Úradný vestník
Európskej únie

SK
Séria L

2026/1731

22.7.2026

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2026/1731

z 15. júla 2026,

ktorým sa menia vykonávacie nariadenia (EÚ) 2024/2977, (EÚ) 2024/2979, (EÚ) 2024/2980 a (EÚ) 2024/2982, pokiaľ ide o uplatniteľné normy a špecifikácie

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES ([1]), a najmä na jeho článok 5a ods. 23,

keďže:

(1) S cieľom zabezpečiť najvyššiu úroveň harmonizácie medzi členskými štátmi pri vývoji európskych peňaženiek digitálnej identity sa technické špecifikácie pre peňaženky opierajú o prácu vykonanú na základe odporúčania Komisie (EÚ) 2021/946 ([2]), a najmä o architektúru a referenčný rámec. Keďže architektúra a referenčný rámec sa od prijatia vykonávacích nariadení Komisie (EÚ) 2024/2977 ([3]), (EÚ) 2024/2979 ([4]), (EÚ) 2024/2980 ([5]) a (EÚ) 2024/2982 ([6]) značne vyvinuli, uvedené vykonávacie nariadenia by sa teraz mali zmeniť s cieľom zosúladiť ich s novými normami, špecifikáciami a postupmi.

V súlade s cieľmi nariadenia (EÚ) č. 910/2014 bolo na splnenie týchto osobitných požiadaviek vybraných niekoľko noriem. Tieto normy by mali odrážať zavedené postupy a mali by byť všeobecne uznávané v príslušných odvetviach. Napríklad keďže formát W3C VCDM sa používa ako referenčný formát pre osvedčenia, najmä v sektore vzdelávania, európske peňaženky digitálnej identity by takisto mali tento formát podporovať, keď budú k dispozícii nové profily formátov W3C VCDM. V prípade potreby by sa tieto normy mali upraviť alebo doplniť v záujme zaistenia bezpečnosti a dôveryhodnosti európskych peňaženiek digitálnej identity, a to pri súčasnom uľahčení cezhraničnej interoperability a účinného fungovania vnútorného trhu.

(2) Pri každom použití peňaženky, ktoré si vyžaduje predloženie podobizne používateľa peňaženky, musia riešenia peňaženky podporovať funkciu selektívneho sprístupňovania a sprístupňovanie musí byť plne pod kontrolou používateľa. S cieľom chrániť schopnosť rozhodovať o sprístupňovaní, ako aj podobizeň pred neúmyselnou alebo neoprávnenou žiadosťou o sprístupnenie by sa v architektonickom návrhu európskych peňaženiek digitálnej identity mali stanoviť mechanizmy varovania a zaznamenávanie všetkých transakcií súvisiacich s používaním podobizne. V snahe zabezpečiť, aby bol používateľ peňaženky informovaný o zdieľaní biometrických údajov, by sa vo

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Odporúčanie Komisie (EÚ) 2021/946 z 3. júna 2021 o spoločnom súbore nástrojov Únie pre koordinovaný prístup k európskemu rámcu digitálnej identity (Ú. v. EÚ L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([3]) Vykonávacie nariadenie Komisie (EÚ) 2024/2977 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o osobné identifikačné údaje a elektronické osvedčenia atribútov vydané pre európske peňaženky digitálnej identity (Ú. v. EÚ L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) Vykonávacie nariadenie Komisie (EÚ) 2024/2979 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o integritu a základné funkcie európskych peňaženiek digitálnej identity (Ú. v. EÚ L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) Vykonávacie nariadenie Komisie (EÚ) 2024/2980 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o oznámenia Komisii týkajúce sa ekosystému európskej peňaženky digitálnej identity (Ú. v. EÚ L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Vykonávacie nariadenie Komisie (EÚ) 2024/2982 z 28. novembra 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o protokoly a rozhrania, ktoré má podporovať európsky rámec digitálnej identity (Ú. v. EÚ L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

varovaniach malo uviesť, že žiadosť zahŕňa zdieľanie biometrických údajov, a od používateľa by sa malo vyžadovať konkrétne potvrdenie sprístupnenia. Ak spoliehajúca sa strana spracúva podobizeň na účely jedinečnej identifikácie fyzickej osoby alebo na potvrdenie jej údajnej totožnosti, uplatňujú sa články 6 a 9 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 ([7]), ako aj všetky ostatné požiadavky uvedeného nariadenia vrátane toho, že spracúvanie podobizne spoliehajúcimi sa stranami by sa malo obmedziť na to, čo je nevyhnutné na zamýšľané použitie. Zamýšľané použitie by sa malo používateľovi peňaženky oznámiť spolu so žiadosťou o sprístupnenie v jasnom a zrozumiteľnom jazyku. S cieľom náležite zohľadniť citlivosť biometrických údajov by mal používateľ peňaženky výslovne a konkrétne potvrdiť sprístupnenie podobizne. Mlčanie ani vopred začiarknuté políčka by sa nemali považovať za potvrdenie používateľom peňaženky. Výslovné potvrdenie používateľom peňaženky by malo byť technickou zárukou a samo osebe by nemalo poskytovať právny základ spracúvania. Ako sa stanovuje v článku 9 ods. 4 nariadenia (EÚ) 2016/679, členské štáty môžu zachovať alebo zaviesť ďalšie podmienky vrátane obmedzení týkajúce sa spracúvania genetických údajov, biometrických údajov alebo údajov týkajúcich sa zdravia.

(3) S cieľom poskytnúť členským štátom dostatočný čas na prispôsobenie svojich vnútroštátnych postupov môže podobizeň používateľa peňaženky patriť medzi povinné osobné identifikačné údaje v prípade fyzickej osoby až od 11. augusta 2028. Ak tieto podoby tváre pochádzajú z existujúcich dokladov totožnosti, ako sú preukazy totožnosti alebo cestovné pasy, uplatňujú sa príslušné požiadavky stanovené v nariadení Rady (EÚ) 2025/1208 ([8]) alebo (ES) č. 2252/2004 ([9]).

(4) V nariadení (EÚ) č. 910/2014 sa vyžaduje, aby peňaženky umožňovali zobraziť značku dôvery EÚ pre peňaženku digitálnej identity ako overiteľné, jednoduché a rozpoznateľné označenie toho, že peňaženka bola poskytnutá v súlade s nariadením. Používaním takejto značky dôvery sa podporí účinné fungovanie vnútorného trhu, zaručí sa spravodlivá hospodárska súťaž a ochránia sa záujmy spotrebiteľov. Na umožnenie používania takejto značky dôvery by sa mali stanoviť jej vizuálne a technické vlastnosti.

(5) Ako sa stanovuje v článku 12b nariadenia (EÚ) č. 910/2014, strážcovia prístupu majú umožniť poskytovateľom európskych peňaženiek digitálnej identity a vydavateľom oznámených prostriedkov elektronickej identifikácie skutočnú interoperabilitu s rovnakým operačným systémom a hardvérovými alebo softvérovými funkciami a prístup k nim na účely interoperability. Takáto skutočná interoperabilita a prístup sa majú poskytovať bezplatne a bez ohľadu na to, či sú tieto hardvérové alebo softvérové funkcie súčasťou operačného systému, ktoré má daný strážca prístupu k dispozícii alebo ktoré tento strážca prístupu používa pri poskytovaní takýchto služieb. Keďže všetky riešenia peňaženky by mali podporovať spoločný súbor protokolov a rozhraní s cieľom zabezpečiť použiteľnosť, bezpečnosť a interoperabilitu vo všetkých členských štátoch, strážcovia prístupu by mali umožniť operačný systém a hardvérové alebo softvérové funkcie potrebné na implementáciu protokolov a rozhraní stanovených v prílohe XII k tomuto nariadeniu. V tejto súvislosti by strážcovia prístupu mali pri online tokoch medzi zariadeniami, pokiaľ ide o kontrolu fyzickej blízkosti aj prenos údajov medzi týmito dvoma zariadeniami, uprednostniť miestny komunikačný kanál, ktorý umožňuje špecifikácia protokolu CTAP (Client To Authenticator Protocol) verzie 2.3 ([10]), pred použitím hybridných tunelových služieb CTAP.

(6) S cieľom poskytnúť členským štátom, poskytovateľom registračných certifikátov strany spoliehajúcej sa na peňaženku a poskytovateľom peňaženky dostatočný čas na to, aby jednotkám peňaženky umožnili autentifikovať a validovať registračné certifikáty strany spoliehajúcej sa na peňaženku, by sa táto požiadavka mala uplatňovať až od 11. augusta 2028.

(7) Na všetky činnosti spracúvania osobných údajov podľa tohto nariadenia sa vzťahuje nariadenie (EÚ) 2016/679 a v relevantných prípadoch smernica Európskeho parlamentu a Rady 2002/58/ES ([11]).

([7]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Nariadenie Rady (EÚ) 2025/1208 z 12. júna 2025 o posilnení zabezpečenia preukazov totožnosti občanov Únie a dokladov o pobyte vydávaných občanom Únie a ich rodinným príslušníkom vykonávajúcim svoje právo na voľný pohyb (Ú. v. EÚ L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Nariadenie Rady (ES) č. 2252/2004 z 13. decembra 2004 o normách pre bezpečnostné znaky a biometriu v pasoch a cestovných dokladoch vydávaných členskými štátmi (Ú. v. EÚ L 385, 29.12.2004, s. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Norma navrhnutá alianciou FIDO, Client to Authenticator Protocol (CTAP), 26. februára 2026.

([11]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([12]) sa uskutočnili konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý 17. apríla 2026 vydal svoje stanovisko ([13]).

(9) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru zriadeného podľa článku 48 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO NARIADENIE:

Článok 1

Zmeny vykonávacieho nariadenia (EÚ) 2024/2977

Vykonávacie nariadenie (EÚ) 2024/2977 sa mení takto:

1. Vkladá sa tento článok 3a:

„*Článok 3a*

Ochrana podobizne

1. Okrem požiadaviek na informácie podľa nariadenia (EÚ) 2016/679 poskytovatelia peňaženky zabezpečia, aby riešenia peňaženky, ktoré poskytujú, vydávali varovania pre používateľov peňaženky, ak strany spoliehajúce sa na peňaženku požiadajú o sprístupnenie podobizne, v ktorých uvedú, že žiadosť zahŕňa zdieľanie biometrických údajov a vyžaduje si potvrdenie selektívneho sprístupnenia podobizne.

2. Na implementáciu selektívneho sprístupňovania podobizne strane spoliehajúcej sa na peňaženku poskytovatelia peňaženky zabezpečia, aby sa v riešeniach peňaženky od používateľa peňaženky vyžadovalo výslovné a konkrétne potvrdenie predloženia podobizne.

3. Strany spoliehajúce sa na peňaženku nesmú podobizeň uchovávať, ak jej spracúvanie nie je potrebné na účely identifikácie a autentifikácie v súlade s právom Únie v oblasti ochrany údajov ani sa to nestanovuje v práve Únie alebo vo vnútroštátnom práve v súlade s právom Únie v oblasti ochrany údajov. Podobizeň sa nesmie prenášať do tretích krajín ani medzinárodným organizáciám, ak to nepovoľuje právo Únie v oblasti ochrany údajov.“

2. V článku 4 sa odsek 1 nahrádza takto:

„1. Elektronické osvedčenia atribútov vydané jednotkám peňaženky musia spĺňať aspoň jednu z noriem stanovených v prílohe II k vykonávaciemu nariadeniu (EÚ) 2024/2979.“

3. V článku 5 ods. 4 sa písmeno b) nahrádza takto:

„b) ak bolo zrušené osvedčenie jednotky peňaženky, ktoré má jednotka peňaženky, ktorej boli osobné identifikačné údaje vydané;“.

4. Príloha sa nahrádza textom uvedeným v prílohe I k tomuto nariadeniu.

([12]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 [Formálne pripomienky EDPS k návrhu vykonávacieho nariadenia, pokiaľ ide o uplatniteľné normy a špecifikácie a opravu vykonávacieho nariadenia (EÚ) 2024/2980] |európsky dozorný úradník pre ochranu údajov.

Článok 2

Zmeny vykonávacieho nariadenia (EÚ) 2024/2979

Vykonávacie nariadenie (EÚ) 2024/2979 sa mení takto:

1. V článku 3 sa vypúšťa odsek 2.

2. V článku 5 ods. 1 sa písmeno a) nahrádza takto:

„a) vykonávali kryptografické operácie peňaženky zahŕňajúce kritické aktíva uložené v zabezpečenom kryptografickom zariadení peňaženky, ktoré sa nevyžadujú na autentifikáciu používateľa peňaženky, len v prípadoch, keď tieto aplikácie úspešne autentifikovali používateľov peňaženky;“.

3. Vkladá sa tento článok 5a:

„*Článok 5a*

Kryptografické mechanizmy

Poskytovatelia peňaženky používajú na účely článku 4 ods. 2 len kryptografické mechanizmy uvedené v prílohe Ia.“

4. Článok 6 sa mení takto:

a) odsek 1 sa nahrádza takto:

„1. Poskytovatelia peňaženky vydajú osvedčenia jednotky peňaženky pre každú jednotku peňaženky. Poskytovatelia peňaženky podpíšu alebo zapečatia osvedčenia jednotky peňaženky tak, aby sa podpisy alebo pečate mohli overiť prostredníctvom certifikátu uvedeného v zozname v súlade s oddielom 2 bodom 1 písm. h) prílohy II k vykonávaciemu nariadeniu (EÚ) 2024/2980.“;

b) odsek 2 sa nahrádza takto:

„2. Poskytovatelia peňaženky zabezpečia, aby osvedčenia jednotky peňaženky uvedené v odseku 1 boli v súlade s technickými špecifikáciami stanovenými v prílohe Ib.“;

c) v odseku 3 sa písmeno b) nahrádza takto:

„b) poskytujú používateľom peňaženky bezpečné mechanizmy identifikácie a autentifikácie, ktoré sú nezávislé od jednotiek peňaženky;“.

5. V článku 9 ods. 2 sa písmeno b) nahrádza takto:

„b) meno, kontaktné údaje a jedinečný identifikátor príslušnej strany spoliehajúcej sa na peňaženku a členský štát, v ktorom je táto strana spoliehajúca sa na peňaženku usadená;“.

6. V článku 10 sa odsek 1 nahrádza takto:

„1. Poskytovatelia peňaženky zabezpečia, aby jednotky peňaženky, ktoré poskytujú, mohli spracúvať elektronické osvedčenia atribútov vydané v súlade s technickými špecifikáciami platnými pre spoločné zahrnuté pravidlá sprístupňovania informácií stanovené v prílohe III.“

7. Článok 12 sa mení takto:

a) v odseku 2 sa písmeno c) nahrádza takto:

„c) vyhotovenie podpisov alebo pečatí aspoň v súlade s povinnými formátmi podpisu alebo pečate uvedenými v prílohe IV;“

b) odsek 3 sa nahrádza takto:

„3. Aplikácie na vyhotovenie podpisu môžu byť buď integrované do inštancií peňaženky, alebo môžu byť externé.“;

c) vkladá sa tento odsek:

„4. Aplikácie na vyhotovenie podpisu, ktoré používajú jednotky peňaženky, podporujú aspoň aplikačné programovacie rozhranie uvedené v prílohe IV.“

8. V článku 14 sa vypúšťa odsek 1.

9. Vkladá sa tento článok 14a:

„Článok 14a

Značka dôvery EÚ pre peňaženku digitálnej identity

1. Poskytovatelia peňaženky zabezpečia, aby jednotky peňaženky zobrazovali značku dôvery EÚ pre peňaženku digitálnej identity. Značka dôvery EÚ pre peňaženku digitálnej identity má podobu uvedenú v prílohách VI a VII.

2. Poskytovatelia peňaženky zabezpečia, aby jednotky peňaženky umožňovali používateľom peňaženky prístup k informáciám na overenie stavu certifikácie riešenia peňaženky. Na tento účel poskytovatelia peňaženky zabezpečia, aby príslušné jednotky peňaženky po registrácii riešenia peňaženky obsahovali adresy URL, ktoré na takéto overovanie poskytuje Európska komisia. Poskytovatelia peňaženky zabezpečia, aby ich jednotky peňaženky mali prístup k údajom o značke dôvery EÚ pre peňaženku digitálnej identity, ktoré sú v súlade s technickými špecifikáciami stanovenými v prílohe VIII.

