Uradni list
Evropske unije

SL
Serija L

2024/2979

4.12.2024

IZVEDBENA UREDBA KOMISIJE (EU) 2024/2979

z dne 28. novembra 2024

o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede celovitosti in temeljnih funkcionalnosti evropskih denarnic za digitalno identiteto

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) in zlasti člena 5a(23) Uredbe,

ob upoštevanju naslednjega:

(1) Evropski okvir za digitalno identiteto, vzpostavljen z Uredbo (EU) št. 910/2014, je ključni element pri vzpostavitvi varnega in interoperabilnega ekosistema digitalne identitete po vsej Uniji. Temelji na evropskih denarnicah za digitalno identiteto (v nadaljnjem besedilu: denarnice), njegov cilj pa je fizičnim in pravnim osebam olajšati dostop do storitev v državah članicah ter hkrati zagotoviti varstvo osebnih podatkov in zasebnosti.

(2) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta ([2]) in, kadar je ustrezno, Direktiva 2002/58/ES Evropskega parlamenta in Sveta ([3]) se uporabljata za vse dejavnosti obdelave osebnih podatkov na podlagi te uredbe.

(3) Člen 5a(23) Uredbe (EU) št. 910/2014 Komisijo pooblašča, da po potrebi določi zadevne specifikacije in postopke. To se doseže s štirimi izvedbenimi uredbami: glede protokolov in vmesnikov: Izvedbena uredba Komisije (EU) 2024/2982 ([4]); glede celovitosti in temeljnih funkcionalnosti: Izvedbena uredba Komisije (EU) 2024/2979 ([5]); glede identifikacijskih podatkov osebe in elektronskih potrdil o atributih: Izvedbena uredba Komisije (EU) 2024/2977 ([6]) ter glede priglasitev Komisiji: Izvedbena uredba Komisije (EU) 2024/2980 ([7]). Ta uredba določa ustrezne zahteve za celovitost in temeljne funkcionalnosti evropskih denarnic za digitalno identiteto.

([1]) UL L 257, 28.8.2014, str. 73, ELI: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

([2]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

([3]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) Izvedbena uredba Komisije (EU) 2024/2982 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede protokolov in vmesnikov, ki jih mora podpirati okvir za evropsko digitalno identiteto (UL L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj)

([5]) Izvedbena uredba Komisije (EU) 2024/2979 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede celovitosti in temeljnih funkcionalnosti evropskih denarnic za digitalno identiteto (UL L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Izvedbena uredba Komisije (EU) 2024/2977 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede identifikacijskih podatkov osebe in elektronskih potrdil o atributih, izdanih evropskim denarnicam za digitalno identiteto (UL L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Izvedbena uredba Komisije (EU) 2024/2980 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede priglasitev Komisiji v zvezi z ekosistemom evropske denarnice za digitalno identiteto (UL L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) Komisija redno ocenjuje nove tehnologije, prakse, standarde ali tehnične specifikacije. Za zagotovitev najvišje ravni harmonizacije med državami članicami za razvoj in certificiranje denarnic se tehnične specifikacije iz te uredbe opirajo na delo, opravljeno na podlagi Priporočila Komisije (EU) 2021/946 z dne 3. junija 2021 o skupnem unijskem naboru orodij za usklajen pristop k okviru za evropsko digitalno identiteto ([8]) ter zlasti arhitekturnega in referenčnega okvira. V skladu z uvodno izjavo 75 Uredbe (EU) 2024/1183 Evropskega parlamenta in Sveta ([9]) bi morala Komisija pregledovati in po potrebi posodabljati to izvedbeno uredbo, da bi bila usklajena s svetovnim razvojem ter arhitekturnim in referenčnim okvirom ter sledila najboljšim praksam na notranjem trgu.

