4.6.2-03: void.

— Pub-EAA-4.6.2-04: void.

— PuB-EAA-4.6.3-03: semnătura digitală PuB-EAA ar trebui să conțină certificatul calificat care stă la baza semnăturii digitale PuB-EAA.

— PuB-EAA-4.6.3-04: certificatul calificat care stă la baza semnăturii digitale PuB-EAA trebuie să îndeplinească cerințele prevăzute la clauza 8 din ETSI TS 119 412-6 v1.1.1 și trebuie să conțină declarația QcType QcStatement, astfel cum este definită în ETSI EN 319 412-5 v2.5.1, valoarea id-etsi-qct-eidaspsbeaa fiind definită după cum urmează:

IDENTIFICATORUL DE OBIECT id-etsi-qct-eidaspsbeaa: = {id-etsi-eidas2-qct-extensions 3} – certificatul menționat la articolul 45f alineatul (1) litera (b) care stă la baza semnăturii electronice calificate sau sigiliul electronic calificat al organismului din sectorul public menționat la articolul 3 alineatul (46) din Regulamentul (UE) nr. 910/2014.

5. 5.2.10.1 General requirements

— EAA-5.2.10.1-04: void.

— EAA-5.2.10.1-05: void.

— EAA-5.2.10.1-06: Câmpul statutului poate conține câmpul status_list, astfel cum se specifică în clauza 6.2 din IETF draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: void.

— EAA-5.2.10.1-08: void.

— EAA-5.2.10.1-09: void.

— EAA-5.2.10.1-10: void.

— EAA-5.2.10.1-11: void.

— EAA-5.2.10.1-12: void.

6. 6.2.10.1 General requirements

— EAA-6.2.10.1-01: atunci când un atestat electronic al atributelor conform cu ISO/IEC mdoc utilizează mecanismul listei de statute ale atestatului, astfel cum este prevăzut în EAA-6.2.10.1-02.2, sau mecanismul listei de revocare a atestatului, astfel cum este prevăzut în EAA-6.2.10.1-02.3, obiectul său de securitate mobilă («MSO») trebuie să conțină structura statutului, astfel cum este specificată în EAA-6.2.10.1-17, care conține informații privind revocarea MSO.

— EAA-6.2.10.1-01.1: la punerea în aplicare a mecanismului listei de identificatori, elementul de statut trebuie să conțină elementul identifier_list, astfel cum se prevede în EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: la punerea în aplicare a mecanismului listei de statute, elementul de statut trebuie să conțină elementul status_list, astfel cum se prevede în EAA-6.2.10.1-13.

— *NOTĂ*:

  — structura statutului conține o trimitere la o listă de revocare a MSO.

  — Lista de revocare a MSO este o structură COSE_Sign1 care indică dacă un anumit MSO este revocat sau nu.

  — Structura statutului conține toate informațiile necesare pentru ca beneficiarul portofelului să stabilească dacă lista de revocare a MSO este autentică.

— EAA-6.2.10.1-02: furnizorul de date de identificare personală, furnizorul de atestate electronice calificate ale atributelor sau furnizorul de atestate electronice ale atributelor furnizate de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism utilizează una dintre următoarele metode de revocare a datelor de identificare personală, a atestatelor electronice calificate ale atributelor sau a atestatelor electronice ale atributelor furnizate de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism:

— EAA-6.2.10.1-02.1: în cazul în care emit atestate electronice de scurtă durată ale atributelor cu o perioadă de valabilitate de 24 de ore sau mai mică, revocarea nu este necesară.

— EAA-6.2.10.1-02.2: utilizează un mecanism al listei de statute ale atestatului pentru a codifica informațiile privind revocarea ca listă de statute.

— EAA-6.2.10.1-02.2.1: mecanismul listei de statute revocă un MSO în funcție de măsura în care bitul poziției bitului definit de emitent în MSO este setat ca «true» în lista de statute.

— EAA-6.2.10.1-02.2.2: mecanismul listei de statute este indicat în specificațiile listei de statute a tokenului (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: utilizează un mecanism al listei de revocări ale atestatului pentru a codifica informațiile privind revocarea ca listă de identificatori.

— EAA-6.2.10.1-02.3.1: mecanismul listei de identificatori revocă un MSO în funcție de prezența sau de absența identificatorului definit de emitent în MSO pe lista identificatorilor.

— 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 și EAA-6.2.10.1-11 precizează mecanismul listei de identificatori, pe baza cerințelor din specificațiile listei de tokenuri, inclusiv caracterul comun al listei de statute și al mecanismului listei de identificatori.

— EAA-6.2.10.1-03: atunci când se utilizează un element de statut pentru date de identificare personală, atestate electronice calificate ale atributelor sau atestate electronice ale atributelor furnizate de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism, se utilizează exclusiv statutul «revoked» (revocat).

— EAA-6.2.10.1-03.1: Pentru o listă de statute, aceasta implică faptul că se utilizează numai valorile «valid» și «invalid», astfel cum se prevede în specificațiile listei de statute ale tokenului.

— EAA-6.2.10.1-03.2: pentru lista de identificatori, numai MSO-urile revocate, spre deosebire de MSO-urile suspendate temporar, se introduc în lista de identificatori.

— EAA-6.2.10.1-04: în cazul în care un MSO este revocat, revocarea MSO-ului este definitivă.