3. Referenčné farby pre značku dôvery EÚ pre peňaženku digitálnej identity sú Pantone č. 661 a 116 alebo modrá (100 % azúrovej + 67 % purpurovej + 0 % žltej + 40 % čiernej) a žltá (0 % purpurovej + 20 % purpurovej + 100 % žltej + 0 % čiernej), ak sa používa štvorfarebná tlač; ak sa používa farebný model RGB, referenčnou farbou je modrá (0 červená + 51 zelená + 153 modrá) a žltá (255 červená + 204 zelená + 0 modrá).

4. Značka dôvery EÚ pre peňaženku digitálnej identity sa môže používať v čiernobielej verzii, ako sa uvádza v prílohe VII, iba v prípade, keď sa nedajú použiť farby.

5. Ak sa značka dôvery EÚ pre peňaženku digitálnej identity používa na tmavom pozadí, môže sa použiť v negatívnom formáte s použitím rovnakej farby pozadia. Ak sa značka dôvery EÚ pre peňaženku digitálnej identity používa vo farbách na farebnom pozadí, na ktorom je slabo viditeľná, môže sa v záujme zvýšenia kontrastu s farbami pozadia ohraničiť vonkajšou čiarou.

6. Značka dôvery EÚ pre peňaženku digitálnej identity má minimálnu veľkosť 64 × 85 pixelov s rozlíšením 150 DPI.

7. Poskytovatelia peňaženky zabezpečia, aby sa značka dôvery EÚ pre peňaženku digitálnej identity používala spôsobom, ktorý umožní jasné označenie jednotky peňaženky, na ktorú sa táto značka vzťahuje. Značka dôvery EÚ pre peňaženku digitálnej identity sa môže spájať s grafickými alebo textovými prvkami jasne označujúcimi jednotku peňaženky, pre ktorú sa používa, za predpokladu, že tieto prvky nemenia jej rozpoznateľnosť ako značky dôvery EÚ pre peňaženku digitálnej identity ani neupravujú prepojenie so zoznamom certifikovaných európskych peňaženiek digitálnej identity uvedeným v článku 5d nariadenia (EÚ) č. 910/2014.

8. Ak poskytovatelia peňaženky zrušia osvedčenie jednotky peňaženky, zabezpečia, aby príslušná jednotka peňaženky už nezobrazovala značku dôvery EÚ pre peňaženku digitálnej identity.“

10. Dopĺňajú sa prílohy Ia a Ib, ako sa stanovujú v prílohách II a III k tomuto nariadeniu.

11. Príloha II sa nahrádza prílohou IV k tomuto nariadeniu.

12. Príloha III sa nahrádza prílohou V k tomuto nariadeniu.

13. Príloha IV sa mení v súlade s prílohou VI k tomuto nariadeniu.

14. Príloha V sa vypúšťa.

15. Text uvedený v prílohe VII k tomuto nariadeniu sa vkladá ako príloha VI.

16. Text uvedený v prílohe VIII k tomuto nariadeniu sa vkladá ako príloha VII.

17. Text uvedený v prílohe IX k tomuto nariadeniu sa vkladá ako príloha VIII.

Článok 3

Zmeny vykonávacieho nariadenia (EÚ) 2024/2980

Vykonávacie nariadenie (EÚ) 2024/2980 sa mení takto:

1. V článku 5 sa odsek 2 nahrádza takto:

„2. Komisia v príslušných prípadoch vytvorí, vedie a uverejňuje zoznam, v ktorom sú zhromaždené informácie oznámené členskými štátmi o poskytovateľoch peňaženky, poskytovateľoch osobných identifikačných údajov, poskytovateľoch prístupových certifikátov strany spoliehajúcej sa na peňaženku a poskytovateľoch registračných certifikátov strany spoliehajúcej sa na peňaženku, ako je uvedené v oddieloch 2, 3, 4 a 5 prílohy II.“

2. Príloha II k vykonávaciemu nariadeniu (EÚ) 2024/2980 sa mení v súlade s prílohou X k tomuto nariadeniu.

Článok 4

Zmeny vykonávacieho nariadenia (EÚ) 2024/2982

Vykonávacie nariadenie (EÚ) 2024/2982 sa mení takto:

1. V článku 1 sa odsek 2 nahrádza takto:

„2. predkladanie atribútov osobných identifikačných údajov a elektronických osvedčení atribútov stranám spoliehajúcim sa na peňaženku;“.

2. Článok 3 sa mení takto:

a) odsek 1 sa nahrádza takto:

„1. autentifikovali a validovali prístupové certifikáty strán spoliehajúcich sa na peňaženku, ak komunikujú so stranami spoliehajúcimi sa na peňaženku, a to bez delegovania výkonu týchto procesov na operačný systém alebo prehliadač alebo inú sprostredkovateľskú aplikáciu;“

b) odsek 2 sa vypúšťa;

c) odsek 3 sa nahrádza takto:

„3. autentifikovali a validovali žiadosti podané s použitím prístupových certifikátov strany spoliehajúcej sa na peňaženku;“

d) odsek 4 sa nahrádza takto:

„4. autentifikovali a validovali registračný certifikát strany spoliehajúcej sa na peňaženku;“

e) odsek 5 sa nahrádza takto:

„5. zobrazovali používateľom peňaženky informácie obsiahnuté v prístupových certifikátoch strany spoliehajúcej sa na peňaženku;“

f) odsek 8 sa vypúšťa;

g) odsek 9 sa nahrádza takto:

„9. nepredkladali žiaden požadovaný atribút stranám spoliehajúcim sa na peňaženku, kým nie sú vykonané tieto kroky:

a) overenie, že sa v rámci jednotky peňaženky spracovali zahrnuté pravidlá sprístupňovania informácií v súlade s článkom 10 vykonávacieho nariadenia (EÚ) 2024/2979;

b) overenie, že používatelia peňaženky predloženie čiastočne alebo v plnej miere schválili.“

3. V článku 4 sa odsek 1 nahrádza takto:

„1. Poskytovatelia peňaženky zabezpečia, aby riešenia peňaženky podporovali protokoly a rozhrania stanovené v prílohe I na vydávanie osobných identifikačných údajov a elektronických osvedčení atribútov jednotkám peňaženky.“

4. Článok 5 sa mení takto:

   a) odseky 1 a 2 sa nahrádzajú takto:

      „1. Poskytovatelia peňaženky zabezpečia, aby riešenia peňaženky podporovali protokoly a rozhrania na predkladanie atribútov stranám spoliehajúcim sa na peňaženku na diaľku a prípadne v blízkosti v súlade s technickými špecifikáciami stanovenými v prílohe II.

      2. Poskytovatelia peňaženky zabezpečia, aby jednotky peňaženky na požiadanie používateľov odpovedali na úspešne autentifikované a validované žiadosti strán spoliehajúcich sa na peňaženku uvedené v článku 3 v súlade s technickými špecifikáciami stanovenými v prílohe II.“;

   b) odsek 5 sa vypúšťa.

5. Článok 8 sa nahrádza takto:

   „Článok 8

   Nadobudnutie účinnosti

   Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

   Článok 3 ods. 4 sa uplatňuje od 11. augusta 2028.

   Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.“

6. Príloha sa vypúšťa.

7. Text uvedený v prílohe XI k tomuto nariadeniu sa dopĺňa ako príloha I.

8. Text uvedený v prílohe XII k tomuto nariadeniu sa dopĺňa ako príloha II.

Článok 5

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 15. júla 2026

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA I

„PRÍLOHA

Technické špecifikácie pre osobné identifikačné údaje uvedené v článku 3 ods. 3

1. Oddiel 1: Súbor identifikačných údajov fyzických osôb

Tabuľka 1

Povinné osobné identifikačné údaje pre selektívne sprístupňovanie v prípade fyzickej osoby

Identifikátor údajov	Definícia
`family_name`	Aktuálne priezvisko (-á) používateľa, na ktorého sa vzťahujú osobné identifikačné údaje.
`given_name`	Aktuálne meno (-á), prípadne aj prostredné meno (-á) používateľa, na ktorého sa vzťahujú osobné identifikačné údaje.
`birth_date`	Deň, mesiac a rok narodenia používateľa, na ktorého sa vzťahujú osobné identifikačné údaje.
`birth_place`	Krajina označená kódom krajiny alpha-2 podľa normy ISO 3166-1 alebo štát, provincia, okres alebo miestna oblasť, alebo obec, mesto alebo dedina, kde sa narodil používateľ, na ktorého sa vzťahujú osobné identifikačné údaje.
`nationality`	Jeden alebo viacero kódov krajiny alpha-2 podľa normy ISO 3166-1, ktoré predstavujú štátnu príslušnosť používateľa, na ktorého sa vzťahujú osobné identifikačné údaje.
`portrait`	V príslušných prípadoch podoba tváre používateľa, na ktorého sa vzťahujú osobné identifikačné údaje, spĺňajúca požiadavky na kvalitu pre úplný frontálny typ snímky stanovené v norme ISO/IEC 39794-5 alebo v prípade spätnej kompatibility v bodoch 8.2, 8.3 a 8.4 normy ISO/IEC 19794-5, ktorá sa poskytuje ako kódované údaje o podobe tváre bez hlavičiek alebo blokov podľa bodu 5 normy ISO/IEC 19794-5, okrem samotných údajov o podobe tváre (JPEG), a to okrem prípadov, keď sa používateľ výslovne rozhodne nepoužívať ju, sa uplatňuje od 11. augusta 2028.

— Členské štáty môžu stanoviť, aby mal používateľ možnosť odmietnuť vloženie podobizne do osobných identifikačných údajov.

— Členské štáty zabezpečia, aby sa selektívne sprístupňovanie vzťahovalo na každý identifikátor údajov vrátane podobizne.

— Ak dátum narodenia fyzickej osoby nie je známy, členské štáty zvolia vhodné hodnoty, ktoré sú v súlade so špecifikáciami stanovenými v oddieloch 4.1 alebo 4.2 (podľa potreby) tejto prílohy.

— Ak štátna príslušnosť fyzickej osoby nie je známa, členské štáty použijú hodnotu ‚QU'.

— Ak fyzická osoba nemá štátnu príslušnosť, členské štáty použijú hodnotu ‚QS'.

— Ak sa používateľ rozhodne odmietnuť zahrnutie podobizne, členské štáty nastavia hodnotu ako prázdnu.

Tabuľka 2

Nepovinné osobné identifikačné údaje pre selektívne sprístupňovanie v prípade fyzickej osoby

Identifikátor údajov	Definícia
resident_address	Úplná adresa miesta, kde má používateľ, na ktorého sa vzťahujú osobné identifikačné údaje, v súčasnosti bydlisko alebo kde ho možno kontaktovať (názov ulice, číslo domu, mesto atď.).
resident_country	Krajina označená kódom krajiny alpha-2 podľa normy ISO 3166-1, v ktorej má používateľ, na ktorého sa vzťahujú osobné identifikačné údaje, v súčasnosti bydlisko.
resident_state	Štát, provincia, okres alebo miestna oblasť, kde má používateľ, na ktorého sa vzťahujú osobné identifikačné údaje, v súčasnosti bydlisko.
resident_city	Obec, mesto alebo dedina, kde má používateľ, na ktorého sa vzťahujú osobné identifikačné údaje, v súčasnosti bydlisko.
resident_postal_code	Poštové smerovacie číslo miesta, kde má používateľ, na ktorého sa vzťahujú osobné identifikačné údaje, v súčasnosti bydlisko.
resident_street	Názov ulice vrátane čísla domu a akejkoľvek predpony alebo prípony, kde má používateľ, na ktorého sa vzťahujú osobné identifikačné údaje, v súčasnosti bydlisko.
personal_administrative_-number	Hodnota pridelená používateľovi, na ktorého sa vzťahujú osobné identifikačné údaje, ktorá je jedinečná medzi všetkými osobnými administratívnymi číslami vydanými poskytovateľom osobných identifikačných údajov. Ak sa členské štáty rozhodnú zahrnúť tento atribút, vo svojich schémach elektronickej identifikácie, v rámci ktorých sa vydávajú osobné identifikačné údaje, opíšu pravidlá, ktoré uplatňujú na hodnoty tohto atribútu, prípadne vrátane osobitných podmienok spracovania tejto hodnoty.
family_name_birth	Priezvisko (-á) používateľa, na ktorého sa vzťahujú osobné identifikačné údaje, v čase narodenia.
given_name_birth	Meno (-á) vrátane prostredného mena (mien) používateľa, na ktorého sa vzťahujú osobné identifikačné údaje, v čase narodenia.
sex	Hodnoty patria do niektorej z týchto kategórií: 0 = neznáme, 1 = muž, 2= žena, 3 = iné, 4 = intersexuálna osoba, 5 = transrodová osoba, 6 = otvorené, 9 = neuplatňuje sa. V prípade hodnôt 0, 1, 2 a 9 sa uplatňuje norma ISO/IEC 5218.
email_address	Elektronická mailová adresa používateľa, na ktorého sa vzťahujú osobné identifikačné údaje [v súlade s normou RFC 5322 ([1])].

Identifikátor údajov	Definícia
`mobile_phone_number`	Číslo mobilného telefónu používateľa, na ktorého sa vzťahujú osobné identifikačné údaje, začínajúce symbolom ‚+' ako medzinárodná predpona a predvoľbou krajiny, za ktorými nasledujú iba čísla.

([1]) P. Resnick, Ed., ‚*Internet Message Format*' (Formát internetových správ), RFC 5322, október 2008.

2. Oddiel 2: Súbor identifikačných údajov právnických osôb

Tabuľka 3

Povinné osobné identifikačné údaje v prípade právnickej osoby

Identifikátor údajov
Súčasný úradný názov
Jedinečný identifikátor vytvorený odosielajúcim členským štátom v súlade s technickými špecifikáciami na účely cezhraničnej identifikácie a pokiaľ možno následne nemenený

— Ak identifikátor údajov nie je pre danú osobu známy alebo ho nemožno vydať inak ako súčasť súboru osobných identifikačných údajov, členské štáty namiesto neho použijú hodnotu atribútu vhodnú pre danú situáciu.