(5) Za zagotovitev natančne komunikacije, tehnične diferenciacije in jasne dodelitve odgovornosti je treba razlikovati med različnimi komponentami in konfiguracijami denarnic. Rešitev denarnice bi bilo treba razumeti kot celoten sistem, ki ga zagotavlja ponudnik denarnice in je potreben za upravljanje denarnice. Vključevati bi morala komponente programske in strojne opreme ter storitve, nastavitve in konfiguracije, potrebne za pravilno delovanje denarnice. Rešitev denarnice je lahko nameščena na napravah uporabnikov in v njihovih okoljih ter v zaledni strukturi ponudnika. Enoto denarnice bi bilo treba razumeti kot posebno nastavitev rešitve denarnice za posameznega uporabnika. Vključevati bi morala aplikacijo, nameščeno na napravi ali v okolju uporabnika denarnice, s katero uporabnik denarnice neposredno komunicira (v nadaljnjem besedilu: instanca denarnice), in potrebne varnostne elemente za zaščito podatkov in transakcij uporabnikov. Ti varnostni elementi bi morali vključevati posebno programsko ali strojno opremo za šifriranje in varovanje občutljivih informacij. Instanca denarnice bi morala biti del enote denarnice in uporabniku denarnice omogočati dostop do funkcionalnosti njegove denarnice.

(6) Varne kriptografske aplikacije denarnice kot ločene specializirane komponente enote denarnice so potrebne ne le za zaščito kritičnih sredstev, kot so kriptografski zasebni ključi, temveč tudi za zagotavljanje ključnih funkcionalnosti, kot je predložitev elektronskih potrdil o atributih. Uporaba skupnih tehničnih specifikacij lahko ponudnikom denarnic olajša dostop do vgrajenih varnostnih elementov. Varne kriptografske aplikacije denarnice se lahko zagotavljajo na različne načine in za različne vrste varnih kriptografskih naprav denarnice. Kadar ponudniki denarnic zagotavljajo varne kriptografske aplikacije denarnice kot programčke Java Card za vgrajene varnostne elemente, bi morali ponudniki denarnic upoštevati standarde iz Priloge I ali enakovredne tehnične specifikacije.

(7) Denarnice morajo ponudnikom identifikacijskih podatkov osebe ali elektronskih potrdil o atributih omogočiti preverjanje, ali te podatke ali potrdila izdajajo pristnim enotam denarnice uporabnika denarnice.

(8) Za zagotovitev vgrajenega in privzetega varstva podatkov bi bilo treba denarnicam zagotoviti razpoložljive najsodobnejše tehnike za izboljšanje zasebnosti. Te funkcije bi morale, če je to ustrezno v scenariju uporabe, omogočati uporabo denarnic, ne da bi bilo pri tem mogoče slediti uporabniku denarnice med različnimi na denarnice zanašajočimi se strankami. Ponudniki denarnic bi morali na primer razmisliti o najsodobnejših ukrepih za zaščito zasebnosti v zvezi s potrdili o enoti denarnice, na primer z uporabo kratkotrajnih potrdil o enoti denarnice ali serijsko izdajo. Poleg tega bi morale vgrajene politike razkrivanja opozarjati uporabnike denarnic pred neprimernim ali nezakonitim razkritjem atributov iz elektronskih potrdil o atributih.

(9) Potrdila o enoti denarnice bi morala na denarnice zanašajočim se strankam, ki od denarnic zahtevajo atribute, omogočiti, da preverijo status veljavnosti enote denarnice, s katero komunicirajo, saj se potrdila o enoti denarnice prekličejo, ko se enota denarnice ne šteje več za veljavno. Informacije o statusu veljavnosti enot denarnic bi morale biti na voljo na interoperabilen način za zagotovitev, da jih lahko uporabljajo vse na denarnice zanašajoče se stranke. Poleg tega bi morali ponudniki denarnic uporabnikom denarnic omogočiti, da zahtevajo preklic svoje enote denarnice v primeru njene izgube ali izgube nadzora nad njo. Za zagotovitev zasebnosti in nepovezljivosti bi morale države članice tehnike za ohranjanje zasebnosti uporabljati tudi za potrdilo o enoti denarnice. To lahko vključuje uporabo več potrdil o enoti denarnice za različne namene, razkritje le minimalnih ustreznih informacij o denarnici, potrebnih za transakcijo, ali omejitev življenjske dobe potrdila o enoti denarnice kot alternativo uporabi identifikatorjev za preklic.