— EAA-6.2.10.1-05: verificarea listei de revocare a MSO-urilor este opțională pentru beneficiarul portofelului și, după caz, verificarea trebuie să respecte cerințele de verificare menționate în specificațiile listei de statute ale tokenului și specificațiile structurii statutului prevăzute în EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: în cazul în care un beneficiar al portofelului trebuie să fie în măsură să verifice statutul de revocare al datelor de identificare personală sau al atestatelor electronice ale atributelor, acesta acceptă atât mecanismul listei de statute ale atestatului, cât și mecanismul listei de revocare a atestatului prevăzute în EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: identifier_list și status_list din MSO pot conține elementul certificat.

— EAA-6.2.10.1-06.1: în cazul în care elementul certificatului este prezent, acesta trebuie să conțină un certificat care conține cheia publică care a semnat sau a sigilat certificatul de nivel superior în elementul x5chain din structura listei de revocare a MSO.

— EAA-6.2.10.1-06.1.1: instanța beneficiarului portofelului utilizează certificatul respectiv ca ancoră de încredere pentru verificarea elementului x5chain din structura listei de revocare a MSO.

— EAA-6.2.10.1-06.2: în cazul în care elementul certificatului nu este prezent, certificatul de nivel superior din elementul x5chain din structura listei de revocări a MSO trebuie semnat sau sigilat de certificatul utilizat pentru semnarea certificatului în elementul x5chain al MSO.

— EAA-6.2.10.1-06.2.1: instanța beneficiarului portofelului utilizează certificatul respectiv ca ancoră de încredere pentru verificarea elementului x5chain din structura listei de revocare a MSO.

— EAA-6.2.10.1-07: o listă de revocare a MSO este implementată în conformitate cu specificațiile listei de statute a tokenului ca token al listei de statute în format CWT.

— EAA-6.2.10.1-08: în ceea ce privește lista de revocare a MSO pentru lista de identificatori și mecanismul listei de statute, se aplică următoarele cerințe:

  — afirmația exp trebuie să fie prezentă.

  — afirmația ttl poate fi prezentă.

  — afirmația aggregation_uri din afirmația IdentifierList sau StatusList poate fi prezentă, iar furnizorul de date de identificare personală, furnizorul de atestate electronice calificate ale atributelor sau furnizorul de atestate electronice ale atributelor furnizate de un organism din sectorul public responsabil de o sursă

autentică sau în numele unui astfel de organism poate utiliza afirmația aggregation_uri pentru a indica compatibilitatea cu mecanismul de agregare, astfel cum se precizează în specificațiile listei de statute a tokenului.

— CWT este un obiect COSE_Sign1 care utilizează unul dintre următorii algoritmi de semnătură pentru calcularea semnăturii:

(a) «ES256» (ECDSA cu curbă NIST P-256 și SHA-256);

(b) «ES384» (ECDSA cu curbă NIST P-384 și SHA-384);

(c) «ES512» (ECDSA cu curbă NIST P-521 și SHA-512);

(d) «ESB256» (ECDSA cu curbă brainpoolP256r1 și SHA-256);

(e) «ESB384» (ECDSA cu curbă brainpoolP384r1 și SHA-384);

(f) «ESB512» (ECDSA cu curbă brainpoolP512r1 și SHA-512);

— CWT conține x5chain în antetul protejat care conține certificatul sau lanțul de certificate pentru verificarea semnăturii listei de revocare a MSO.

— utilizarea extinsă a cheii identificatorului de obiect precizată în specificațiile listei de statute a tokenului poate fi folosită pentru lista de statute și pentru certificatul de semnare a listei de identificatori, iar instanțele beneficiarului portofelului pot accepta utilizarea extinsă a cheii identificatorilor de obiect precizată în specificațiile listei de statute a tokenului și, pentru identificatorul de obiect, furnizorul de atestate electronice calificate ale atributelor sau furnizorul de atestate electronice ale atributelor furnizate de un organism din sectorul public sau în numele acestuia nu trebuie să facă în așa fel încât câmpul extins de utilizare a cheii să fie esențial atunci când folosește OID-ul extins de utilizare a cheii precizat în specificațiile listei de statute a tokenului.

— EAA-6.2.10.1-09: în mod contrar cerințelor din specificațiile listei de statute ale tokenului, pentru mecanismul listei de identificatori se aplică următoarele cerințe:

— valoarea afirmației de tip este «application/identifierlist+cwt»;

— afirmația StatusList nu trebuie să fie prezentă în setul de afirmații CWT;

— structura IdentifierList definită în EAA-6.2.10.1-11 trebuie să fie prezentă ca afirmație în afirmațiile CWT stabilite utilizând cheia 65530.

— EAA-6.2.10.1-10: structura IdentifierList este o structură CBOR cu următorul 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: în cazul în care identificatorul din IdentifierList este prezent, MSO-ul care conține identificatorul în elementul de statut este revocat.

— EAA-6.2.10.1-10.2: afirmația Aggregation_uri este menționată în secțiunea 9.2 din specificațiile listei de statute a tokenului.

— EAA-6.2.10.1-10.3: Tipul de conținut al listei de identificatori este «application/identifierlist+cwt», prevăzut în cerințele de la secțiunea 8.2 din specificațiile listei de statute a tokenului.