Tabuľka 4

Nepovinné osobné identifikačné údaje v prípade právnickej osoby

Identifikátor údajov
Súčasná adresa
Registračné číslo na účely DPH
Daňové referenčné číslo
Európsky jedinečný identifikačný znak uvedený v smernici Európskeho parlamentu a Rady (EÚ) 2017/1132 ([1])
Identifikátor právneho subjektu (LEI) uvedený vo vykonávacom nariadení Komisie (EÚ) 2022/1860 ([2])
Číslo registrácie a identifikácie hospodárskych subjektov (EORI) uvedené vo vykonávacom nariadení Komisie (EÚ) č. 1352/2013 ([3])
Číslo pre spotrebnú daň stanovené v článku 2 bode 12 nariadenia Rady (EÚ) č. 389/2012 ([4])

([1]) Smernica Európskeho parlamentu a Rady (EÚ) 2017/1132 zo 14. júna 2017 týkajúca sa niektorých aspektov práva obchodných spoločností (Ú. v. EÚ L 169, 30.6.2017, s. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Vykonávacie nariadenie Komisie (EÚ) 2022/1860 z 10. júna 2022, ktorým sa stanovujú vykonávacie technické normy na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012, pokiaľ ide o štandardy, formáty, frekvenciu, metódy a mechanizmy ohlasovania (Ú. v. EÚ L 262, 7.10.2022, s. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Vykonávacie nariadenie Komisie (EÚ) č. 1352/2013 zo 4. decembra 2013, ktorým sa stanovujú formuláre podľa nariadenia Európskeho parlamentu a Rady (EÚ) č. 608/2013 o presadzovaní práv duševného vlastníctva colnými orgánmi (Ú. v. EÚ L 341, 18.12.2013, s. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Nariadenie Rady (EÚ) č. 389/2012 z 2. mája 2012 o administratívnej spolupráci v oblasti spotrebných daní a zrušení nariadenia (ES) č. 2073/2004 (Ú. v. EÚ L 121, 8.5.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. Oddiel 3: Súbor metaúdajov o osobných identifikačných údajoch

Tabuľka 5

Metaúdaje o osobných identifikačných údajoch

Identifikátor údajov	Definícia	Prítomnosť
`issuing_authority`	Názov správneho orgánu, ktorý osobné identifikačné údaje vydal, alebo kód krajiny alpha-2 príslušného členského štátu podľa normy ISO 3166, ak neexistuje samostatný orgán oprávnený vydávať osobné identifikačné údaje.	povinný údaj
`issuing_country`	Kód krajiny alpha-2 označujúci krajinu alebo územie poskytovateľa osobných identifikačných údajov podľa normy ISO 3166-1.	povinný údaj
`expiry_date`	Dátum (a podľa možnosti aj čas) skončenia obdobia administratívnej platnosti osobných identifikačných údajov.	nepovinný údaj
`document_number`	Číslo osobných identifikačných údajov, ktoré prideľuje poskytovateľ osobných identifikačných údajov.	nepovinný údaj
`issuing_jurisdiction`	Kód nižšej územnej jednotky krajiny jurisdikcie, ktorá osobné identifikačné údaje vydala, podľa bodu 8 normy ISO 3166-2:2020. Prvá časť kódu je rovnaká ako hodnota pre krajinu vydania.	nepovinný údaj
`issuance_date`	Dátum, a ak je to možné, aj čas začatia obdobia administratívnej platnosti osobných identifikačných údajov.	nepovinný údaj

4. Oddiel 4: Kódovanie atribútov identifikačných údajov fyzických osôb

— Identifikačné údaje fyzických osôb sa vydávajú v súlade s normami stanovenými v prílohe II k vykonávaciemu nariadeniu (EÚ) 2024/2979, bodoch 5 (formát SD-JWT VC) a 6 (formát ISO/IEC-mdoc), ktoré sa vzťahujú na elektronické osvedčenia atribútov. Body 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3,6.2.4 a 6.2.5 sa neuplatňujú.

— Kódovanie identifikačných údajov fyzických osôb musí byť v súlade s technickými špecifikáciami v oddieloch 4.1 a 4.2 tejto prílohy.

4.1. Kódovanie identifikačných údajov fyzických osôb vo formáte ISO/IEC-mdoc

— Typ osvedčenia pre osobné identifikačné údaje vo formáte ISO/IEC mdoc je ‚eu.europa.ec.eudi.pid.1'. Identifikátor priestoru názvov pre atribúty osobných identifikačných údajov uvedené v tejto prílohe je ‚eu.europa.ec.eudi.pid.1'.

— Ak osobné identifikačné údaje obsahujú údaje, ktorých identifikátory údajov nie sú uvedené v tejto prílohe, tieto údaje sa definujú v rámci domáceho priestoru názvov osobných identifikačných údajov, ktorý používa všeobecný formát eu.europa.ec.eudi.pid. [kód krajiny alpha-2 podľa normy ISO 3166-1 alebo kód regiónu podľa normy ISO 3166-2], za ktorým nasleduje nepovinná bodka a číslo verzie.

— Ak sa používa domáci priestor názvov, jeho schéma vrátane všetkých identifikátorov údajov, ich definícií, prítomnosti a formátov kódovania sa uverejní v súlade s článkom 8 vykonávacieho nariadenia Komisie (EÚ) 2025/1569 ([1]).

— Osobné identifikačné údaje a ich metaúdaje uvedené v oddieloch 1 a 3 tejto prílohy sa zahrnú do prvkov osobných identifikačných údajov v zmysle špecifikácií formátu ISO/IEC mdoc.

— Člen deviceKey v rámci člena deviceKeyInfo inštancie typu MobileSecurityObject obsahuje verejný kľúč.

— Tento verejný kľúč zodpovedá súkromnému kľúču, ktorý je uložený v zabezpečenom kryptografickom zariadení peňaženky (ďalej len ‚WSCD‘) používateľa peňaženky.

— Chránené záhlavie digitálneho podpisu CB-AdES, ktorým sa podpisujú osobné identifikačné údaje vo formáte ISO/IEC-mdoc, obsahuje parametre záhlavia x5u a x5t, ktoré sú špecifikované v norme RFC 9360 ([2]).

— V parametri záhlavia x5t sa používa hašovací (digest) algoritmus SHA-256.

— Požiadavky na kódovanie osobných identifikačných údajov vo formáte ISO/IEC-mdoc sú uvedené v tabuľke 6:

Tabuľka 6

Požiadavky na kódovanie osobných identifikačných údajov vo formáte ISO/IEC-mdoc

Identifikátor údajov	Identifikátor atribútu	Formát kódovania
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]) Vykonávacie nariadenie Komisie (EÚ) 2025/1569 z 29. júla 2025, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o kvalifikované elektronické osvedčenia atribútov a elektronické osvedčenia atribútov poskytované subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene (Ú. v. EÚ 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*‘ (Parametre záhlavia pre prenos a odkazovanie na certifikáty X.509) (https://datatracker.ietf.org/doc/rfc9360/).

Identifikátor údajov	Identifikátor atribútu	Formát kódovania
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate alebo 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 alebo full-date

— Pri zápise formátu kódovania atribútov uvedených v tabuľke 6 sa používajú typy zobrazenia podľa normy RFC 8610 ([3]) s týmito dodatočnými požiadavkami:

a) tstr sa kóduje v UTF-8;

b) tstr podporuje celý rozsah Unicode;

c) tstr má maximálnu dĺžku 150 znakov;

d) dátum sa kóduje podľa normy RFC 8943 ([4]);

e) atribút full-date predstavuje #6.1004(tstr), pričom tag 1004 je špecifikovaný v norme RFC 8943;

f) atribút tdate obsahuje reťazec dátumu a času podľa normy RFC 3339 ([5]);

g) atribút full-date obsahuje reťazec full-date podľa normy RFC 3339, a to v súlade s normou RFC 8943;

h) zobrazenie dátumu v atribútoch, ak nie je uvedené inak:

— nepoužívajú sa zlomky sekúnd,

— nepoužíva sa miestny posun od UTC a časový posun podľa normy RFC 3339 je nastavený na ‚Z‘;

i) celé číslo s hlavnými typmi 0 a 1 je čo najmenšie, ako sa špecifikuje v oddiele 4.2 normy RFC 8949 ([6]);

j) place_of_birth obsahuje aspoň jednu z týchto dvojíc kľúč – hodnota: ‚country‘, ‚region‘ alebo ‚locality‘;

k) vyjadrenie dĺžky v bstr, tstr, poli alebo mape je čo najkratšie, ako sa špecifikuje v oddiele 4.2 normy RFC 8949;

([3]) C. Vigano a H. Birkholz, ‚*Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures*‘ [Stručný jazyk definície údajov (CDDL): notačná konvencia na vyjadrenie štruktúr údajov vo formáte stručnej reprezentácie binárnych objektov (CBOR) a JSON], RFC 8610, jún 2019.

([4]) M. Jones, A. Nadalin a J. Richter, ‚*Concise Binary Object Representation (CBOR) Tags for Date*‘ [Značky pre dátum vo formáte stručnej reprezentácie binárnych objektov (CBOR)], RFC 8943, november 2020.

([5]) G. Klyne a C. Newman, ‚*Date and Time on the Internet: Timestamps*‘ (Dátum a čas na internete: časové pečiatky), RFC 3339, júl 2002.

([6]) C. Bormann a P. Hoffman, ‚*Concise Binary Object Representation (CBOR)*‘ [Stručná reprezentácia binárnych objektov (CBOR)], RFC 8949, december 2020.

l) atribút štátna príslušnosť sa kóduje ako pole kódov krajín alpha-2 podľa normy ISO 3166-1. Ak sa používa zápis v CDDL podľa normy RFC 8610, kódovanie tohto atribútu je:

— nationalities = [+ CountryCode],

— CountryCode = tstr; kód krajiny alfa-2 podľa normy ISO 3166-1,

— ak má používateľ peňaženky, na ktorého sa vzťahujú osobné identifikačné údaje, viacero štátnych príslušností a poskytovateľ osobných identifikačných údajov osvedčuje tieto viaceré štátne príslušnosti, poskytovateľ osobných identifikačných údajov môže do osobných identifikačných údajov zahrnúť všetky štátne príslušnosti,

— atribút place_of_birth sa kóduje ako typ place_of_birth. Ak sa používa zápis v CDDL podľa normy RFC 8610, kódovanie tohto atribútu je:

place_of_birth =

{

? ‚country': tstr; jediný kód krajiny alfa-2 podľa normy ISO 3166-1

? ‚region': tstr; názov štátu, provincie, okresu alebo miestnej oblasti

? ‚locality': tstr; názov obce, mesta alebo dediny

}

4.2. Požiadavky na kódovanie osobných identifikačných údajov vo formáte SD-JWT VC

— Osobné identifikačné údaje a ich metaúdaje uvedené v tomto oddiele sa zahrnú do osobných identifikačných údajov ako tvrdenia v zmysle špecifikácií formátu SD-JWT VC.

— Všetky tvrdenia vo vydaných osobných identifikačných údajoch uvedených v predchádzajúcej zarážke musia byť individuálne selektívne sprístupniteľné, s výnimkou tých údajov, ktoré sú vo formáte SD-JWT VC definované ako neselektívne sprístupniteľné.

— V tabuľke 7 sa špecifikuje kódovanie názvov tvrdení, ktoré sú verejnými názvami.

— V tabuľke 8 sa špecifikuje kódovanie názvov tvrdení, ktoré sa týkajú konkrétnych osobných identifikačných údajov.

— Reťazec JSON použitý v osobných identifikačných údajoch kódovaných vo formáte SD-JWT VC musí byť kódovaný vo formáte UTF-8 a musí podporovať celý rozsah Unicode, pokiaľ sa v tabuľke 8 alebo v odkazoch v nej výslovne neuvádza inak.

— Na vyjadrenie obdobia technickej platnosti osobných identifikačných údajov, ktoré sú v súlade s formátom SD-JWT VC, sa používajú tvrdenia JWT nbf a exp definované v norme RFC 7519 ([7]).

([7]) J. Jones a kol., *‚JSON Web Token (JWT)'* [Webový token JSON (JWT)], RFC 7519, máj 2015.

— Osobné identifikačné údaje obsahujú tvrdenie cnf, ako je definované v norme RFC 7800 ([8]), ktoré je verejným kľúčom vygenerovaným zo súkromného kľúča uloženého v zariadení WSCD jednotky peňaženky používateľa peňaženky.

— Chránené záhlavie digitálneho podpisu, ktorým sa podpisujú osobné identifikačné údaje vo formáte SD-JWT VC, obsahuje parametre záhlavia x5u a x5t#S256 podľa normy RFC 7515 ([9]).

Tabuľka 7

Požiadavky na kódovanie osobných identifikačných údajov vo formáte SD-JWT VC s použitím verejných názvov

Identifikátor údajov	Identifikátor atribútu	Formát kódovania
`family_name`	`family_name`	reťazec
`given_name`	`given_name`	reťazec
`birth_date`	`birthdate`	reťazec, ISO 8601-1, formát RRRR-MM-DD
`birth_place`	`place_of_birth`	štruktúra JSON
`nationality`	`nationalities`	pole reťazcov
`resident_address`	`address.formatted`	reťazec
`resident_country`	`address.country`	reťazec
`resident_state`	`address.region`	reťazec
`resident_city`	`address.locality`	reťazec
`resident_postal_code`	`address.postal_code`	reťazec
`resident_street`	`address.street_address`	reťazec
`family_name_birth`	`birth_family_name`	reťazec
`given_name_birth`	`birth_given_name`	reťazec
`email_address`	`email`	reťazec
`mobile_phone_number`	`phone_number`	reťazec
`portrait`	`picture`	reťazec; adresa URL údajov obsahujúca podobizeň vo formáte JPEG zakódovanú v base64.

([8]) M. Jones a kol., *‚Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)‘* [Sémantika kľúča dôkazu o vlastníctve pre webové tokeny JSON (JWT)], RFC 7800, apríl 2016.

([9]) M. Jones a kol., *‚JSON Web Signature (JWS)‘* [Webový podpis JSON (JWS)], RFC 7515, máj 2015.

Tabuľka 8

Požiadavky na kódovanie osobných identifikačných údajov vo formáte SD-JWT VC s použitím súkromných názvov

Identifikátor údajov	Identifikátor atribútu	Formát kódovania
`expiry_date`	`date_of_expiry`	reťazec, ISO 8601-1, formát RRRR-MM-DD
`issuance_date`	`date_of_issuance`	reťazec, ISO 8601-1, formát RRRR-MM-DD
`personal_administrative_number`	`personal_administrative_number`	reťazec
`sex`	`sex`	počet
`issuing_authority`	`issuing_authority`	reťazec
`issuing_country`	`issuing_country`	reťazec
`document_number`	`document_number`	reťazec
`issuing_jurisdiction`	`issuing_jurisdiction`	reťazec

— Základný typ osobných identifikačných údajov je ‚urn:eudi:pid:1', zahrnutý v tvrdení vct. Všetky osobné identifikačné údaje používajú typy v priestore názvov ‚urn:eudi:pid:'.

— Ak osobné identifikačné údaje obsahujú atribúty, ktoré nie sú špecifikované v tejto prílohe, tieto atribúty sa definujú v rámci domáceho typu.

— Ak sa používa domáci typ, jeho schéma vrátane všetkých identifikátorov údajov, ich definícií, prítomnosti a formátov kódovania sa vymedzí v schéme uverejnenej v súlade s článkom 8 vykonávacieho nariadenia (EÚ) 2025/1569.

5. Oddiel 5: Podrobné údaje o dôveryhodnej infraštruktúre

Zoznam poskytovateľov osobných identifikačných údajov sprístupnený Komisiou v súlade s vykonávacím nariadením (EÚ) 2024/2980 umožňuje autentifikáciu osobných identifikačných údajov."

PRÍLOHA II

„*PRÍLOHA Ia*

Kryptografické mechanizmy uvedené v článku 5a

Európska skupina pre certifikáciu kybernetickej bezpečnosti, podskupina pre kryptografiu: ‚*Agreed Cryptographic Mechanisms*' (Dohodnuté kryptografické mechanizmy), uverejnené Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) ([1]).“

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

PRÍLOHA III

„PRÍLOHA Ib

Technické špecifikácie pre osvedčenia jednotky peňaženky uvedené v článku 6 ods. 2a

1. Osvedčenie jednotky peňaženky obsahuje jedno alebo viacero osvedčení inštancie peňaženky a jedno alebo viacero osvedčení kľúča.

2. Osvedčenie inštancie peňaženky a osvedčenia kľúča musia spĺňať tieto požiadavky:

   a) Požiadavky na formát

      — FR-WIA-1: Osvedčenie inštancie peňaženky je webový token JSON Web Token (JWT) podľa normy RFC 7519 ([1]), podpísaný alebo zapečatený poskytovateľom peňaženky pomocou kompaktného základného podpisu JAdES B.

         — FR-WIA-1.1: Osvedčenie inštancie peňaženky je osvedčenie peňaženky podľa dodatku E k OpenID for Verifiable Credential Issuance v1.0 ([2]) (ďalej len ‚OID4VCI') a rozšírené podľa C-WIA-1 a C-WIA-2 ďalej v texte.

      — FR-KA-1: Osvedčenie kľúča je token JWT podľa normy RFC 7519, podpísaný alebo zapečatený poskytovateľom peňaženky pomocou kompaktného základného podpisu JAdES B.

         — FR_KA_1.1: Osvedčenie kľúča je osvedčenie kľúča podľa dodatku D k OID4VCI, rozšírené podľa C_KA-1 a C_KA-2 ďalej v texte.

   b) Požiadavky na prenos

      — TR-WIA-1: Jednotka peňaženky používa osvedčenie inštancie peňaženky pri vydávaní osobných identifikačných údajov, kvalifikovaných alebo nekvalifikovaných elektronických osvedčení atribútov alebo elektronických osvedčení atribútov poskytovaných subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene.