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

([9]) Uredba (EU) 2024/1183 Evropskega parlamenta in Sveta z dne 11. aprila 2024 o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo evropskega okvira za digitalno identiteto (UL L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) Za zagotovitev, da so vse denarnice tehnično sposobne prejemati in predstavljati identifikacijske podatke osebe in elektronska potrdila o atributih v čezmejnih scenarijih, ne da bi pri tem ovirale interoperabilnost, bi morale denarnice podpirati vnaprej določene oblike zapisa podatkov in selektivno razkrivanje. Kot je določeno v Uredbi (EU) št. 910/2014, je selektivno razkrivanje koncept, ki lastniku podatkov omogoča, da razkrije le nekatere dele večjega nabora podatkov, da bi lahko prejemnik pridobil le tiste informacije, ki so potrebne za zagotavljanje storitve, ki jo zahteva uporabnik. Ker morajo denarnice uporabniku omogočiti selektivno razkrivanje atributov, bi bilo treba standarde iz Priloge II izvajati na način, ki omogoča to funkcijo denarnic. Poleg tega lahko denarnice podpirajo druge oblike in funkcionalnosti za omogočanje specifičnih primerov uporabe.

(11) Evidence transakcij so pomembno orodje za zagotavljanje preglednosti, saj uporabniku denarnice omogočajo pregled transakcij. Poleg tega bi se morale evidence uporabljati za omogočanje hitre in enostavne izmenjave nekaterih informacij na zahtevo uporabnika denarnice s pristojnimi nadzornimi organi, ustanovljenimi v skladu s členom 51 Uredbe (EU) 2016/679, v primeru sumljivega ravnanja na denarnice zanašajočih se strank.

(12) Da bi se uporabnik denarnice lahko elektronsko podpisal, bi se mu moralo izdati kvalificirano potrdilo, ki je vezano na napravo za ustvarjanje kvalificiranega elektronskega podpisa. Uporabnik denarnice bi moral imeti dostop do aplikacije za ustvarjanje podpisa. Čeprav je izdaja kvalificiranih potrdil v domeni ponudnikov kvalificiranih storitev zaupanja, bi morali imeti ponudniki denarnic ali drugi subjekti možnost, da zagotovijo druge komponente. Naprave za ustvarjanje kvalificiranega elektronskega podpisa lahko na primer upravljajo ponudniki kvalificiranih storitev zaupanja kot storitev ali pa so lahko nameščene lokalno v napravi uporabnika denarnice, na primer kot pametne kartice. Podobno so aplikacije za ustvarjanje podpisa lahko del instance denarnice, ločena aplikacija na napravi uporabnika denarnice ali pa se zagotavljajo na daljavo.

(13) Objekti za izvoz in prenosljivost podatkov lahko evidentirajo identifikacijske podatke osebe in elektronska potrdila o atributih, ki so bila izdana določeni enoti denarnice. Ti objekti uporabnikom denarnic omogočajo, da iz svoje enote denarnice pridobijo ustrezne podatke za okrepitev njihove pravice do prenosljivosti podatkov. Ponudnike denarnic se spodbuja k uporabi istih tehničnih rešitev tudi za izvajanje postopkov varnostnega kopiranja in obnovitve za enote denarnic, ki omogočajo obnovo izgubljenih enot denarnic ali prenos informacij od enega ponudnika denarnice k drugemu, kadar je to ustrezno in če je to mogoče storiti brez poseganja v pravico do varstva podatkov in varnost ekosistema digitalne identitete.

(14) Ustvarjanje psevdonimov, ki so specifični za na denarnice zanašajočo se stranko, bi moralo uporabnikom denarnic omogočiti, da se avtenticirajo, ne da bi na denarnice zanašajočim se strankam zagotovili nepotrebne informacije. Kot je določeno v Uredbi (EU) št. 910/2014, uporabniki denarnic ne smejo biti ovirani pri dostopu do storitev z uporabo psevdonima, kadar pravna identiteta za avtentikacijo ni zakonsko predpisana. Denarnice morajo zato vključevati funkcionalnost ustvarjanja psevdonimov, ki jih izbere in upravlja uporabnik, za avtentikacijo pri dostopanju do spletnih storitev. Izvajanje specifikacij iz Priloge V bi moralo ustrezno omogočati te funkcionalnosti. Na denarnice zanašajoče se stranke od uporabnikov tudi ne smejo zahtevati, da zagotovijo druge podatke, razen tistih, ki so v registru zanašajočih se strank navedeni za predvideno uporabo denarnic. Uporabnikom denarnice bi bilo treba omogočiti, da kadar koli preverijo podatke o registraciji zanašajočih se strank.