— EAA-6.2.10.1-11: următoarele cerințe se aplică elementului «identifier_list» din MSO (a se vedea EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: elementul identifier_list este o structură CBOR cu următorul CDDL:

```
IdentifierListInfo = {

        «id»: Identifier ,

        «uri»: URI,

        ? «certificate»: Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: pentru a preveni utilizarea identificatorului ca o corelație între prezentări, acesta trebuie să fie unic pentru fiecare MSO în parte.

— EAA-6.2.10.1-12: pentru lista de statute se aplică următoarele cerințe:

  — EAA-6.2.10.1-12.1: elementul de biți din structura StatusList se setează la 1.

— EAA-6.2.10.1-13: pentru elementul status_list din MSO se aplică următoarele cerințe (a se vedea EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: elementul status_list trebuie să respecte cerințele pentru structura StatusListInfo, astfel cum se precizează în specificațiile privind lista de statute ale tokenului și trebuie adăugat elementul certificatului opțional definit în EAA-6.2.10.1-06.

  — EAA-6.2.10.1-13.2: pentru a evita ca indexul statutului să fie o corelație între prezentări, combinația dintre indexul statutului și URI trebuie să fie unică pentru fiecare MSO în parte.

— EAA-6.2.10.1-14: furnizorul de portofel utilizează a doua (EAA-6.2.10.1-02.2) sau a treia (EAA-6.2.10.1-02.3) dintre metodele specificate în EAA-6.2.10.1-02 pentru revocarea unui atestat al instanței portofelului (WIA) și pentru revocarea unui atestat al cheii (KA).

— EAA-6.2.10.1-15: furnizorul de portofel implementează mecanismele de revocare a atestatului specificate în EAA-6.2.10.1-02 în soluția sa pentru portofel.

— EAA-6.2.10.1-16: furnizorul de date de identificare personală și furnizorul de atestate electronice ale atributelor acceptă atât mecanismul listei de statute ale atestatului, cât și mecanismul listei de revocare a atestatului specificat în EAA-6.2.10.1-02 pentru verificarea statutului de revocare al unui atestat al instanței portofelului (WIA) și al unui atestat al cheii (KA).

— EAA-6.2.10.1-17: structura statutului în MSO este o structură CBOR cu următorul CDDL:

Status = {

? «identifier_list»: IdentifierListInfo,

? «status_list»: StatusListInfo,

* tstr => RFU

}”

ANEXA V

„ANEXA III

Specificațiile tehnice menționate la articolul 10

— Specificații tehnice:

  — Clauza 4.2.5 din ETSI TS 119 472-3 V1.1.1 (2026-03).”

ANEXA VI

Anexa IV la Regulamentul de punere în aplicare (UE) 2024/2979 se modifică după cum urmează:

1. Punctul 1 se înlocuiește cu următorul text:

„1. Format obligatoriu de semnătură sau sigiliu:

(a) PAdES (semnătură electronică avansată în format PDF – PDF Advanced Electronic Signature), astfel cum se indică în standardul ETSI EN 319 142-1 V1.2.1 (2024-01); Semnături electronice și infrastructuri (ESI); Semnături digitale în format PAdES; Partea 1: Elemente de construcție și semnături de bază PAdES."

2. Punctul 3 se înlocuiește cu următorul text:

„3. Interfața de programare a aplicațiilor:
ETSI TS 119 432 v1.3.1 (2026-03) clauzele 6.4.3, A.6, A.7 și A.8."

ANEXA VII

„ANEXA VI

Marca de încredere a portofelului UE pentru identitatea digitală, în culori



”

ANEXA VIII

„ANEXA VII

Marca de încredere a portofelului UE pentru identitatea digitală, în alb și negru



”

ANEXA IX

„ANEXA VIII

Date privind marca de încredere a portofelului UE pentru identitatea digitală

Date	Descriere	Codificare	Statut
TrustMarkResourceURL	Adresa URL a elementelor grafice ale mărcii de încredere a portofelului UE pentru identitatea digitală și resursele de informații pentru utilizatori din interfața pentru utilizatori a portofelului.	URL	obligatoriu
ListOfCertifiedWalletsURL	Adresa URL a listei publice a soluțiilor pentru portofel certificate în UE, astfel cum se prevede în Regulamentul de punere în aplicare (UE) 2025/849 al Comisiei ([1]).	URL	obligatoriu
ListOfCertifiedWalletsQRCode	Codul QR care conține informațiile despre ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	opțional
WalletSolutionInfoPageURL	Adresa URL către pagina de informații a soluției certificate pentru portofel din lista de soluții certificate pentru portofel de la adresa URL ListOfCertifiedWalletsURL atașată cu un «?» și identificatorul WalletSolutionID al soluției pentru portofel.	URL	obligatoriu
WalletSolutionInfoPageQRCode	Cod QR care conține informațiile despre WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	opțional
WalletVerifierToolURL*	Adresa URL care redirecționează către punctul final */.well-known/openid-credential-issuer* al instrumentului de verificare a portofelului, utilizat pentru recuperarea metadatelor furnizorului atestatului.	URL	opțional

([1]) Regulamentul de punere în aplicare (UE) 2025/849 al Comisiei din 6 mai 2025 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește transmiterea de informații către Comisie și Grupul de cooperare privind lista portofelelor europene pentru identitatea digitală certificate (JO L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj)."

ANEXA X

Anexa II la Regulamentul de punere în aplicare (UE) 2024/2980 se modifică după cum urmează:

1. În anexa II secțiunea 1, punctul 1 litera (i) se înlocuiește cu următorul text:

„(i) unul sau mai multe certificate conforme cu standardul ETSI EN 319 412-2 V2.4.1 (2025-06) sau cu standardul ETSI EN 319 412-3 V1.3.1 (2023-09), care pot fi utilizate pentru a verifica semnătura sau sigiliul creat(ă) de operatorul de registru pe datele din registru și pentru care datele de identitate certificate includ numele operatorului de registru și, după caz, numărul de înregistrare al operatorului de registru, astfel cum se prevede la literele (c) și, respectiv, (d);".

2. În anexa II secțiunea 2, punctul 1 litera (h) se înlocuiește cu următorul text:

„(h) unul sau mai multe certificate conforme cu standardul ETSI EN 319 412-2 V2.4.1 (2025-06) sau cu standardul ETSI EN 319 412-3 V1.3.1 (2023-09) care pot fi utilizate pentru autentificarea și validarea atestatelor unităților de portofel pe care furnizorul de portofel le-a emis și pentru care datele de identitate certificate includ numele și, după caz, numărul de înregistrare al furnizorului de portofel, astfel cum se prevede la literele (a) și, respectiv, (b);".

3. În anexa II secțiunea 3, punctul 1 litera (h) se înlocuiește cu următorul text:

„(h) unul sau mai multe certificate conforme cu standardul ETSI EN 319 412-2 V2.4.1 (2025-06) sau cu standardul ETSI EN 319 412-3 V1.3.1 (2023-09), care pot fi utilizate pentru a verifica semnătura sau sigiliul creat(ă) de furnizorul de date de identificare personală pentru datele de identificare personală furnizate și pentru care datele de identitate certificate includ numele și, după caz, numărul de înregistrare al furnizorului de date de identificare personală, astfel cum se prevede la literele (a) și, respectiv, (b)."

4. În anexa II secțiunea 4, punctul 1 litera (g) se înlocuiește cu următorul text:

„(g) unul sau mai multe certificate conforme cu standardul ETSI EN 319 412-2 V2.4.1 (2025-06) sau cu standardul ETSI EN 319 412-3 V1.3.1 (2023-09), care pot fi utilizate pentru a verifica semnătura sau sigiliul creat(ă) de furnizorul de certificate de acces pentru beneficiarii portofelelor pentru certificatul de acces furnizat beneficiarului portofelului, împreună, după caz, cu informațiile necesare pentru a distinge certificatele de acces pentru beneficiarii portofelelor de alte certificate."

5. În anexa II, se adaugă secțiunea 5 după cum urmează:

„5. Notificări de informații referitoare la furnizorii de certificate de înregistrare pentru beneficiarii portofelelor

1. Statele membre furnizează Comisiei următoarele informații privind furnizorii de certificate de înregistrare pentru beneficiarii portofelelor:

(a) numele furnizorului de certificate de înregistrare pentru beneficiarii portofelelor;

(b) după caz, numărul de înregistrare al furnizorului de certificate de înregistrare pentru beneficiarii portofelelor;

(c) statul membru în care este stabilit furnizorul de certificate de înregistrare pentru beneficiarii portofelelor;

(d) adresa de e-mail și numărul de telefon la care poate fi contactat furnizorul de certificate de înregistrare pentru beneficiarii portofelelor, pentru chestiunile legate de certificatele de înregistrare furnizate beneficiarilor portofelelor;

(e) după caz, adresa URL a paginii web a furnizorului de certificate de înregistrare pentru beneficiarii portofelelor care conține informații suplimentare cu privire la furnizor și la certificatele de înregistrare furnizate beneficiarilor portofelelor;

(f) adresa URL a paginii web care conține politicile și condițiile generale care se aplică furnizării și utilizării certificatelor de înregistrare furnizate beneficiarilor portofelelor;

(g) unul sau mai multe certificate conforme cu standardul ETSI EN 319 412-2 V2.4.1 (2025-06) sau cu standardul ETSI EN 319 412-3 V1.3.1 (2023-09), care pot fi utilizate pentru a verifica semnătura sau sigiliul creat(ă) de furnizorul de certificate de înregistrare pentru beneficiarii portofelelor pentru certificatele de înregistrare furnizate beneficiarului portofelului, împreună, după caz, cu informațiile necesare pentru a distinge certificatele de înregistrare pentru beneficiarii portofelelor de alte certificate.

2. Informațiile menționate la punctul 1 se furnizează pentru fiecare furnizor de certificate de înregistrare pentru beneficiarii portofelelor.”

ANEXA XI

„ANEXA I

Protocoalele și interfețele menționate la articolul 4

Specificațiile tehnice ETSI TS 119 472-3 V1.1.1 (2026-03) se aplică cu următoarele adaptări:

1. 4.1. General requirements

   — GEN-REQ-4.1-05: necompletat

   — NOTĂ: necompletat

2. 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet

   — ISS-MDATA-REG_CERT-4.2.3-04: unul dintre elementele parametrului seriei issuer_info trebuie să conțină certificatul de înregistrare PID/EAA al furnizorului.

   — ISS-MDATA-REG_CERT-4.2.3-07: necompletat

   — ISS-MDATA-REG_CERT-4.2.3-08: necompletat

   — ISS-MDATA-REG_CERT-4.2.3-09: necompletat

   — ISS-MDATA-REG_CERT-4.2.3-10: necompletat

   — ISS-MDATA-REG_CERT-4.2.3-11: necompletat

   — ISS-MDATA-REG_CERT-4.2.3-12: necompletat

   — ISS-MDATA-REG_CERT-4.2.3-13: necompletat

3. 4.2.4.2 ARF pre-defined PID/EAA reuse policy

   — ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: În cazul în care membrul id are valoarea «arf_annex_ii», iar seria asociată cu eticheta «details» conține valoarea «once_only» sau valoarea «per-relying-party», atunci obiectul JSON care conține această serie asociată cu eticheta «details» conține, de asemenea, un număr JSON asociat cu eticheta «reissue_trigger_not».