      — TR-WIA-2: Poskytovateľ peňaženky overí integritu inštancie peňaženky a podpíše alebo zapečatí osvedčenie inštancie peňaženky.

         — TR-WIA-2.1: Ak poskytovateľ peňaženky vydá osvedčenie inštancie peňaženky, rozdiel medzi časom, keď poskytovateľ peňaženky overil integritu inštancie peňaženky, a časom, ktorý uvedie v parametri záhlavia ‚exp' vydaného osvedčenia inštancie peňaženky, musí byť kratší ako 24 hodín.

         — TR-WIA-2.2: Poskytovateľ peňaženky zabezpečí, aby jednotka peňaženky obsahovala osvedčenia inštancie peňaženky potrebné na vydanie osobných identifikačných údajov a elektronických osvedčení atribútov.

      — TR-WIA-3: Počas vydávania jednotka peňaženky zašle autorizačnému serveru v odoslanej žiadosti o autorizáciu a v žiadosti o token osvedčenie inštancie peňaženky podľa OID4VCI.

         — TR-WIA-3.1: Jednotka peňaženky zašle osvedčenie inštancie peňaženky spolu s dôkazom o vlastníctve (ďalej len ‚PoP') podľa dodatku E k OID4VCI.

         — TR-WIA-3.2: Jednotka peňaženky zašle to isté osvedčenie inštancie peňaženky iba jednému autorizačnému serveru.

([1]) RFC 7519: *JSON Web Token (JWT)* [Webový token JSON (JWT)], máj 2015.
([2]) *OpenID for Verifiable Credential Issuance v1.0* (OpenID pre vydávanie overiteľných poverení 1.0), https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: Ak poskytovateľ peňaženky používa možnosť ‚per-issuer reuse' podľa R_WIA_1, jednotka peňaženky môže poslať osvedčenie inštancie peňaženky tomu istému autorizačnému serveru viackrát.

— TR-WIA-3.2.2: Ak poskytovateľ peňaženky nepoužíva možnosť ‚per-issuer reuse', jednotka peňaženky použije osvedčenie inštancie peňaženky najviac v jednom procese vydávania.

— TR-WIA-4: Keď autorizačný server dostane osvedčenie inštancie peňaženky, overí podpis osvedčenia inštancie peňaženky s použitím verejného kľúča v podpisovom certifikáte uvedenom v parametri ‚x5c' v záhlaví JOSE osvedčenia inštancie peňaženky.

— TR-WIA-4.1: Autorizačný server takisto overí, či tento podpisový certifikát možno overiť pomocou dôveryhodného bodu v zozname poskytovateľov peňaženky uvedenom v článku 5 vykonávacieho nariadenia (EÚ) 2024/2980, prípadne pomocou sprostredkovateľských certifikátov zahrnutých v parametri x5c.

— TR-WIA-4.2: Autorizačný server overí, či platnosť osvedčenia inštancie peňaženky neuplynula.

— TR-WIA-4.3: Autorizačný server overí podpis PoP pomocou verejného kľúča uvedeného v tvrdení ‚cnf'.

— TR_KA-1: Jednotka peňaženky používa osvedčenie kľúča pri vydávaní osobných identifikačných údajov a pri vydávaní kvalifikovaných alebo nekvalifikovaných elektronických osvedčení atribútov viazaných na zariadenie alebo elektronických osvedčení atribútov poskytovaných subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene.

— TR_KA-1.1: Jednotka peňaženky nepoužíva osvedčenie kľúča pri vydávaní kvalifikovaných alebo nekvalifikovaných elektronických osvedčení atribútov neviazaných na zariadenie alebo elektronických osvedčení atribútov poskytovaných subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene.

— TR_KA-2: Poskytovateľ peňaženky poskytuje jednotku peňaženky s rôznymi osvedčeniami kľúča pre zariadenie WSCD jednotky peňaženky a pre každé z jej úložísk kľúčov.

— TR_KA-2.1: Poskytovateľ peňaženky podpíše alebo zapečatí osvedčenie kľúča po tom, ako overí, že kľúče, ktoré sú v osvedčení kľúča osvedčené, sú uložené v zariadení WSCD jednotky peňaženky alebo v úložisku kľúčov opísanom v osvedčení kľúča.

— TR_KA-2.2: Osvedčenie kľúča obsahuje aspoň jeden osvedčený verejný kľúč. Počet kľúčov v osvedčení kľúča zaslanom vydavateľovi poverení by nemal prekročiť maximálnu veľkosť dávky určenú týmto vydavateľom poverení v jeho metaúdajoch vydavateľa poverení; pozri ETSI TS 119 472-3 ([3]), parameter ‚credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size'.

— TR_KA-2.3: Poskytovateľ peňaženky zahrnie verejný kľúč (zodpovedajúci súkromnému kľúču uloženému v zariadení WSCD alebo v úložisku kľúčov jednotky peňaženky) najviac do jedného osvedčenia kľúča.

— TR_KA-2.4: Jednotka peňaženky používa osvedčenie kľúča najviac v jednom procese vydávania alebo opakovaného vydávania poverenia.

— TR_KA-2.5: Poskytovateľ peňaženky zabezpečí, aby mala jednotka peňaženky k dispozícii osvedčenia kľúča potrebné na vydávanie osobných identifikačných údajov a elektronických osvedčení atribútov viazaných na zariadenie.

([3]) ETSI, *‚Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles'* [Elektronické podpisy a infraštruktúry (ESI); digitálne podpisy JAdES; časť 3: úrovne a základné profily JAdES], ETSI TS 119 472-3, V1.1.1, marec 2026.

— TR_KA-3: Ak je to počas vydávania potrebné, jednotka peňaženky zahrnie osvedčenie kľúča do poľa ‚proofs' žiadosti o poverenie adresovanej vydavateľovi poverení podľa OID4VCI, a to buď v dôkaze typu ‚jwt', alebo typu ‚attestation'.

— TR_KA_3.1: Ak jednotka peňaženky obsahuje osvedčenie kľúča v prvku ‚jwt', podpíše alebo zapečatí osvedčenie kľúča pomocou súkromného kľúča zodpovedajúceho verejnému kľúču v indexe 0 poľa ‚attested_keys' v rámci objektu ‚key_attestation'.

— TR_KA-4: Ak vydavateľ poverení vydáva poverenia viazané na zariadenie, v parametri ‚proof_types_supported' vo svojich metaúdajoch vydavateľa poverení podľa oddielu 12.2.4 OID4VCI uvedie, že pre osvedčenia kľúča, ktoré zahŕňajú objekt ‚key_attestations_required', podporuje dôkaz typu ‚jwt' aj ‚attestation'.

— TR_KA-4.1: Ak vydavateľ poverení vydáva poverenia, ktoré nie sú viazané na zariadenie, v metaúdajoch vydavateľa poverení vynechá parametre ‚proof_types_supported' a ‚cryptographic_binding_methods_supported'.

— TR_KA-5: Ak vydavateľ poverení dostane osvedčenie kľúča v dôkaze typu ‚jwt' alebo ‚attestation', overí podpis osvedčenia kľúča pomocou verejného kľúča v podpisovom certifikáte, ktorý je súčasťou parametra ‚x5c' v záhlaví JOSE osvedčenia kľúča, a či sa tento podpisový certifikát dá overiť pomocou dôveryhodného bodu v zozname poskytovateľov peňaženky uvedenom v článku 5 vykonávacieho nariadenia (EÚ) 2024/2980, prípadne pomocou sprostredkovateľských poverení zahrnutých v parametri ‚x5c'.

— TR_KA-6: Ak vydavateľ poverení dostane osvedčenie kľúča v dôkaze typu ‚jwt', overí podpis prvku ‚jwt' pod kľúčom v indexe 0 poľa ‚attested_keys' v rámci objektu ‚key_attestation' zahrnutého v prvku ‚jwt'.

— TR_KA-6.1: Vydavateľ poverení overí, či pole ‚nonce' prvku ‚jwt' obsahuje platný parameter c_nonce z jeho koncového bodu nonce_endpoint podľa OID4VCI.

— TR_KA-7: Ak vydavateľ poverení dostane osvedčenie kľúča v dôkaze typu ‚attestation', overí, či objekt ‚key_attestation' obsahuje platný parameter c_nonce z jeho koncového bodu nonce_endpoint.

— TR_KA-8: Poskytovateľ osobných identifikačných údajov zabezpečí, aby osobné identifikačné údaje boli viazané na verejný kľúč, ktorý pochádza z osvedčenia kľúča s uvedením zariadenia WSCD.

c) Požiadavky na obsah

— C_WIA-1: Osvedčenie inštancie peňaženky obsahuje tieto údaje:

— tvrdenie ‚wallet_name' podľa dodatku E k OID4VCI, pričom jeho hodnotou je identifikátor riešenia peňaženky, ktoré možno nájsť v zozname poskytovateľov peňaženky uvedenom v článku 5 vykonávacieho nariadenia (EÚ) 2024/2980,

— tvrdenie ([4]) ‚wallet_version', ktorým je reťazec, ktorého hodnotou je verzia riešenia peňaženky,

— tvrdenie ‚wallet_solution_certification_information', ktorým je objekt JSON obsahujúci informácie o orgáne posudzovania zhody, ktorý certifikoval riešenie peňaženky, prípadne číslo certifikácie a ďalšie relevantné podrobnosti týkajúce sa certifikácie,

([4]) Toto tvrdenie je vymedzené v tomto vykonávacom nariadení Komisie, keďže nie je súčasťou špecifikácie OID4VCI.

— tvrdenie ‚client_status‘, ktoré obsahuje dve podpolia:

— ‚status‘: odkaz na zoznam stavov, ako je špecifikovaný v dodatku E k OID4VCI, ktorý predstavuje stav zrušenia inštancie peňaženky. Podrobnosti sú uvedené v písmene e),

— ‚exp‘: NumericDate podľa normy RFC 7519 určujúci čas, do ktorého bude poskytovateľ peňaženky zachovávať stav zrušenia v indexe zoznamu stavov, na ktorý sa odkazuje v tvrdení ‚status‘,

— tvrdenie ‚exp‘ uvedené v dodatku E k OID4VCI.

— *POZNÁMKA*: Tvrdenie ‚client_status.status‘ v osvedčení inštancie peňaženky predstavuje stav zrušenia inštancie peňaženky, nie stav zrušenia samotného osvedčenia. Ako sa opisuje v R_WIA-1, poskytovateľ peňaženky sa môže rozhodnúť, že každé osvedčenie inštancie peňaženky bude smerovať na konkrétny autorizačný server na základe toho, že všetky osvedčenia odoslané na tento server obsahujú v položke ‚client_status.status‘ rovnakú hodnotu indexu.

— *POZNÁMKA*: Hodnotu ‚idx‘ v tvrdení ‚status‘ možno použiť ako (párový) jedinečný identifikátor inštancie peňaženky a jednotky peňaženky.

— C_WIA-2: Osvedčenie inštancie peňaženky by malo obsahovať aj tvrdenie ‚wallet_link‘ podľa dodatku E k OID4VCI a hodnotou tohto tvrdenia musí byť adresa URI, kde možno získať ďalšie informácie o riešení peňaženky.

— C_WIA-3: Autorizačný server nesmie vykladať parameter ‚exp‘ na najvyššej úrovni osvedčenia inštancie peňaženky ako koniec obdobia zachovávania stavu zrušenia inštancie peňaženky.

— *POZNÁMKA*: Parameter ‚exp‘ na najvyššej úrovni osvedčenia inštancie peňaženky označuje, kedy uplynie platnosť samotného osvedčenia.

— C_KA-1: Osvedčenie kľúča obsahuje:

— tvrdenia ‚key_storage‘ a ‚user_authentication‘ podľa dodatku D k OID4VCI,

— atribúty ‚key_storage‘ a ‚user_authentication‘ majú hodnotu ‚iso_18045_high‘, ak sa v osvedčení kľúča uvádza zariadenie WSCD,

— tvrdenie ‚certification‘ podľa dodatku D k OID4VCI, obsahujúce adresu URL, kde možno získať informácie o certifikácii, ktorú získalo zariadenie WSCD alebo úložisko kľúčov, prípadne schéma, ako napr. Common Criteria alebo GlobalPlatform, hodnotené požiadavky, ako napr. príslušný profil ochrany, a úroveň hodnotenia,

— na základe týchto informácií je možné určiť, či je úložisko kľúčov zariadením WSCD,

— tvrdenie ‚key_storage_status‘, ktoré obsahuje dve podpolia:

— ‚status‘: odkaz na zoznam stavov podľa dodatku D.1 k OID4VCI. Táto hodnota predstavuje buď stav zrušenia zariadenia WSCD, alebo typu úložiska kľúčov použitého na uloženie osvedčených kľúčov, alebo – v rámci možnosti indexu per-key-attestation – stav zrušenia zariadenia WSCD alebo úložiska kľúčov konkrétnej jednotky peňaženky. Pozri R_KA_1 ďalej v texte, kde sú uvedené dostupné možnosti priradenia indexov,

— ‚exp‘: NumericDate podľa normy RFC 7519 určujúci čas, do ktorého bude poskytovateľ peňaženky zachovávať stav zrušenia v indexe zoznamu stavov, na ktorý sa odkazuje v tvrdení ‚status‘,

— tvrdenie ‚exp‘ uvedené v dodatku D k OID4VCI.

— *POZNÁMKA* k hodnote ‚idx' v tvrdení ‚key_storage_status.status' v osvedčení kľúča: Ak poskytovateľ peňaženky používa možnosť ‚type-shared index' (pozri R_KA_1 ďalej v texte), všetky osvedčenia kľúča pre rovnaký typ zariadenia WSCD alebo úložiska kľúčov majú rovnaký index zoznamu stavov. Hodnota ‚idx' teda nie je pre každú jednotku peňaženky jedinečná. Naopak, ak poskytovateľ peňaženky používa možnosť ‚per-key-attestation index', hodnota ‚idx' je jedinečná pre jednotku peňaženky (alebo párovo jedinečná pre vydavateľa poverení). Vo všetkých prípadoch však platí, že vydavateľ poverení nepoužije hodnotu ‚idx' v osvedčení kľúča ako identifikátor jednotky peňaženky, ale túto hodnotu použije v osvedčení inštancie peňaženky.

— C_KA-2: Ak sa osvedčenie kľúča posiela v dôkaze typu ‚attestation', musí obsahovať aj platný parameter ‚c_nonce' podľa dodatku F.3 k OID4VCI.

— C_KA-3: Vydavateľ poverení nesmie vykladať parameter ‚exp' na najvyššej úrovni osvedčenia kľúča ako koniec obdobia zachovávania stavu zrušenia v zariadení WSCD alebo úložisku kľúčov.

— *POZNÁMKA*: Parameter ‚exp' na najvyššej úrovni osvedčenia kľúča označuje, kedy uplynie platnosť samotného osvedčenia kľúča.

d) Požiadavky na životný cyklus

— V tejto prílohe sa špecifikujú tieto parametre metaúdajov vydavateľa poverení:

  — ‚preferred_client_status_period': OPTIONAL. Celé číslo vyjadrujúce preferované zostávajúce obdobie zachovávania stavu osvedčenia inštancie peňaženky, ktoré má byť predložené jednotkou peňaženky počas vydávania, v sekundách. Zostávajúce obdobie zachovávania stavu je definované ako hodnota ‚client_status.exp' v osvedčení mínus čas prijatia osvedčenia.

  — ‚preferred_key_storage_status_period': OPTIONAL. Celé číslo vyjadrujúce preferované zostávajúce obdobie zachovávania stavu osvedčenia kľúča, ktoré má byť predložené jednotkou peňaženky počas vydávania, v sekundách. Zostávajúce obdobie zachovávania stavu je definované ako hodnota ‚key_storage_status.exp' v osvedčení mínus čas prijatia osvedčenia.