(15) Kot je določeno v Uredbi (EU) 2024/1183, države članice ne smejo neposredno ali posredno omejevati dostopa do javnih ali zasebnih storitev za fizične ali pravne osebe, ki se ne odločijo za uporabo denarnic, in morajo dati na voljo ustrezne alternativne rešitve.

(16) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([10]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 30. septembra 2024.

([10]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(17) Ukrepi iz te uredbe so v skladu z mnenjem odbora iz člena 48 Uredbe (EU) št. 910/2014 –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja in področje uporabe

Ta uredba določa pravila za celovitost in temeljne funkcionalnosti denarnic, ki jih je treba redno posodabljati, da bodo skladna z razvojem tehnologije in standardov ter delom, opravljenim na podlagi Priporočila Komisije (EU) 2021/946 ter zlasti arhitekturnega in referenčnega okvira.

Člen 2

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „varna kriptografska aplikacija denarnice“ pomeni aplikacijo, ki upravlja kritična sredstva tako, da je povezana s kriptografskimi in nekriptografskimi funkcijami, ki jih zagotavlja varna kriptografska naprava denarnice, in jih uporablja;

(2) „enota denarnice“ pomeni edinstveno konfiguracijo rešitve denarnice, ki vključuje instance denarnice, varne kriptografske aplikacije denarnice in varne kriptografske naprave denarnice, ki jih ponudnik denarnice zagotavlja posameznemu uporabniku denarnice;

(3) „kritična sredstva“ pomenijo sredstva znotraj enote denarnice ali v zvezi z njo, ki so tako izjemno pomembna, da bi ogrožanje njihove razpoložljivosti, zaupnosti ali celovitosti resno ogrozilo zmožnost zanašanja na enoto denarnice;

(4) „ponudnik identifikacijskih podatkov osebe“ pomeni fizično ali pravno osebo, odgovorno za izdajo in preklic identifikacijskih podatkov osebe ter zagotavljanje, da so uporabnikovi identifikacijski podatki osebe kriptografsko vezani na enoto denarnice;

(5) „uporabnik denarnice“ pomeni uporabnika, ki upravlja enoto denarnice;

(6) „na denarnice zanašajoča se stranka,“ pomeni zanašajočo se stranko, ki se namerava zanašati na enote denarnice za zagotavljanje javnih ali zasebnih storitev prek digitalne interakcije;

(7) „ponudnik denarnice“ pomeni fizično ali pravno osebo, ki zagotavlja rešitve denarnice;

(8) „potrdilo o enoti denarnice“ pomeni podatkovni objekt, ki opisuje komponente enote denarnice ali omogoča avtentikacijo in potrjevanje teh komponent;

(9) „vgrajena politika razkrivanja“ pomeni sklop pravil, ki jih ponudnik vključi v elektronsko potrdilo o atributih in v katerih so navedeni pogoji, ki jih mora izpolniti na denarnice zanašajoča se stranka za dostop do elektronskega potrdila o atributih;

(10) „instanca denarnice“ pomeni aplikacijo, nameščeno in konfigurirano na napravi ali v okolju uporabnika denarnice, ki je del enote denarnice in ki jo uporabnik denarnice uporablja za interakcijo z enoto denarnice;

(11) „rešitev denarnice“ pomeni kombinacijo programske opreme, strojne opreme, storitev, nastavitev in konfiguracij, vključno z instancami denarnic, eno ali več varnimi kriptografskimi aplikacijami denarnic in eno ali več varnimi kriptografskimi napravami denarnic;

(12) „varna kriptografska naprava denarnice“ pomeni napravo, odporno proti nedovoljenim posegom, ki zagotavlja okolje, ki je povezano z varno kriptografsko aplikacijo denarnice in ga ta uporablja za zaščito kritičnih sredstev ter zagotavljanje kriptografskih funkcij za varno izvajanje kritičnih operacij;