4. Anexa A nu se aplică.”

ANEXA XII

„ANEXA II

Specificațiile tehnice menționate la articolul 5

Se aplică specificațiile tehnice din anexa C la standardul ISO/IEC 18013-7: 2025.

Specificațiile tehnice din clauzele 4.1, 4.2, 5 și 6 din ETSI TS 119 472-2 V1.2.1 (2026-03) se aplică cu următoarele adaptări, inclusiv introducerea unei noi clauze 4.3:

1. 1 Scope

— Prezentul document specifică două profiluri de protocoale pentru a permite beneficiarilor [denumiți în continuare Relying Parties (RP)] să solicite prezentări ale atestatelor electronice ale atributelor (EAAP) sau date de identificare personale (denumite în continuare PID) portofelului EUDI și portofelului EUDI să trimită EAAP/PID solicitate către PR. Fiecare dintre profiluri este compatibil cu două mecanisme de transmitere, și anume: mediate prin API și nemediate prin API, după cum se arată mai jos:

(a) Un profil se bazează pe:

— ISO/IEC 18013-5 [10] numai pentru mecanismul de transmitere nemediat prin API și

— anexa C la ISO/IEC 18013-7 [16] pentru mecanismul de transmitere mediat prin API.

Acest profil este denumit profil ISO/IEC-mdoc și este definit în clauza 5 din prezentul document.

(b) Un profil se bazează pe:

OpenID4VC-HAIP [11] atât pentru mecanismele de transmitere mediate prin API, cât și pentru cele nemediate prin API, după cum urmează:

— secțiunile 5, 5.1, 5.3, 7 și 8 din [11] pentru transmiterea prin redirecționare sau prin mecanismul de transmitere mediat prin API; și

— secțiunile 5, 5.2, 5.3, 7 și 8 din [11] pentru mecanismul de transmitere mediat prin API.

Acest profil este denumit profil OpenID4VC-HAIP și este definit în clauza 6 din prezentul document.

2. 2.1 Normative references

— [15] ISO 639: «Language code».

— [16] ISO/IEC 18013-7:2025 «Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions» [Identificare personală – ISO – permis de conducere conform – Partea 7: Funcții suplimentare la permisul de conducere mobil (mDL)].

3. 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: necompletat.

4. 4.2 EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: necompletat.

— Note2: necompletat.

— EAAP-ISO/IEC-mdoc-02: necompletat.

5. 4.3 Implementarea EAAP cu API de mediere

— EAAP-API-GEN-01: portofelul EUDI trebuie să fie compatibil cu o API de mediere care este compatibilă cu ambele protocoale definite în clauza 5.2 din [11] și în anexa C la [16].

— *NOTĂ*: în cazul în care dispozitivul pe care este instalat portofelul EUDI nu este compatibil cu niciunul din cele două protocoale, această cerință nu poate fi îndeplinită și declanșează o neconformitate din cauza faptului că browserele și sistemele de operare subiacente nu implementează caracteristicile de interoperabilitate necesare.

— EAAP-API-GEN-02: portofelul EUDI este compatibil cu o API de mediere cel puțin pentru tipurile de PID și EAA înregistrate în catalogul sistemelor de atestare a atributelor, astfel cum sunt definite în Regulamentul de punere în aplicare (UE) 2025/1569, și cel puțin pentru toate formatele definite în anexa II la Regulamentul de punere în aplicare (UE) 2024/2979.

— *NOTA 1*: în cazul în care sistemul de operare subiacent, browserul, API de mediere sau orice alt nivel tehnic aflat în afara controlului portofelului EUDI restricționează, filtrează, preselectează sau limitează în alt mod formatele acreditărilor, precum și tipurile PID și EAA înregistrate în catalogul sistemelor de atestare a atributelor, această cerință nu poate fi îndeplinită. În cazul în care o astfel de restricție împiedică portofelul EUDI să accepte un tip sau un format de acreditare înregistrat, neconformitatea rezultată poate fi atribuită defectării sistemelor de operare, browserelor, API-urilor de mediere subiacente sau altui nivel tehnic relevant pentru a asigura caracteristicile de interoperabilitate necesare.

6. 4.4 Validarea beneficiarilor portofelelor și verificări ale solicitării excesive de date

— WRP-VALIDATION-01: portofelul EUDI validează certificatul de înregistrare al beneficiarului portofelului primit în cerere înainte de a prezenta utilizatorului portofelului, spre aprobare, orice PID sau atestat electronic al atributelor solicitat.

— WRP-VALIDATION-02: în cazul în care validarea certificatului de înregistrare al beneficiarului portofelului nu este reușită, inclusiv în cazul în care certificatul este expirat, revocat, nu este emis de un furnizor de certificate de înregistrare pentru beneficiarii portofelelor care să fie de încredere și valabil, este într-un format necorespunzător sau nu poate fi verificat criptografic, portofelul EUDI avertizează utilizatorul portofelului că beneficiarul portofelului nu a putut fi validat și nu prezintă cererea ca fiind validată cu succes. Utilizatorul portofelului aprobă în mod explicit cererea beneficiarului. Lipsa unei confirmări explicite sau căsuțele bifate în prealabil nu sunt suficiente pentru o aprobare explicită.

— WRP-VALIDATION-03: furnizorul de portofel stabilește, pe baza analizei riscurilor și a politicii sale de securitate, dacă și în ce condiții utilizatorul portofelului poate trece peste anumite verificări ale validărilor nereușite.