— LC_WIA-1: Autorizačný server môže oznámiť svoje preferencie pre zostávajúce obdobie zachovávania stavu v osvedčeniach inštancie peňaženky zahrnutím parametra metaúdajov ‚preferred_client_status_period' do svojho koncového bodu metaúdajov vydavateľa poverení podľa oddielu 12.2.2 OID4VCI.

  — LC_WIA-1.1: Toto pole sa umiestni na najvyššiu úroveň metaúdajov vydavateľa poverení.

— LC_WIA_2: Autorizačný server nesmie vykladať parameter ‚exp' na najvyššej úrovni osvedčenia inštancie peňaženky ako koniec obdobia zachovávania stavu zrušenia inštancie peňaženky.

— LC_WIA_3: Ak poskytovateľ peňaženky podpíše alebo zapečatí osvedčenie inštancie peňaženky, zachováva stav zrušenia príslušnej inštancie peňaženky, kým neuplynie platnosť parametra ‚wallet_instance_status.exp' uvedeného v danom osvedčení inštancie peňaženky.

— LC_KA-1: Ak je potrebné osvedčenie kľúča, vydavateľ poverení môže oznámiť svoje preferencie pre zostávajúce obdobie zachovávania stavu v osvedčeniach kľúča zahrnutím parametra metaúdajov ‚preferred_key_storage_status_period' uvedeného v predchádzajúcom texte do svojho koncového bodu metaúdajov vydavateľa poverení podľa oddielu 12.2.2 OID4VCI.

  — LC_KA-1.1: Toto pole sa umiestni do objektu ‚key_attestations_required' podľa oddielu 12.2.4 OID4VCI.

— LC_KA-2: Poskytovateľ peňaženky si zvolí obdobie technickej platnosti osvedčení kľúčov, ktoré vydáva.

— LC_KA-3: Ak poskytovateľ peňaženky podpíše alebo zapečatí osvedčenie o kľúči, zachováva stav zrušenia príslušného zariadenia WSCD alebo úložiska kľúčov, kým neuplynie platnosť parametra ‚key_storage_status.exp' uvedeného v danom osvedčení kľúča.

— LC_GEN-1: Poskytovateľ peňaženky zabezpečí, aby jednotka peňaženky mohla vždy predložiť osvedčenia jednotky peňaženky a osvedčenia kľúča, ktorých parametre ‚client_status.exp' a ‚key_storage_-status.exp' (v uvedenom poradí) sú v čase predloženia autorizačnému serveru alebo vydavateľovi poverení najmenej 31 dní v budúcnosti.

— *POZNÁMKA*: Tým sa zaručuje, aby sa poskytovatelia osobných identifikačných údajov mohli spoľahnúť na reťazenie zrušení bez toho, aby boli nútení vydávať krátkodobé osobné identifikačné údaje.

— LC_GEN-2: Poskytovateľ peňaženky zabezpečí, aby jednotka peňaženky počas vydávania získala metaúdaje vydavateľa poverení.

  — LC_GEN_2.1: Ak je v týchto metaúdajoch zahrnuté pole ‚preferred_key_storage_status_period', jednotka peňaženky zašle osvedčenie kľúča s hodnotou (‚key_storage_status.exp' – aktuálny čas) – ‚preferred_key_storage_status_period', ktorá je čo najmenšia, ale nie záporná. Ak jednotka peňaženky nemá k dispozícii žiadne takéto osvedčenie kľúča, získa od poskytovateľa peňaženky nové osvedčenie kľúča, v prípade ktorého platí, že parameter ‚key_storage_status.exp' – aktuálny čas ≥ ‚preferred_key_storage_status_period'.

  — LC_GEN_2.2: Ak je v týchto metaúdajoch zahrnuté pole ‚preferred_client_status_period', jednotka peňaženky zašle osvedčenie inštancie peňaženky s hodnotou (‚client_status.exp' – aktuálny čas) – ‚preferred_client_status_period', ktorá je čo najmenšia, ale nie záporná. Ak jednotka peňaženky nemá k dispozícii žiadne takéto osvedčenie inštancie peňaženky, požiada poskytovateľa peňaženky o nové osvedčenie inštancie peňaženky, v prípade ktorého platí, že parameter ‚client_status.exp' – aktuálny čas ≥ ‚preferred_client_status_period'.

— LC_GEN-3: Obdobie technickej platnosti osobných identifikačných údajov sa končí pred uplynutím platnosti parametra ‚client_status.exp' osvedčenia inštancie peňaženky aj parametra ‚key_storage_-status.exp' osvedčenia kľúča zaslaného poskytovateľovi osobných identifikačných údajov v procese vydávania.

— LC_GEN-4: Poskytovateľ osobných identifikačných údajov, ktorých technická platnosť je dlhšia ako 24 hodín, kontroluje počas obdobia technickej platnosti osobných identifikačných údajov aspoň raz za 24 hodín stav zrušenia osvedčenia inštancie peňaženky aj osvedčenia kľúča prijatého počas vydávania. Ak je niektorý z nich zrušený, poskytovateľ zruší osobné identifikačné údaje.

e) Požiadavky na zrušenie

— R_GEN-1: Poskytovateľ peňaženky používa ako mechanizmus zrušenia osvedčení kľúča aj osvedčení inštancie peňaženky podľa dodatku D a E k OID4VCI zoznamy stavov tokenov (podľa zoznamu IETF Token Status List).

— *POZNÁMKA*: Na zlepšenie škálovateľnosti svojich zoznamov stavov môže poskytovateľ peňaženky použiť tieto optimalizácie:

  — rozdelenie zoznamu stavov na viacero častí, ak má poskytovateľ peňaženky veľký počet používateľov a vydaných osvedčení. Na výber je množstvo stratégií delenia na časti, napríklad na základe pevnej veľkosti alebo podľa časového obdobia. O stratégii delenia na časti rozhoduje poskytovateľ peňaženky. Zohľadniť možno okrem iného veľkosť zoznamu stavov na stiahnutie a súkromie používateľa,

  — vedenie viacerých zoznamov stavov,

  — komprimovanie zoznamu stavov na účely zmenšenia jeho veľkosti.

— R_WIA-1: Poskytovateľ peňaženky môže vo všetkých osvedčeniach inštancie peňaženky, ktoré daná jednotka peňaženky predkladá tomu istému autorizačnému serveru, priradiť rovnakú hodnotu tvrdeniu ‚idx' v parametri ‚client_status.status'. Táto možnosť sa nazýva možnosť ‚per-issuer reuse'. Ak sa použije táto možnosť:

  — R_WIA-1.1: Jednotka peňaženky uchováva informáciu o tom, akú hodnotu indexu použila pre každý autorizačný server, s ktorým už v minulosti komunikovala, a pri opätovnej komunikácii s tým istým autorizačným serverom požiada o osvedčenie inštancie peňaženky obsahujúce rovnakú hodnotu indexu.

  — R_WIA-1.2: Ak poskytovateľ peňaženky dostane žiadosť o osvedčenie inštancie peňaženky obsahujúce konkrétnu hodnotu indexu, pred vydaním nového osvedčenia inštancie peňaženky s touto hodnotou indexu overí, či žiadajúca jednotka peňaženky už uvedenú hodnotu indexu dostala.

  — R_WIA-1.3: Jednotka peňaženky nesmie opätovne použiť rovnakú hodnotu indexu na interakcie s rôznymi autorizačnými servermi.

— *POZNÁMKA*: Ak sa používa možnosť ‚per-issuer reuse', poskytovateľ peňaženky bude môcť určiť, s koľkými autorizačnými servermi jednotka peňaženky komunikovala a ako často komunikovala s každým z nich.

— R_WIA-2: Poskytovateľ peňaženky vo svojich zásadách ochrany osobných údajov uvedie, či na zrušenie inštancie peňaženky používa možnosť ‚per-issuer reuse'.

— R_WIA-3: Ak poskytovateľ peňaženky nepoužíva možnosť ‚per-issuer reuse', každému osvedčeniu inštancie peňaženky, ktoré vydáva, priradí novú, neprepojiteľnú hodnotu indexu.

— R_WIA-4: Ak sa jednotka peňaženky musí zrušiť, poskytovateľ peňaženky zruší hodnoty indexu v tvrdení ‚client_status.status' vo všetkých osvedčeniach inštancie peňaženky spojených s danou jednotkou peňaženky.

— R_WIA-5: Poskytovateľ peňaženky pri určovaní veľkosti zoznamov stavov osvedčení inštancií peňaženky zohľadní rozsah jeho nasadenia a použitú architektúru, pričom musí zabezpečiť, aby boli tieto zoznamy dostatočne veľké na zabránenie korelácii a na ochranu súkromia používateľov. Ak je to možné, zoznam stavov sa musí vzťahovať minimálne na 10 000 osvedčení.

— R_KA_1: Poskytovateľ peňaženky si v osvedčení kľúča vyberie jednu z týchto možností priradenia indexu pre tvrdenie ‚key_storage_status.status':

  — možnosť 1, t. j. ‚type-shared index', pri ktorej všetky osvedčenia kľúča osvedčujúce kľúče uložené v rovnakom type zariadenia WSCD alebo úložiska kľúčov obsahujú v tvrdení ‚key_storage_status.status' rovnakú hodnotu indexu,

  — možnosť 2, t. j. ‚per-key-attestion index', pri ktorej osvedčenie kľúča osvedčujúce kľúče uložené v jednotlivom zariadení WSCD alebo úložisku kľúčov obsahuje v tvrdení ‚key_storage_status.status' (párovú) jedinečnú hodnotu indexu.

— *POZNÁMKA*: Ak poskytovateľ peňaženky používa možnosť 1, jediná akcia zrušenia zruší platnosť všetkých osvedčení kľúča dotknutého typu vo všetkých jednotkách peňaženky. Okrem toho, keďže všetky osvedčenia kľúča pre rovnaký typ zariadenia WSCD alebo úložiska kľúčov majú rovnaký index zoznamu stavov, počet položiek v zozname stavov osvedčení kľúča odráža počet typov zariadení WSCD alebo úložísk kľúčov podporovaných poskytovateľom peňaženky, a nie počet nasadených jednotiek peňaženky. Aspekty ochrany súkromia, ktorými sa odôvodňuje minimálna veľkosť zoznamu stavov pre zoznamy stavov inštancie peňaženky, sa preto neuplatňujú na zoznamy stavov osvedčenia kľúča podľa možnosti 1 za predpokladu, že existuje dostatočný počet jednotiek peňaženky, ktoré používajú rovnaký typ zariadenia WSCD alebo úložiska kľúčov.

— *POZNÁMKA*: Ak poskytovateľ peňaženky používa možnosť 2, každý index predstavuje stav zrušenia konkrétneho zariadenia WSCD alebo úložiska kľúčov, ktoré sú v uvedenom osvedčení kľúča osvedčené.

— *POZNÁMKA*: Ak poskytovateľ peňaženky používa možnosť 2, na žiadosť používateľa možno konkrétne zariadenie WSCD alebo úložisko kľúčov takisto zrušiť.

— R_KA-2: Ak poskytovateľ peňaženky používa možnosť 2, voliteľne môže používať možnosť ‚per-issuer reuse' opísanú v R_WIA-1. Ak poskytovateľ peňaženky používa túto možnosť, požiadavky R_WIA-1 - R_WIA-3 sa uplatňujú *mutatis mutandis*.

— R_KA-3: Ak poskytovateľ peňaženky používa možnosť 2, pri určovaní veľkosti zoznamov stavov osvedčení kľúča zohľadní rozsah jeho nasadenia a použitú architektúru, pričom musí zabezpečiť, aby boli tieto zoznamy dostatočne veľké na zabránenie korelácii a na ochranu súkromia používateľov. Ak je to možné, zoznam stavov sa musí vzťahovať minimálne na 10 000 osvedčení kľúča.

— R_KA-4: Ak poskytovateľ peňaženky používa možnosť 1 (rovnaká hodnota indexu pre daný typ), zruší záznam ‚key_storage_status.status' iba v prípade, že typ zariadenia WSCD alebo úložiska kľúčov vykazuje zraniteľnosť v oblasti bezpečnosti.

f) Požiadavky na podpisové algoritmy

— SA-1: Na podpisovanie osvedčení inštancie peňaženky, osvedčení kľúča, súvisiacich dôkazov o vlastníctve a zoznamov stavov tokenov sa používa jeden z týchto algoritmov:

— ES256 (ECDSA) s SHA-256 a P-256),

— ES384 (ECDSA s SHA-384 a P-384),

— ES512 (ECDSA s SHA-512 a P-521).

— SA-2: Poskytovateľ peňaženky si vyberie, ktorý z algoritmov uvedených v SA-1 použije.

— SA-3: Autorizačný server alebo vydavateľ poverení (podľa OID4VCI) musí podporovať všetky algoritmy uvedené v SA-1."

PRÍLOHA IV

„PRÍLOHA II

Zoznam noriem uvedených v článku 8

Uplatňujú sa technické špecifikácie uvedené v bodoch 2 až 6 ETSI TS 119 472-1 V1.2.1 (2026-02). Vykladajú sa s týmito úpravami:

1. 2.1. Normative references (Normatívne odkazy)

— [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' [Elektronické podpisy a infraštruktúry (ESI); profily certifikátov; časť 1: prehľad a spoločné štruktúry údajov],

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): ‚Electronic Signatures and Trust Infrastructures; Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers' [Elektronické podpisy a infraštruktúry dôvery (ESI); profily certifikátov; časť 6: požiadavky na profil certifikátu pre poskytovateľov PID, peňaženky, EAA, QEAA a PSBEAA],

— [25] IETF Token Status List (TSL), draft-ietf-oauth-status-list-20: ‚Token status list' (Zoznam stavov tokenov), 20. apríla 2026.

2. 4.2.11.1. General requirements (Všeobecné požiadavky)

— EAA-4.2.11.1-06: Ak sa prvok stavu používa v prípade osobných identifikačných údajov, kvalifikovaných elektronických osvedčení atribútov alebo elektronických osvedčení atribútov poskytovaných subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene, uvádza sa v ňom len to, či bolo osvedčenie zrušené alebo nie, a nepodporujú sa ním žiadne iné hodnoty stavu, ako je pozastavenie.

— EAA-4.2.11.1-06.1: Ak je osvedčenie zrušené, je zrušené natrvalo.

3. 4.2.13. EAA short-lived

— EAA-4.2.13-03: Ak sa vydávajú krátkodobé elektronické osvedčenia atribútov s platnosťou 24 hodín alebo kratšou, zrušenie sa nevyžaduje.

4. 4.6.3. Požiadavky na elektronické osvedčenia atribútov (EAA) EÚ vydané subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene (PuB-EAA)

— PuB-EAA-4.6.2-03: neplatné.

— Pub-EAA-4.6.2-04: neplatné.

— PuB-EAA-4.6.3-03: Digitálny podpis PuB-EAA by mal obsahovať kvalifikovaný certifikát podporujúci digitálny podpis PuB-EAA.

— PuB-EAA-4.6.3-04: Kvalifikovaný certifikát podporujúci digitálny podpis PuB-EAA musí spĺňať požiadavky bodu 8 normy ETSI TS 119 412-6 v1.1.1 a musí obsahovať QcType qcStatement, ako je vymedzený v norme ETSI EN 319 412-5 v2.5.1, s hodnotou id-etsi-qct-eidaspsbeaa vymedzenou takto:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } – certifikát uvedený v článku 45f ods. 1 písm. b) podporujúci kvalifikovaný elektronický podpis alebo kvalifikovanú elektronickú pečať subjektu verejného sektora uvedeného v článku 3 bode 46 nariadenia (EÚ) č. 910/2014.

5. 5.2.10.1. General requirements (Všeobecné požiadavky)

— EAA-5.2.10.1-04: neplatné.

— EAA-5.2.10.1-05: neplatné.

— EAA-5.2.10.1-06: Člen stavu môže obsahovať člen status_list, ako sa uvádza v bode 6.2 IETF draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: neplatné.

— EAA-5.2.10.1-08: neplatné.

— EAA-5.2.10.1-09: neplatné.