— WRP-OVERASKING-01: portofelul EUDI compară atestatele și atributele solicitate de beneficiarul portofelului cu atestatele și atributele înregistrate în certificatul de înregistrare al beneficiarului portofelului.

— WRP-OVERASKING-02: În cazul în care beneficiarul portofelului solicită PID sau atestate electronice ale atributelor sau afirmații care nu sunt acoperite de certificatul de înregistrare al beneficiarului portofelului, portofelul EUDI avertizează în mod clar utilizatorul portofelului înainte de orice divulgare. Avertismentul identifică faptul că beneficiarul portofelului solicită mai multe informații decât a înregistrat. Utilizatorul portofelului aprobă în mod explicit cererea beneficiarului. Lipsa unei confirmări explicite sau căsuțele bifate în prealabil nu sunt suficiente pentru o aprobare explicită.

— WRP-OVERASKING-03: furnizorul de portofel stabilește, pe baza analizei riscurilor, a politicii de securitate și a legislației aplicabile, dacă utilizatorul portofelului poate merge mai departe în pofida unui astfel de avertisment, dacă poate fi divulgat numai subsetul de date solicitate care fac obiectul certificatului de înregistrare sau dacă cererea trebuie respinsă.

7. 5.1 Introduction

— Clauza 5 și subclauzele sale definesc un profil pentru un protocol care permite unui RP să solicite EAAP sau PID de la portofelul EUDI și portofelului EUDI să trimită EAAP/PID-urile solicitate către RP utilizând fie un mecanism de transmitere nemediat prin API, bazat pe ISO/IEC 18013-5 [10], fie un mecanism de transmitere mediat prin API bazat pe anexa C la ISO/IEC 18013-7 [16] pentru transferul structurilor de date definite în ISO/IEC 18013-5 [10] încapsulate în mod corespunzător.

— Restul clauzei 5 este organizat după cum urmează:

  — Clauza 5.2 definește cerințele privind acceptarea profilului și a mecanismelor de transmitere de către RP și portofelul EUDI;

  — Clauza 5.3 prevede cerințe specifice pentru mecanismul de transmitere nemediat prin API;

  — Clauza 5.4 și subclauzele sale prevăd cerințe specifice pentru mecanismul de transmitere mediat prin API.

8. 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: unitățile de portofel, furnizorii de PID, furnizorii de atestate, furnizorii de portofele și beneficiarii nu permit extragerea serverului, astfel cum se specifică în ISO/IEC 18013-5 [10], pentru solicitarea și prezentarea atributelor PID sau ale atestatelor.

— ISO/IEC 18013-SUPPORT-02: portofelul EUDI trebuie să îndeplinească cerințele definite la clauzele 5.3 și 5.4 din prezentul document.

— ISO/IEC 18013-SUPPORT-04: un beneficiar ar trebui să implementeze profilul definit în clauza 5.4 din prezentul document.

9. 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: solicitările de dispozitive trimise portofelelor EUDI conțin perechea de valori ale cheii «requestInfo» specificată în clauza 8.3.2.1.2.1 din [10]. Valoarea acestei perechi trebuie să fie de tipul RequestInfo.

— ISO/IEC 18013-5-REQ-05: Tipul RequestInfo este cel indicat în definiția CDDL de mai jos.

RequestInfo = {

«euWrprc»: bstr; conține un certificat de înregistrare (a se vedea cerințele de mai jos)

}

— ISO/IEC 18013-5-REQ-06: câmpul requestInfo menționat conține un câmp cu eticheta «euWrprc»

— ISO/IEC 18013-5-REQ-07: valoarea «euWrprc» va fi un certificat de înregistrare codificat în format CBOR.

— ISO/IEC 18013-5-REQ-08: necompletat.

— NOTA 3: necompletat.

— ISO/IEC 18013-5-REQ-09: void.

— ISO/IEC 18013-5-REQ-10: necompletat.

— ISO/IEC 18013-5-REQ-11: void.

10. 5.3.3 ISO/IEC-mdoc EAAP Response profile

— Prezenta clauză stabilește cerințele pentru tipul de mesaj DeviceResponse, care este comun celor două tipuri de mecanisme de transmitere (mediate prin API și nemediate prin API).

— *NOTA 1*: în cazul în care se utilizează un mecanism nemediat prin API bazat pe ISO/IEC 18013-5 [10], un răspuns EAAP este exact un exemplu de DeviceResponse astfel cum a fost profilat în prezenta clauză. În cazul în care se utilizează un mecanism mediat prin API bazat pe anexa C la ISO/IEC 18013-7 [16], instanța DeviceRequest este încapsulat astfel cum se specifică în anexa C la [16].

— ISO/IEC 18013-5-RESP-02: furnizorul de date de identificare personală și de atestate electronice ale atributelor nu include niciun element de date în harta KeyAuthorizations din obiectul de securitate mobilă al datelor de identificare personală și al atestatelor electronice ale atributelor pe care le emite, cu excepția elementelor de date care sunt furnizate de beneficiarul portofelului în datele de tranzacționare din solicitarea mdoc care urmează să fie semnată sau sigilată de unitatea de portofel utilizând cheia privată a datelor de identificare personală sau atestatele electronice ale atributelor.

— *NOTA 2*: prin urmare, unitățile de portofel nu pot prezenta niciun element de date semnat de dispozitiv beneficiarilor portofelului, cu excepția datelor de semnare pe care beneficiarul portofelului le-a furnizat, de exemplu, în cazurile de utilizare pentru autentificarea securizată a utilizatorilor.

— *NOTA 3*: ISO/IEC 18013-5: 2021 nu specifică modul în care beneficiarii portofelelor pot include date privind tranzacțiile într-o solicitare mdoc. Includerea datelor privind tranzacțiile într-o solicitare mdoc are loc cu adăugarea unor specificații tehnice.