— EAA-5.2.10.1-10: neplatné.

— EAA-5.2.10.1-11: neplatné.

— EAA-5.2.10.1-12: neplatné.

6. 6.2.10.1. General requirements (Všeobecné požiadavky)

— EAA-6.2.10.1-01: Ak elektronické osvedčenie atribútov v súlade s formátom ISO/IEC mdoc používa mechanizmus zoznamu stavov osvedčení podľa požiadavky EAA-6.2.10.1-02.2 alebo mechanizmus zoznamu zrušení osvedčení podľa požiadavky EAA-6.2.10.1-02.3, jeho objekt mobilnej bezpečnosti (mobile security object – ďalej len ‚MSO') obsahuje štruktúru stavu podľa požiadavky EAA-6.2.10.1-17, ktorá obsahuje informácie o zrušení objektu MSO.

— EAA-6.2.10.1-01.1: Pri zavádzaní mechanizmu zoznamu identifikátorov musí prvok stav obsahovať prvok identifier_list podľa požiadavky EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: Pri zavádzaní mechanizmu zoznamu stavov musí prvok stav obsahovať prvok status_list podľa požiadavky EAA-6.2.10.1-13.

— *POZNÁMKA*:

  — Štruktúra stavu obsahuje odkaz na zoznam zrušení objektov MSO.

  — Zoznam zrušení objektov MSO je štruktúrou typu COSE_Sign1, ktorá označuje, či konkrétny objekt MSO je alebo nie je zrušený.

  — Štruktúra stavu obsahuje všetky informácie potrebné na to, aby strana spoliehajúca sa na peňaženku mohla určiť, či je zoznam zrušení objektov MSO autentický.

— EAA-6.2.10.1-02: Poskytovateľ osobných identifikačných údajov, poskytovateľ kvalifikovaných elektronických osvedčení atribútov alebo poskytovateľ elektronických osvedčení atribútov poskytovaných subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene použije na zrušenie osobných identifikačných údajov, kvalifikovaných elektronických osvedčení atribútov alebo elektronických osvedčení atribútov poskytnutých subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene jednu z týchto metód:

— EAA-6.2.10.1-02.1: Ak vydávajú krátkodobé elektronické osvedčenia atribútov s obdobím platnosti rovným 24 hodinám alebo kratším, zrušenie sa nevyžaduje.

— EAA-6.2.10.1-02.2: Na zakódovanie informácií o zrušení vo forme zoznamu stavov sa používa mechanizmus zoznamu stavov osvedčení.

— EAA-6.2.10.1-02.2.1: Mechanizmus zoznamu stavov zrušuje objekt MSO na základe toho, či je bit na pozícii definovanej vydavateľom v objekte MSO v zozname stavov nastavený na hodnotu true.

— EAA-6.2.10.1-02.2.2: Mechanizmus zoznamu stavov je špecifikovaný v špecifikácii zoznamu stavov tokenov (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: Na zakódovanie informácií o zrušení vo forme zoznamu identifikátorov sa používa mechanizmus zoznamu zrušení osvedčení.

— EAA-6.2.10.1-02.3.1: mechanizmus zoznamu identifikátorov zrušuje objekt MSO na základe toho, či sa identifikátor definovaný vydavateľom v objekte MSO nachádza v zozname identifikátorov.

— EAA-6.2.10.1-02.3.2: V požiadavkách EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 a EAA-6.2.10.1-11 sa špecifikuje mechanizmus zoznamu identifikátorov na základe požiadaviek špecifikácie zoznamu stavov tokenov vrátane spoločných prvkov medzi mechanizmom zoznamu stavov a mechanizmom zoznamu identifikátorov.

— EAA-6.2.10.1-03: Ak sa prvok stavu používa v prípade osobných identifikačných údajov, kvalifikovaných elektronických osvedčení atribútov alebo elektronických osvedčení atribútov poskytovaných subjektom verejného sektora zodpovedným za autentický zdroj alebo v jeho mene, používa sa výlučne stav ‚zrušené'.

— EAA-6.2.10.1-03.1: Pre zoznam stavov to znamená, že sa používajú len hodnoty ‚valid' a ‚invalid' podľa špecifikácie zoznamu stavov tokenov.

— EAA-6.2.10.1-03.2: V zozname identifikátorov sa uvádzajú len zrušené objekty MSO, a nie objekty MSO, ktoré sú dočasne pozastavené.

— EAA-6.2.10.1-04: Ak je objekt MSO zrušený, zruší sa natrvalo.

— EAA-6.2.10.1-05: Overenie zoznamu zrušení objektov MSO je pre stranu spoliehajúcu sa na peňaženku nepovinné, pričom v prípade potreby musí overenie spĺňať požiadavky na overenie uvedené v špecifikácii zoznamu stavov tokenov a špecifikácii štruktúry stavov uvedených v požiadavke EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: Ak strana spoliehajúca sa na peňaženku potrebuje byť schopná overiť stav zrušenia osobných identifikačných údajov alebo elektronických osvedčení atribútov, musí podporovať mechanizmus zoznamu stavov osvedčení aj mechanizmus zoznamu zrušení osvedčení stanovený v požiadavke EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: Zoznamy identifier_list a status_list v objekte MSO môžu obsahovať prvok certifikátu.

— EAA-6.2.10.1-06.1: Ak je prvok certifikátu prítomný, obsahuje certifikát s verejným kľúčom, ktorým bol podpísaný alebo zapečatený certifikát najvyššej úrovne v prvku x5chain v štruktúre zoznamu zrušení objektov MSO.

— EAA-6.2.10.1-06.1.1: Inštancia strany spoliehajúcej sa na peňaženku použije tento certifikát ako dôveryhodný bod na overenie prvku x5chain v štruktúre zoznamu zrušení objektov MSO.

— EAA-6.2.10.1-06.2: Ak prvok certifikátu nie je prítomný, certifikát najvyššej úrovne v prvku x5chain v štruktúre zoznamu zrušení objektov MSO musí byť podpísaný alebo zapečatený certifikátom použitým na podpísanie certifikátu v prvku x5chain v objekte MSO.

— EAA-6.2.10.1-06.2.1: Inštancia strany spoliehajúcej sa na peňaženku použije tento certifikát ako dôveryhodný bod na overenie prvku x5chain v štruktúre zoznamu zrušení objektov MSO.

— EAA-6.2.10.1-07: Zoznam zrušení objektov MSO sa zavedie v súlade so špecifikáciou zoznamu stavov tokenov ako token zoznamu stavov vo formáte CWT.

— EAA-6.2.10.1-08: Pre zoznam zrušení objektov MSO pre mechanizmus zoznamu identifikátorov a mechanizmus zoznamu stavov platia tieto požiadavky:

  — tvrdenie exp musí byť prítomné,

  — tvrdenie ttl môže byť prítomné,

  — tvrdenie aggregation_uri v tvrdení IdentifierList alebo StatusList môže byť prítomné a poskytovateľ osobných identifikačných údajov, poskytovateľ kvalifikovaných elektronických osvedčení atribútov alebo poskytovateľ elektronických osvedčení atribútov poskytovaných subjektom verejného sektora

zodpovedným za autentický zdroj alebo v jeho mene môže použiť tvrdenie aggregation_uri na vyjadrenie podpory mechanizmu agregácie podľa špecifikácie zoznamu stavov tokenov,

— formát CWT musí byť objektom typu COSE_Sign1, ktorý na výpočet podpisu používa jeden z týchto podpisových algoritmov:

a) ‚ES256‘ (ECDSA s krivkou NIST P-256 a SHA-256);

b) ‚ES384‘ (ECDSA s krivkou NIST P-384 a SHA-384);

c) ‚ES512‘ (ECDSA s krivkou NIST P-521 a SHA-512);

d) ‚ESB256‘ (ECDSA s krivkou brainpoolP256r1 a SHA-256);

e) ‚ESB384‘ (ECDSA s krivkou brainpoolP384r1 a SHA-384);

f) ‚ESB512‘ (ECDSA s krivkou brainpoolP512r1 a SHA-512);

— formát CWT obsahuje prvok x5chain v chránenom záhlaví, ktoré obsahuje certifikát alebo reťazec certifikátov na overenie podpisu zoznamu zrušení objektov MSO,

— rozšírené používanie kľúča objektového identifikátora (ďalej len ‚OID‘) uvedené v špecifikácii zoznamu stavov tokenov sa môže použiť pre zoznam stavov a podpisový certifikát zoznamu identifikátorov a inštancie peňaženky spoliehajúcej sa strany môžu podporovať rozšírené používanie kľúča identifikátorov objektu uvedené v špecifikácii zoznamu stavov tokenov a pre objektový identifikátor. Pri použití tohto rozšíreného používania kľúča OID uvedeného v špecifikácii zoznamu stavov tokenov poskytovateľ kvalifikovaných elektronických osvedčení atribútov alebo poskytovateľ elektronických osvedčení atribútov poskytovaných subjektom verejného sektora alebo v jeho mene nesmie označiť pole rozšíreného používania kľúča ako kritické.

— EAA-6.2.10.1-09: Na rozdiel od požiadaviek špecifikácie zoznamu stavov tokenov platia pre mechanizmus zoznamu identifikátorov tieto požiadavky:

— hodnota tvrdenia type je ‚application/identifierlist+cwt‘,

— tvrdenie StatusList sa nesmie vyskytovať v súbore tvrdení CWT,

— štruktúra IdentifierList definovaná v požiadavke EAA-6.2.10.1-11 musí byť prítomná ako tvrdenie v súbore tvrdení CWT s použitím kľúča 65530.

— EAA-6.2.10.1-10: Štruktúra IdentifierList je štruktúrou CBOR s touto definíciou 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: Ak je identifikátor prítomný v tvrdení IdentifierList, objekt MSO, ktorý obsahuje identifikátor v prvku stavu, sa zruší.

— EAA-6.2.10.1-10.2: Tvrdenie Aggregation_uri je špecifikované v oddiele 9.2 špecifikácie zoznamu stavov tokenov.

— EAA-6.2.10.1-10.3: Typ obsahu zoznamu identifikátorov musí byť ‚application/identifierlist+cwt' stanovený v požiadavkách uvedených v oddiele 8.2 špecifikácie zoznamu stavov tokenov.

— EAA-6.2.10.1-11: Na prvok identifier_list v objekte MSO sa vzťahujú tieto požiadavky (pozri požiadavku EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: Prvok identifier_list je štruktúrou CBOR s touto definíciou CDDL:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: S cieľom zabrániť korelácii medzi predloženiami prostredníctvom identifikátora musí byť identifikátor pre každý objekt MSO jedinečný.

— EAA-6.2.10.1-12: Na zoznam stavov sa vzťahujú tieto požiadavky:

  — EAA-6.2.10.1-12.1: Prvok bits v štruktúre StatusList sa nastaví na 1.

— EAA-6.2.10.1-13: Na prvok status_list v objekte MSO sa vzťahujú tieto požiadavky (pozri požiadavku EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: Prvok status_list sa riadi požiadavkami na štruktúru StatusListInfo podľa špecifikácie zoznamu stavov tokenov a pridáva sa nepovinný prvok certifikátu podľa požiadavky EAA-6.2.10.1-06.

  — EAA-6.2.10.1-13.2: S cieľom zabrániť korelácii medzi predloženiami prostredníctvom indexu stavu musí byť kombinácia indexu stavu a adresy URI pre každý objekt MSO jedinečná.

— EAA-6.2.10.1-14: Poskytovateľ peňaženky používa na zrušenie osvedčenia inštancie peňaženky (WIA) a zrušenie osvedčenia kľúča (KA) druhú (EAA-6.2.10.1-02.2) alebo tretiu (EAA-6.2.10.1-02.3) z metód špecifikovaných v požiadavke EAA-6.2.10.1-02.

— EAA-6.2.10.1-15: Poskytovateľ peňaženky zavedie do svojho riešenia peňaženky mechanizmy na zrušenie osvedčenia uvedené v požiadavke EAA-6.2.10.1-02.

— EAA-6.2.10.1-16: Poskytovateľ osobných identifikačných údajov a poskytovateľ elektronických osvedčení atribútov podporujú pri overovaní stavu zrušenia osvedčenia inštancie peňaženky (WIA) a osvedčenia kľúča (KA) mechanizmus zoznamu stavov osvedčenia, ako aj mechanizmus zoznamu zrušení osvedčení podľa požiadavky EAA-6.2.10.1-02.

— EAA-6.2.10.1-17: Štruktúra stavu v objekte MSO je štruktúrou CBOR s touto definíciou CDDL:

Status = {

? 'identifier_list': IdentifierListInfo,

? 'status_list': StatusListInfo,

* tstr => RFU

}“

PRÍLOHA V

„PRÍLOHA III

Technické špecifikácie uvedené v článku 10

— Technické špecifikácie:

  — bod 4.2.5 ETSI TS 119 472-3 V1.1.1 (2026-03).“

PRÍLOHA VI

Príloha IV vykonávacieho nariadenia (EÚ) 2024/2979 sa mení takto:

1. Bod 1 sa nahrádza takto:

„1. Povinný formát podpisu alebo pečate:

a) PAdES (PDF Advanced Electronic Signature) špecifikovaný v ETSI EN 319 142-1 V1.2.1 (2024-01); elektronické podpisy a infraštruktúry (ESI); digitálne podpisy PAdES; časť 1: základné moduly a základné podpisy PAdES.“

2. Bod 3 sa nahrádza takto:

„3. Aplikačné programovacie rozhranie:
body 6.4.3, A.6, A.7 a A.8 ETSI TS 119 432 v1.3.1 (2026-03).“

PRÍLOHA VII

„PRÍLOHA VI

Značka dôvery EÚ pre peňaženku digitálnej identity vo farebnej verzii



“

PRÍLOHA VIII

„PRÍLOHA VII

Značka dôvery EÚ pre peňaženku digitálnej identity v čiernobielej verzii



“

PRÍLOHA IX

„PRÍLOHA VIII

Údaje o značke dôvery EÚ pre peňaženku digitálnej identity

Údaje	Opis	Kódovanie	Stav
TrustMarkResourceURL	Adresa URL grafiky značky dôvery EÚ pre peňaženku digitálnej identity a zdrojov informácií pre používateľov v používateľskom rozhraní peňaženky.	URL	povinný údaj
ListOfCertifiedWalletsURL	Adresa URL verejného zoznamu certifikovaných riešení peňaženky v EÚ, ako sa uvádza vo vykonávacom nariadení Komisie (EÚ) 2025/849 ([1]).	URL	povinný údaj
ListOfCertifiedWalletsQRCode	QR Code obsahujúci informácie o ListOfCertifiedWalletsURL.	ISO-8859-1 Byte mode QR code	nepovinný údaj
WalletSolutionInfoPageURL	Adresa URL stránky s informáciami o certifikovanom riešení peňaženky zo zoznamu stránky certifikovaných riešení peňaženky z ListOfCertifiedWalletsURL URL doplnená o „?“ a identifikátor riešenia peňaženky WalletSolutionID.	URL	povinný údaj
WalletSolutionInfoPageQRCode	Kód QR obsahujúci informácie o WalletSolutionInfoPageURL.	ISO-8859-1 Byte mode QR code	nepovinný údaj
WalletVerifierToolURL*	Adresa URL smerujúca na koncový bod */.well-known/openid-credential-issuer* nástroja na overenie peňaženky, ktorý sa používa na získanie metaúdajov poskytovateľa osvedčenia.	URL	nepovinný údaj

([1]) Vykonávacie nariadenie Komisie (EÚ) 2025/849 zo 6. mája 2025, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o predkladanie informácií do zoznamu certifikovaných európskych peňaženiek digitálnej identity Komisii a skupine pre spoluprácu (Ú. v. EÚ L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).“

PRÍLOHA X

Príloha II k vykonávaciemu nariadeniu (EÚ) 2024/2980 sa mení takto:

1. V prílohe II oddiele 1 bode 1 sa písmeno i) nahrádza takto:

„i) jeden alebo viacero certifikátov spĺňajúcich normu ETSI EN 319 412-2 V2.4.1 (2025-06) alebo normu ETSI EN 319 412-3 V1.3.1 (2023-09), ktoré možno použiť na overenie podpisu alebo pečate vytvorenej registrátorom na registračných údajoch a v prípade ktorých certifikované údaje o totožnosti obsahujú meno a prípadne registračné číslo registrátora, ako je stanovené v písmenách c) a d).“

2. V prílohe II oddiele 2 bode 1 sa písmeno h) nahrádza takto:

„h) jeden alebo viacero certifikátov spĺňajúcich normu ETSI EN 319 412-2 V2.4.1 (2025-06) alebo normu ETSI EN 319 412-3 V1.3.1 (2023-09), ktoré možno použiť na autentifikáciu a validáciu osvedčení jednotky peňaženky, ktoré vydal poskytovateľ peňaženky a v prípade ktorých certifikované údaje o totožnosti obsahujú názov a prípadne registračné číslo poskytovateľa peňaženky, ako je stanovené v písmenách a) a b);“.