— ISO/IEC 18013-5-RESP-03: furnizorii de date de identificare personală nu permit cheii private a datelor de identificare personală să semneze elementele de date care sunt furnizate de beneficiarul portofelului în datele privind tranzacțiile din solicitarea mdoc.

11. 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

Prezenta clauză definește cerințele pentru mecanismul de transmitere mediat prin API legate de cerințele definite la anexa C la [16].

— ISO/IEC 18013-7-API-01: profilul care susține prezentările mediate de API trebuie să respecte cerințele din anexa C la ISO/IEC 18013-7 [16], astfel cum sunt prevăzute la clauzele 5.3 și 5.4 din prezentul document.

— ISO/IEC 18013-7-API-02: toate cerințele obligatorii definite în anexa C la [16] se aplică conform profilurilor suplimentare de la clauzele 5.3 și 5.4 din prezentul document.

— ISO/IEC 18013-7-API-03: toate cerințele opționale definite în anexa C la [16] rămân opționale, cu excepția cazului în care se prevede altfel în prezentul document.

12. 5.4.2 Additional requirements

— Prezenta clauză prevede cerințe suplimentare pentru mecanismul de transmitere mediat prin API.

— ISO/IEC 18013-ADD-API-01: portofelul EUDI divulgă implicit prezența tuturor atestatelor electronice stocate ale tipului de atribute către API de mediere care funcționează în conformitate cu anexa C la [16], dar nu divulgă atributele și valorile acestora în aceste atestări electronice ale atributelor.

— *NOTA 1*: restricția privind valoarea atributelor se aplică chiar dacă o astfel de divulgare ar îmbunătăți serviciile furnizate de sistemul de operare portofelului EUDI, de exemplu, selectarea atestatului în contextul API de mediere.

— Există considerații legate de sistemele de operare și de browsere care nu se află sub controlul instrumentelor de implementare, care pot fi luate în considerare astfel cum se indică la notele 2-4 de mai jos:

— *NOTA 2*: o solicitare de prezentare din partea unui beneficiar care este compatibilă cu anexa C la [16] poate fi prelucrată de browser și/sau de sistemul de operare pentru căutarea EAA disponibile, pentru prevenirea fraudei care vizează utilizatorul sau în scopuri de depanare.

— *NOTA 3*: se preconizează că o solicitare de prezentare din partea unui beneficiar care este compatibilă cu anexa C la [16] va fi prelucrată de browser și/sau de sistemul de operare în scopul securității utilizatorului.

— *NOTA 4*: se preconizează că o solicitare de prezentare din partea unui beneficiar care este compatibilă cu anexa C la [16] nu va fi prelucrată de browser și/sau de sistemul de operare în scopuri de analiză de piață (inclusiv ca scop secundar) sau în scopurile interne ale browserului și/sau ale sistemului de operare.

— ISO/IEC 18013-ADD-API-02: în cazul în care un portofel EUDI șterge, la cererea utilizatorului, un PID sau EAA divulgat anterior către API de mediere care funcționează în conformitate cu anexa C la [16], portofelul EUDI divulgă faptul că nu mai stochează aceste PID sau EAA către API de mediere.

— ISO/IEC 18013-ADD-API-03: în cazul în care utilizatorul își dezinstalează portofelul EUDI, portofelul EUDI divulgă faptul că nu mai stochează PID sau EAA divulgate anterior către API de mediere care funcționează în conformitate cu anexa C la [16].

— ISO/IEC 18013-ADD-API-04: portofelul EUDI oferă o setare globală a utilizatorului pentru a dezactiva divulgarea EAA-urilor stocate prin intermediul unei API de mediere care funcționează astfel cum se specifică în ISO/IEC 18013-ADD-API-01. Atunci când această setare este dezactivată, portofelul EUDI nu face publicitate și nu răspunde solicitărilor de prezentare sau de emitere mediate prin AIP.

— ISO/IEC 18013-ADD-API-05: portofelele EUDI verifică în fluxurile între dispozitive, utilizând API de mediere, dacă dispozitivul cu care interacționează se află în proximitatea fizică imediată a portofelului EUDI, utilizând un canal de comunicații local securizat, direct și mediat de utilizator, cum ar fi o tehnologie de comunicații fără fir cu rază scurtă de acțiune pentru a efectua verificarea proximității fizice.

— *NOTĂ*: CTAP 2.3 permite utilizarea BLE pentru a efectua verificarea proximității fizice și, atunci când este implementat de ambele dispozitive, permite, de asemenea, transportul datelor între dispozitive prin intermediul tehnologiilor de transmisie cu rază mică de acțiune. Efectuarea atât a verificării proximității fizice, cât și a transferului de date între cele două dispozitive utilizând un canal de comunicații local, astfel cum permite CTAP 2.3, ar trebui să fie preferată de sistemele de operare subiacente, de browsere, de API de mediere sau de orice alt nivel tehnic aflat în afara controlului portofelului EUDI în detrimentul utilizării serviciilor CTAP de tuneluri hibride de transport.

13. 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: portofelul EUDI trebuie să îndeplinească cerințele specificate în clauza 6.5 din prezenta anexă.

— OIDFVP-HAIP-SUPPORT-03: portofelul EUDI nu ar trebui să accepte mecanismul bazat pe redirecționare specificat în clauza 6.4 pentru fluxurile de prezentare între dispozitive.