3. V prílohe II oddiele 3 bode 1 sa písmeno h) nahrádza takto:

„h) jeden alebo viacero certifikátov spĺňajúcich normu ETSI EN 319 412-2 V2.4.1 (2025-06) alebo normu ETSI EN 319 412-3 V1.3.1 (2023-09), ktoré možno použiť na overenie podpisu alebo pečate vytvorenej poskytovateľom osobných identifikačných údajov na osobných identifikačných údajoch, ktoré poskytuje, a v prípade ktorých certifikované údaje o totožnosti zahŕňajú meno a prípadne registračné číslo poskytovateľa osobných identifikačných údajov, ako je stanovené v písmenách a) a b).“

4. V prílohe II oddiele 4 bode 1 sa písmeno g) nahrádza takto:

„g) jeden alebo viacero certifikátov spĺňajúcich normu ETSI EN 319 412-2 V2.4.1 (2025-06) alebo normu ETSI EN 319 412-3 V1.3.1 (2023-09), ktoré možno použiť na overenie podpisu alebo pečate vytvorenej poskytovateľom prístupových certifikátov strany spoliehajúcej sa na peňaženku na prístupovom certifikáte, ktorý poskytuje stranám spoliehajúcim sa na peňaženku, prípadne s informáciami potrebnými na odlíšenie prístupových certifikátov strany spoliehajúcej sa na peňaženku od iných certifikátov.“

5. V prílohe II sa pridáva tento oddiel 5:

„5. Oznámenia informácií o poskytovateľoch registračných certifikátov strany spoliehajúcej sa na peňaženku

1. Členské štáty poskytnú Komisii tieto informácie o poskytovateľoch registračných certifikátov strany spoliehajúcej sa na peňaženku:

a) názov poskytovateľa registračných certifikátov strany spoliehajúcej sa na peňaženku;

b) prípadne registračné číslo poskytovateľa registračných certifikátov strany spoliehajúcej sa na peňaženku;

c) členský štát, v ktorom je poskytovateľ registračných certifikátov strany spoliehajúcej sa na peňaženku usadený;

d) kontaktnú e-mailovú adresu a kontaktné telefónne číslo poskytovateľa registračných certifikátov strany spoliehajúcej sa na peňaženku v záležitostiach týkajúcich sa registračných certifikátov, ktoré poskytuje stranám spoliehajúcim sa na peňaženku;

e) prípadne adresu URL webovej stránky poskytovateľa registračných certifikátov strany spoliehajúcej sa na peňaženku, ktorá obsahuje ďalšie informácie o poskytovateľovi a registračných certifikátoch, ktoré poskytuje stranám spoliehajúcim sa na peňaženku;

f) adresu URL webovej stránky, ktorá obsahuje pravidlá a podmienky vzťahujúce sa na poskytovanie a používanie registračných certifikátov, ktoré poskytuje stranám spoliehajúcim sa na peňaženku;

g) jeden alebo viacero certifikátov spĺňajúcich normu ETSI EN 319 412-2 V2.4.1 (2025-06) alebo normu ETSI EN 319 412-3 V1.3.1 (2023-09), ktoré možno použiť na overenie podpisu alebo pečate vytvorenej poskytovateľom registračných certifikátov strany spoliehajúcej sa na peňaženku na registračných certifikátoch, ktoré poskytuje stranám spoliehajúcim sa na peňaženku, prípadne s informáciami potrebnými na odlíšenie registračných certifikátov strany spoliehajúcej sa na peňaženku od iných certifikátov.

2. Informácie uvedené v bode 1 sa poskytujú za každého poskytovateľa registračných certifikátov strany spoliehajúcej sa na peňaženku.“

PRÍLOHA XI

„PRÍLOHA I

Protokoly a rozhrania uvedené v článku 4

Technická špecifikácia ETSI TS 119 472-3 V1.1.1 (2026-03) sa uplatňuje s týmito úpravami:

1. 4.1. General requirements (Všeobecné požiadavky)

   — GEN-REQ-4.1-05: neplatné.

   — POZNÁMKA: neplatné.

2. 4.2.3. Provision of registration certificates of PID/EAA Provider to EUDI Wallet (Poskytovanie registračných certifikátov poskytovateľa PID/EAA európskej peňaženke digitálnej identity)

   — ISS-MDATA-REG_CERT-4.2.3-04: Jeden z prvkov v parametri poľa issuer_info musí obsahovať registračný certifikát poskytovateľa PID/EAA.

   — ISS-MDATA-REG_CERT-4.2.3-07: neplatné.

   — ISS-MDATA-REG_CERT-4.2.3-08: neplatné.

   — ISS-MDATA-REG_CERT-4.2.3-09: neplatné.

   — ISS-MDATA-REG_CERT-4.2.3-10: neplatné.

   — ISS-MDATA-REG_CERT-4.2.3-11: neplatné.

   — ISS-MDATA-REG_CERT-4.2.3-12: neplatné.

   — ISS-MDATA-REG_CERT-4.2.3-13: neplatné.

3. 4.2.4.2 ARF pre-defined PID/EAA reuse policy (Preddefinovaná politika ARF týkajúca sa opätovného použitia PID/EAA)

   — ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Ak má člen id hodnotu ‚arf_annex_ii' a pole priradené k označeniu ‚details' obsahuje hodnotu ‚once_only' alebo hodnotu ‚per-relying-party', potom objekt JSON, ktorý obsahuje toto pole priradené k označeniu ‚details', obsahuje aj číslo JSON priradené k označeniu ‚reissue_trigger_unused'.

4. Príloha A sa neuplatňuje."

PRÍLOHA XII

„PRÍLOHA II

Technické špecifikácie uvedené v článku 5

Uplatňuje sa technická špecifikácia v prílohe C k norme ISO/IEC 18013-7:2025.

Technické špecifikácie v bodoch 4.1, 4.2, 5 a 6 ETSI TS 119 472-2 V1.2.1 (2026-03) sa uplatňujú s týmito úpravami vrátane vloženia nového bodu 4.3:

1. 1. Scope (Rozsah)

— V tomto dokumente sa špecifikujú dva profily protokolov, ktoré umožňujú spoliehajúcim sa stranám (ďalej len ‚RP‘) požiadať európsku peňaženku digitálnej identity o EAAP alebo osobné identifikačné údaje (ďalej len ‚PID‘) a európskej peňaženke digitálnej identity umožňujú zaslať RP požadované EAAP/PID. Každý z profilov podporuje dva mechanizmy prenosu, a to: sprostredkovaný API a nesprostredkovaný API, ako je uvedené ďalej v texte:

a) Profil vychádza z normy:

— ISO/IEC 18013-5 [10] len v prípade mechanizmu prenosu nesprostredkovaného API a

— prílohy C k norme ISO/IEC 18013-7 [16] v prípade mechanizmu prenosu sprostredkovaného API.

Tento profil sa nazýva profil ISO/IEC-mdoc a je definovaný v bode 5 tohto dokumentu.

b) Profil vychádza z normy:

OpenID4VC-HAIP [11] v prípade mechanizmu prenosu sprostredkovaného aj nesprostredkovaného API, a to takto:

— oddiely 5, 5.1, 5.3, 7 a 8 [11] v prípade prenosu prostredníctvom presmerovania alebo mechanizmu prenosu nesprostredkovaného API a

— oddiely 5, 5.2, 5.3, 7 a 8 [11] v prípade mechanizmu prenosu sprostredkovaného API.

Tento profil sa nazýva profil OpenID4VC-HAIP a je definovaný v bode 6 tohto dokumentu.

2. 2.1. Normative references (Normatívne odkazy)

— [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‘ [Osobná identifikácia – vodičský preukaz v súlade s normou ISO – časť 7: doplnkové funkcie mobilného vodičského preukazu (mDL)].

3. 4.1. EAAP implementation based on SD-JWT VC (Zavádzanie EAAP založené na SD-JWT VC)

— EAAP-SD-JWT VC-04: neplatné.

4. 4.2. EAAP implementation based on ISO/IEC-mdoc (Zavádzanie EAAP založené na ISO/IEC-mdoc)

— EAAP-ISO/IEC-mdoc-01: neplatné.

— *Poznámka 2*: neplatné.

— EAAP-ISO/IEC-mdoc-02: neplatné.

5. 4.3. EAAP implementation with mediating API (Zavádzanie EAAP so sprostredkujúcim API)

— EAAP-API-GEN-01: Európska peňaženka digitálnej identity podporuje sprostredkujúce API, ktoré podporuje oba protokoly definované v bode 5.2 [11] a v prílohe C k [16].

— *POZNÁMKA*: Ak zariadenie, v ktorom je európska peňaženka digitálnej identity nainštalovaná, nepodporuje oba protokoly, túto požiadavku nemožno splniť a vzniká nesúlad, pretože základné operačné systémy a prehliadače nezavádzajú potrebné prvky interoperability.

— EAAP-API-GEN-02: Európska peňaženka digitálnej identity podporuje sprostredkujúce API aspoň pre PID a typy EAA registrované v katalógu schém, ako sa vymedzuje vo vykonávacom nariadení (EÚ) 2025/1569, a aspoň pre všetky formáty vymedzené v prílohe II k vykonávaciemu nariadeniu (EÚ) 2024/2979.

— *POZNÁMKA* 1: Ak základný operačný systém, prehliadač, sprostredkujúce API alebo akákoľvek iná technická vrstva mimo kontroly európskej peňaženky digitálnej identity obmedzuje, filtruje, predbežne vyberá alebo inak limituje formáty poverení a typy PID a EAA registrované v katalógu schém, túto požiadavku nemožno splniť. Ak takéto obmedzenie bráni európskej peňaženke digitálnej identity podporovať registrovaný typ alebo formát poverenia, výsledný nesúlad možno pripísať tomu, že uvedené základné operačné systémy, prehliadače, sprostredkujúce rozhranie API alebo iná príslušná technická vrstva pri neposkytla potrebné prvky interoperability.

6. 4.4. Validácia strany spoliehajúcej sa na peňaženku a kontroly nadmerných žiadostí

— WRP-VALIDATION-01: Európska peňaženka digitálnej identity validuje registračný certifikát strany spoliehajúcej sa na peňaženku prijatý v žiadosti pred tým, ako používateľovi peňaženky predloží na schválenie akékoľvek požadované PID alebo elektronické osvedčenie atribútov.

— WRP-VALIDATION-02: Ak validácia registračného certifikátu strany spoliehajúcej sa na peňaženku zlyhá, a to aj v prípade, že platnosť certifikátu uplynula, bol zrušený, nebol vydaný platným dôveryhodným poskytovateľom registračných certifikátov strany spoliehajúcej sa na peňaženku, bol chybne vytvorený alebo ho nemožno kryptograficky overiť, európska peňaženka digitálnej identity upozorní používateľa peňaženky, že stranu spoliehajúcu sa na peňaženku nebolo možné validovať, a žiadosť nepredloží ako úspešne validovanú. Používateľ peňaženky výslovne schváli žiadosť spoliehajúcej sa strany. Mlčanie ani vopred začiarknuté políčka na výslovné schválenie nestačia.

— WRP-VALIDATION-03: Poskytovateľ peňaženky na základe svojej analýzy rizík a bezpečnostnej politiky určí, či a za akých podmienok môže používateľ peňaženky obísť konkrétne neúspešné validačné kontroly.

— WRP-OVERASKING-01: Európska peňaženka digitálnej identity porovná osvedčenia a atribúty požadované stranou spoliehajúcou sa na peňaženku s registrovanými osvedčeniami a atribútmi v registračnom certifikáte strany spoliehajúcej sa na peňaženku.

— WRP-OVERASKING-02: Ak strana spoliehajúca sa na peňaženku požaduje PID alebo elektronické osvedčenia atribútov, alebo tvrdenia, na ktoré sa nevzťahuje registračný certifikát strany spoliehajúcej sa na peňaženku, európska peňaženka digitálnej identity používateľa peňaženky jasne varuje pred akýmkoľvek sprístupnením. Vo varovaní sa uvedie, že strana spoliehajúca sa na peňaženku žiada o viac informácií, než zaregistrovala. Používateľ peňaženky výslovne schváli žiadosť spoliehajúcej sa strany. Mlčanie ani vopred začiarknuté políčka na výslovné schválenie nestačia.

— WRP-OVERASKING-03: Poskytovateľ peňaženky na základe svojej analýzy rizík, bezpečnostnej politiky a uplatniteľného práva určí, či používateľ peňaženky môže pokračovať napriek takémuto varovaniu, či sa môže sprístupniť len podsúbor požadovaných údajov, na ktoré sa vzťahuje registračný certifikát, alebo či sa žiadosť zamietne.

7. 5.1. Introduction (Úvod)

— V bode 5 a jeho podbodoch sa vymedzuje profil protokolu, ktorý umožňuje RP požiadať európsku peňaženku digitálnej identity o EAAP alebo PID a európskej peňaženke digitálnej identity umožňuje zaslať RP požadované EAAP/PID buď pomocou mechanizmu prenosu nesprostredkovaného API, ktorý vychádza z normy ISO/IEC 18013-5 [10], alebo mechanizmu prenosu sprostredkovaného API, ktorý vychádza z prílohy C k norme ISO/IEC 18013-7 [16], na prenos dátových štruktúr vymedzených v norme ISO/IEC 18013-5 [10], ktoré sú vhodne zapuzdrené.

— Zvyšok bodu 5 je štruktúrovaný takto:

— v bode 5.2 sa definujú požiadavky na podporu profilu a mechanizmy prenosu zo strany RP a európskej peňaženky digitálnej identity,

— v bode 5.3 sa špecifikujú požiadavky, ktoré sú špecifické pre mechanizmus prenosu nesprostredkovaný API,

— v bode 5.4 a jeho podbodoch sa špecifikujú požiadavky, ktoré sú špecifické pre mechanizmus prenosu sprostredkovaný API.

8. 5.2. Requirements on EUDI Wallet and RP support (Požiadavky na podporu európskej peňaženky digitálnej identity a RP)

— ISO/IEC 18013-SUPPORT-01: Jednotky peňaženky, poskytovatelia PID, poskytovatelia osvedčení, poskytovatelia peňaženky a spoliehajúce sa strany nepodporujú získavanie údajov zo serverov podľa normy ISO/IEC 18013-5 [10] na vyžiadanie a predloženie PID alebo osvedčenia atribútov.

— ISO/IEC 18013-SUPPORT-02: Európska peňaženka digitálnej identity musí spĺňať požiadavky definované v bodoch 5.3 a 5.4 tohto dokumentu.

— ISO/IEC 18013-SUPPORT-04: Spoliehajúca sa strana by mala zaviesť profil definovaný v bode 5.4 tohto dokumentu.

9. 5.3.2. ISO/IEC-mdoc EAAP Request contents (Obsah žiadosti EAAP ISO/IEC-mdoc)

— ISO/IEC 18013-5-REQ-04: Žiadosti zariadenia odoslané do európskych peňaženiek digitálnej identity obsahujú dvojicu kľúč – hodnota ‚requestInfo' podľa bodu 8.3.2.1.2.1 [10]. Hodnota tejto dvojice musí byť typu RequestInfo.