— NOTA 3: utilizarea acestui mecanism este vulnerabilă la atacuri, cum ar fi cele bazate pe fixarea identificatorului de sesiune. Atenuarea unor astfel de atacuri este la latitudinea beneficiarilor. Punerea în aplicare a acestui mecanism nu ar trebui să genereze o neconformitate.

— OIDFVP-HAIP-SUPPORT-05: un beneficiar trebuie să îndeplinească cerințele specificate la clauzele 6.5 din prezenta anexă.

— NOTA 5: necompletat.

14. 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: se aplică toate cerințele obligatorii specificate în clauzele 5, 5.3, 7 și 8 din HAIP [11].

— *NOTA 1*: «HAIP [11] secțiunea 5» se referă numai la cerințele prevăzute direct în titlul secțiunii 5. Aici nu sunt incluse secțiunile 5,1, 5.2 și 5.3.

— OIDFVP-HAIP-GEN-03: în cazul în care prezenta anexă modifică o cerință din OpenID4VC-HAIP [11], prevalează cerința modificată specificată în prezenta anexă.

— *NOTA 2*: acest lucru ar permite, de exemplu, transformarea obligatorie a unei cerințe opționale din OpenID4VC-HAIP [11] sau extinderea cerințelor obligatorii.

— OIDFVP-HAIP-GEN-04: atunci când formatul atestatului solicitat respectă [10], beneficiarii și portofelele EUDI respectă profilul «ISO mdocs» prevăzut la secțiunea 6 din [11].

— *NOTA 3*: din motive de claritate, profilul «ISO mdocs» din HAIP implică faptul că beneficiarii și portofelele EUDI respectă cerințele aplicabile din anexa B.2 la [7].

— OIDFVP-HAIP-GEN-05: atunci când formatul atestatului solicitat este conform cu [2], beneficiarii și portofelele EUDI respectă profilul «IETF SD-JWT VCs» din secțiunea 6 la [11].

— *NOTA 4*: din motive de claritate, profilul «IETF SD-JWT VCs» implică faptul că beneficiarii și portofelele EUDI respectă cerințele din anexa B.3 la [7], precum și cerințele din secțiunea 6.1 la [11].

15. 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: void.

16. 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-03: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-04: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-05: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-06: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-07: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-08: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-09: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-10: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-11: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-12: necompletat

— *Nota 2*: necompletat

— OIDFVP-HAIP-COMMON-REQ-RO-13: unul dintre elementele parametrului verifier_info include certificatul de înregistrare.

— OIDFVP-HAIP-COMMON-REQ-RO-23: certificatul de entitate finală menționat în secțiunea 5.9.3 din OpenID4VP pentru utilizare cu x509_hash Client Identifier Prefix este un certificat de acces al PR, astfel cum se specifică în ETSI TS 119 475 [14].

17. 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: necompletat.

18. 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: necompletat.

— *NOTĂ*: necompletat.

19. 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: portofelul EUDI divulgă implicit prezența tuturor tipurilor de EAA stocate către API de mediere care funcționează în conformitate cu clauza 5.2 din [11], dar nu divulgă atributele și valorile acestora din aceste EAA.

— OIDFVP-HAIP-ADD-API-04: în cazul în care portofelul EUDI este compatibil cu o API de mediere care funcționează astfel cum se specifică în OIDFVP-HAIP-ADD-API-01, acesta oferă o setare globală a utilizatorului pentru a dezactiva divulgarea EAA stocate prin intermediul API de mediere. Atunci când această setare este configurată pe divulgare dezactivată, portofelul EUDI ar trebui să permită ulterior utilizatorului să selecteze atestatele individuale care urmează să fie divulgate către API de mediere.

— OIDFVP-HAIP-ADD-API-05: portofelele EUDI verifică, în fluxurile între dispozitive, utilizând API de mediere, dacă dispozitivul de interacțiune se află în imediata apropiere fizică a portofelului EUDI, utilizând un canal de comunicare locală securizat, direct și mediat de utilizator, cum ar fi o tehnologie de comunicații fără fir cu rază scurtă de acțiune pentru a efectua verificarea fizică a proximității.

— *NOTA 5*: CTAP 2.3 permite utilizarea BLE pentru a efectua verificarea proximității fizice și, atunci când este implementat de ambele dispozitive, permite, de asemenea, transportul datelor între dispozitive prin intermediul tehnologiilor de transmisie cu rază mică de acțiune. Efectuarea atât a verificării proximității fizice, cât și a transferului de date între cele două dispozitive utilizând un canal de comunicații local, astfel cum permite CTAP 2.3, ar trebui să fie preferată de sistemele de operare subiacente, de browsere, de API de mediere sau de orice alt nivel tehnic aflat în afara controlului portofelului EUDI în detrimentul utilizării serviciilor CTAP de tuneluri hibride de transport.

20. 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: toate cerințele specificate în prezentul document aplicabile structurilor de solicitare trimise către un dispozitiv și structurilor de răspuns din partea dispozitivului specificate în ISO/IEC 18013-5 se aplică și atunci când portofelul EUDI primește o solicitare de prezentare ISO/IEC mdoc prin intermediul unui mecanism transmis prin AIP specificat în clauza C.1 din [16].”