— ISO/IEC 18013-5-REQ-05: Typ RequestInfo musí zodpovedať definícii CDDL uvedenej ďalej v texte.

RequestInfo = {

‚euWrprc': bstr ; obsahuje registračný certifikát (pozri požiadavky uvedené ďalej).

}

— ISO/IEC 18013-5-REQ-06: Uvedený člen requestInfo obsahuje člen s označením ‚euWrprc'.

— ISO/IEC 18013-5-REQ-07: Hodnotou ‚euWrprc' je registračný certifikát zakódovaný v CBOR.

— ISO/IEC 18013-5-REQ-08: neplatné.

— *POZNÁMKA 3*: neplatné.

— ISO/IEC 18013-5-REQ-09: neplatné.

— ISO/IEC 18013-5-REQ-10: neplatné.

— ISO/IEC 18013-5-REQ-11: neplatné.

10. 5.3.3. ISO/IEC-mdoc EAAP Response profile (Profil odpovede EAAP ISO/IEC-mdoc)

— V tomto bode sa vymedzujú požiadavky na typ správy DeviceResponse, ktorý je spoločný pre oba typy mechanizmov prenosu (sprostredkovaných API a nesprostredkovaných API).

— *POZNÁMKA 1:* Ak sa používa mechanizmus nesprostredkovaný API vychádzajúci z normy ISO/IEC 18013-5 [10], odpoveď EAAP je presne inštanciou DeviceResponse, ako sa špecifikuje v tomto bode. Ak sa používa mechanizmus sprostredkovaný API, ktorý vychádza z prílohy C k norme ISO/IEC 18013-7 [16], inštancia DeviceRequest je zapuzdrená, ako sa uvádza v prílohe C k [16].

— ISO/IEC 18013-5-RESP-02: Poskytovateľ osobných identifikačných údajov a elektronických osvedčení atribútov nezahrnie do mapy KeyAuthorizations v objekte mobilnej bezpečnosti žiadne údajové prvky osobných identifikačných údajov a elektronických osvedčení atribútov, ktoré vydáva, s výnimkou údajových prvkov, ktoré poskytuje strana spoliehajúca sa na peňaženku v údajoch o transakciách v žiadosti o mdoc, ktorú má podpísať alebo zapečatiť jednotka peňaženky pomocou súkromného kľúča osobných identifikačných údajov alebo elektronických osvedčení atribútov.

— *POZNÁMKA 2:* V dôsledku toho jednotky peňaženky nemôžu stranám spoliehajúcim sa na peňaženku predložiť žiadne údajové prvky podpísané zariadením s výnimkou podpisovania údajov, ktoré poskytla strana spoliehajúca sa na peňaženku, napríklad v prípadoch použitia na zabezpečenú autentifikáciu používateľa.

— *POZNÁMKA 3:* V norme ISO/IEC 18013-5:2021 sa nešpecifikuje, ako môžu strany spoliehajúce sa na peňaženku zahrnúť údaje o transakciách do žiadosti o mdoc. Zahrnutie údajov o transakciách do žiadosti o mdoc sa uskutoční spolu s doplnením technických špecifikácií.

— ISO/IEC 18013-5-RESP-03: Poskytovatelia osobných identifikačných údajov nesmú umožniť, aby súkromný kľúč osobných identifikačných údajov podpisoval údajové prvky, ktoré poskytuje strana spoliehajúca sa na peňaženku, v údajoch o transakciách v žiadosti o mdoc.

11. 5.4. Requirements for API mediated mechanism (Požiadavky na mechanizmus sprostredkovaný API)

5.4.1. ISO/IEC 18013-7-related requirements (Požiadavky súvisiace s ISO/IEC 18013-7)

V tomto bode sa definujú požiadavky na mechanizmus prenosu sprostredkovaný API, ktoré súvisia s požiadavkami definovanými v prílohe C k [16].

— ISO/IEC 18013-7-API-01: Profil podporujúci predloženia sprostredkované API musí spĺňať požiadavky prílohy C k norme ISO/IEC 18013-7 [16], ako sa ďalej špecifikuje v bodoch 5.3 a 5.4 tohto dokumentu.

— ISO/IEC 18013-7-API-02: Všetky povinné požiadavky definované v prílohe C [16] sa uplatňujú, ako sa ďalej špecifikuje v bodoch 5.3 a 5.4 tohto dokumentu.

— ISO/IEC 18013-7-API-03: Všetky nepovinné požiadavky definované v prílohe C [16] zostávajú nepovinnými, pokiaľ nie je v tomto dokumente uvedené inak.

12. 5.4.2. Additional requirements (Dodatočné požiadavky)

— V tomto bode sa špecifikujú dodatočné požiadavky na mechanizmus prenosu sprostredkovaný API.

— ISO/IEC 18013-ADD-API-01: V európskej peňaženke digitálnej identity sa štandardne zverejňuje prítomnosť všetkých uložených typov elektronických osvedčení atribútov sprostredkujúcemu API, ktoré funguje v súlade s prílohou C k [16], ale nezverejňujú sa atribúty a ich hodnoty v týchto elektronických osvedčeniach atribútov.

  — *POZNÁMKA 1*: Obmedzenie hodnoty atribútu sa uplatňuje aj vtedy, ak by sa takýmto zverejnením zlepšili služby, ktoré operačný systém poskytuje európskej peňaženke digitálnej identity, napríklad výber osvedčenia v kontexte sprostredkujúceho API.

— Niektoré aspekty týkajúce sa operačných systémov a prehliadačov sú mimo kontroly implementátorov, tieto možno zohľadniť spôsobom uvedeným v poznámkach 2 až 4.

  — *POZNÁMKA 2*: Žiadosť o predloženie od spoliehajúcej sa strany, ktorá podporuje prílohu C k [16], môže byť spracovaná prehliadačom a/alebo operačným systémom na účely vyhľadania dostupných EAA, predchádzania podvodom zameraným na používateľa alebo riešenia problémov.

  — *POZNÁMKA 3*: Očakáva sa, že žiadosť o predloženie od spoliehajúcej sa strany, ktorá podporuje prílohu C k [16], bude spracovaná prehliadačom a/alebo operačným systémom na účely bezpečnosti používateľa.

— *POZNÁMKA 4*: Očakáva sa, že žiadosť o predloženie od spoliehajúcej sa strany, ktorá podporuje prílohu C k [16], nebude spracovaná prehliadačom a/ani operačným systémom na účely analýzy trhu (vrátane sekundárneho účelu) ani na interné účely prehliadača a/alebo operačného systému.

— ISO/IEC 18013-ADD-API-02: Ak európska peňaženka digitálnej identity na žiadosť používateľa vymaže PID alebo osvedčenia EAA, ktoré boli predtým poskytnuté sprostredkujúcemu API fungujúcemu v súlade s prílohou C k [16], európska peňaženka digitálnej identity zverejní skutočnosť, že tieto PID alebo osvedčenie EAA už neuchováva v sprostredkujúcom API.

— ISO/IEC 18013-ADD-API-03: Ak používateľ odinštaluje svoju európsku peňaženku digitálnej identity, táto peňaženka zverejní skutočnosť, že už neuchováva žiadne predtým zverejnené PID ani EAA, pre sprostredkovateľské API fungujúce v súlade s prílohou C k [16].

— ISO/IEC 18013-ADD-API-04: Európska peňaženka digitálnej identity poskytuje globálne používateľské nastavenie na znemožnenie zverejnenia uložených osvedčení EAA prostredníctvom sprostredkujúceho API fungujúceho podľa normy ISO/IEC 18013-ADD-API-01. Ak je toto nastavenie deaktivované, európska peňaženka digitálnej identity nesmie oznamovať svoju dostupnosť ani reagovať na žiadosti o predloženie alebo vydanie sprostredkované API.

— ISO/IEC 18013-ADD-API-05: Európske peňaženky digitálnej identity v tokoch medzi zariadeniami pomocou sprostredkujúceho API overujú, či sa komunikujúce zariadenie nachádza v tesnej fyzickej blízkosti európskej peňaženky digitálnej identity, pričom kontrolu fyzickej blízkosti vykonávajú pomocou zabezpečeného, priameho miestneho komunikačného kanála sprostredkovaného používateľom, ako je bezdrôtová komunikačná technológia s krátkym dosahom.

— *POZNÁMKA*: CTAP 2.3 umožňuje použiť BLE na vykonanie kontroly tesnej fyzickej blízkosti, a ak je zavedený oboma zariadeniami, umožňuje aj prenos údajov medzi zariadeniami prostredníctvom prenosových technológií s krátkym dosahom. Základné operačné systémy, prehliadače, sprostredkujúce rozhrania API alebo akákoľvek iná technická vrstva mimo kontroly európskej peňaženky digitálnej identity by mali pri vykonávaní kontroly fyzickej blízkosti aj prenosu údajov medzi danými dvoma zariadeniami uprednostniť použitie miestneho komunikačného kanála, ako to umožňuje CTAP 2.3, pred použitím hybridných tunelových služieb CTAP.

13. 6.2. Requirements on EUDI Wallet and RP support (Požiadavky na podporu európskej peňaženky digitálnej identity a RP)

— OIDFVP-HAIP-SUPPORT-02: Európska peňaženka digitálnej identity musí spĺňať požiadavky uvedené v bode 6.5 tejto prílohy.

— OIDFVP-HAIP-SUPPORT-03: Európska peňaženka digitálnej identity by nemala podporovať mechanizmus založený na presmerovaní uvedený v bode 6.4 pre toky predkladania medzi zariadeniami.

— *POZNÁMKA 3*: Použitie tohto mechanizmu je zraniteľné voči útokom, ako je fixovanie relácií. Zmierňovanie takýchto útokov je na spoliehajúcich sa stranách. Zavedenie tohto mechanizmu by nemalo viesť k nedodržiavaniu predpisov.

— OIDFVP-HAIP-SUPPORT-05: Spoliehajúca sa strana musí spĺňať požiadavky uvedené v bodoch 6.5 tejto prílohy.

— *POZNÁMKA 5*: neplatné.

14. 6.3.1. General requirements (Všeobecné požiadavky)

— OIDFVP-HAIP-GEN-01: Uplatňujú sa všetky povinné požiadavky uvedené v bodoch 5, 5.3, 7 a 8 HAIP [11].

— *POZNÁMKA 1*: ‚Oddiel 5 HAIP [11]' odkazuje len na požiadavky priamo pod nadpisom oddielu 5. Nezahŕňa to oddiely 5.1, 5.2 a 5.3.

— OIDFVP-HAIP-GEN-03: Ak sa touto prílohou mení požiadavka v OpenID4VC-HAIP [11], prednosť má zmenená požiadavka uvedená v tejto prílohe.

— *POZNÁMKA 2*: Umožnilo by to napr. zmeniť nepovinnú požiadavku z OpenID4VC-HAIP [11] na povinnú alebo rozšíriť povinné požiadavky.

— OIDFVP-HAIP-GEN-04: Ak je formát požadovaného osvedčenia v súlade s [10], spoliehajúce sa strany a európske peňaženky digitálnej identity musia byť v súlade s profilom ‚ISO mdocs' v [11] oddiele 6.

— *POZNÁMKA 3*: Na účely lepšej zrozumiteľnosti: profil ‚ISO mdocs' v HAIP znamená, že spoliehajúce sa strany a európske peňaženky digitálnej identity musia spĺňať príslušné požiadavky uvedené prílohe B.2 k [7].

— OIDFVP-HAIP-GEN-05: Ak je formát požadovaného osvedčenia v súlade s [2], spoliehajúce sa strany a európske peňaženky digitálnej identity musia byť v súlade s profilom ‚IETF SD-JWT VCs' v [11] oddiele 6.

— *POZNÁMKA 4*: Na účely lepšej zrozumiteľnosti: profil ‚IETF SD-JWT VCs' znamená, že spoliehajúce sa strany a európske peňaženky digitálnej identity musia spĺňať požiadavky uvedené v prílohe B.3 k [7], ako aj požiadavky uvedené v [11] oddiele 6.1.

15. 6.3.2.1. General requirements (Všeobecné požiadavky)

— OIDFVP-HAIP-COMMON-REQ-01: void.

16. 6.3.2.2. Requirements for the Request Object (Požiadavky na objekt žiadosti)

— OIDFVP-HAIP-COMMON-REQ-RO-02: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-03: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-04: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-05: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-06: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-07: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-08: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-09: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-10: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-11: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-12: neplatné.

— *Poznámka 2*: neplatné.

— OIDFVP-HAIP-COMMON-REQ-RO-13: Jeden z prvkov parametra verifier_info zahŕňa registračný certifikát.

— OIDFVP-HAIP-COMMON-REQ-RO-23: Koncový certifikát uvedený v oddiele 5.9.3 OpenID4VP, ktorý sa má použiť s predponou identifikátora klienta x509_hash Client Identifier Prefix, je prístupovým certifikátom RP podľa ETSI TS 119 475 [14].

17. 6.3.3. Authorization Response (EAAP response) profile [Profil autorizačnej odpovede (EAAP)]

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

18. 6.4.1. General requirements (Všeobecné požiadavky)

— OIDFVP-HAIP-REDIRECTS-04: neplatné.

— POZNÁMKA: neplatné.

19. 6.5.2. Additional requirements (Dodatočné požiadavky)

— OIDFVP-HAIP-ADD-API-01: V európskej peňaženke digitálnej identity sa štandardne zverejňuje prítomnosť všetkých typov elektronických osvedčení atribútov sprostredkujúcemu API fungujúcemu v súlade s bodom 5.2 [11], ale nezverejňujú sa atribúty a ich hodnoty v týchto osvedčeniach.

— OIDFVP-HAIP-ADD-API-04: Ak európska peňaženka digitálnej identity podporuje sprostredkujúce API, ktoré funguje podľa požiadavky OIDFVP-HAIP-ADD-API-01, musí poskytovať globálne používateľské nastavenie na zakázanie sprístupňovania uložených osvedčení EAA prostredníctvom sprostredkujúceho API. Ak je toto nastavenie nastavené na zakázané sprístupňovanie, európska peňaženka digitálnej identity by mala následne umožniť používateľovi vybrať jednotlivé osvedčenia, ktoré budú sprístupnené sprostredkujúcemu API.

— OIDFVP-HAIP-ADD-API-05: Európske peňaženky digitálnej identity v tokoch medzi zariadeniami pomocou sprostredkujúceho API overujú, či sa komunikujúce zariadenie nachádza v tesnej fyzickej blízkosti európskej peňaženky digitálnej identity, pričom kontrolu fyzickej blízkosti vykonávajú pomocou zabezpečeného, priameho miestneho komunikačného kanála sprostredkovaného používateľom, ako je bezdrôtová komunikačná technológia s krátkym dosahom.

— *POZNÁMKA 5*: CTAP 2.3 umožňuje použiť BLE na vykonanie kontroly tesnej fyzickej blízkosti, a ak je zavedený oboma zariadeniami, umožňuje aj prenos údajov medzi zariadeniami prostredníctvom prenosových technológií s krátkym dosahom. Základné operačné systémy, prehliadače, sprostredkujúce rozhrania API alebo akákoľvek iná technická vrstva mimo kontroly európskej peňaženky digitálnej identity by mali pri vykonávaní kontroly fyzickej blízkosti aj prenosu údajov medzi danými dvoma zariadeniami uprednostniť použitie miestneho komunikačného kanála, ako to umožňuje CTAP 2.3, pred použitím hybridných tunelových služieb CTAP.

20. 6.5.3. Specific requirements when requesting ISO/IEC 18013-5 EAAP (Osobitné požiadavky pri žiadostiach o EAAP podľa ISO/IEC 18013-5)

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Všetky požiadavky uvedené v tomto dokumente, ktoré sa vzťahujú na štruktúry žiadosti zariadenia a odpovede zariadenia uvedené v norme ISO/IEC 18013-5, sa uplatňujú aj vtedy, keď európska peňaženka digitálnej identity dostane žiadosť o predloženie ISO/IEC mdoc prostredníctvom mechanizmu prenosu pomocou API uvedeného v bode C.1 [16].“