(13) „kriptografska operacija denarnice“ pomeni kriptografski mehanizem, potreben v okviru avtentikacije uporabnika denarnice in izdaje ali predstavitve identifikacijskih podatkov osebe ali elektronskih potrdil o atributih;

(14) „potrdilo o dostopu za na denarnice zanašajoče se stranke“ pomeni potrdilo za elektronski žig ali podpis za avtentikacijo ali potrjevanje na denarnice zanašajoče se stranke, ki ga izda ponudnik potrdil o dostopu za na denarnice zanašajoče se stranke;

(15) „ponudnik potrdil o dostopu za na denarnice zanašajoče se stranke“ pomeni fizično ali pravno osebo, ki jo država članica pooblasti za izdajanje potrdil o dostopu za na denarnice zanašajoče se stranke, registrirane v tej državi članici.

POGLAVJE II

CELOVITOST EVROPSKIH DENARNIC ZA DIGITALNO IDENTITETO

Člen 3

Celovitost enote denarnice

1. Denarnice ne izvajajo nobene funkcionalnosti iz člena 5a(4) Uredbe (EU) št. 910/2014, razen avtentikacije uporabnika denarnice za dostop do enote denarnice, dokler enota denarnice ne izvede uspešne avtentikacije uporabnika denarnice.

2. Ponudniki denarnic za vsako enoto denarnice podpišejo ali ožigosajo najmanj eno potrdilo o enoti denarnice, ki izpolnjuje zahteve iz člena 6. Potrdilo, ki se uporablja za podpisovanje ali žigosanje potrdila enote denarnice, se izda na podlagi certifikata z zanesljivega seznama iz Izvedbene uredbe (EU) 2024/2980.

Člen 4

Instance denarnice

1. Instance denarnic uporabljajo najmanj eno varno kriptografsko napravo denarnice za upravljanje kritičnih sredstev.

2. Ponudniki denarnic zagotovijo celovitost, avtentičnost in zaupnost komunikacije med instancami denarnic in varnimi kriptografskimi aplikacijami denarnic.

3. Kadar se kritična sredstva nanašajo na izvajanje elektronske identifikacije na visoki ravni zanesljivosti, se kriptografske operacije denarnice ali drugi postopki obdelave kritičnih sredstev izvajajo v skladu z zahtevami glede lastnosti in zasnove sredstev elektronske identifikacije na visoki ravni zanesljivosti, kot je določeno v Izvedbeni uredbi Komisije (EU) 2015/1502 ([11]).

Člen 5

Varne kriptografske aplikacije denarnice

1. Ponudniki denarnic zagotovijo, da varne kriptografske aplikacije denarnice:

(a) izvajajo kriptografske operacije denarnice, ki vključujejo kritična sredstva, razen tistih, ki jih enota denarnice potrebuje za avtentikacijo uporabnika denarnice, samo v primerih, ko so te aplikacije uspešno avtenticirale uporabnike denarnice;

([11]) Izvedbena uredba Komisije (EU) 2015/1502 z dne 8. septembra 2015 o določitvi minimalnih tehničnih specifikacij in postopkov za ravni zanesljivosti za sredstva elektronske identifikacije v skladu s členom 8(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (UL L 235, 9.9.2015, str. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

(b) kadar avtenticirajo uporabnike denarnic v okviru izvajanja elektronske identifikacije na visoki ravni zanesljivosti, to avtentikacijo opravijo v skladu z zahtevami glede lastnosti in zasnove sredstev elektronske identifikacije na visoki ravni zanesljivosti, kot je določeno v Izvedbeni uredbi (EU) 2015/1502;

(c) lahko varno ustvarjajo nove kriptografske ključe;

(d) lahko varno izbrišejo kritična sredstva;

(e) lahko ustvarijo dokazilo o imetju zasebnih ključev;

(f) ščitijo zasebne ključe, ki jih ustvarijo, med njihovim obstojem;

(g) izpolnjujejo zahteve glede lastnosti in zasnove sredstev elektronske identifikacije na visoki ravni zanesljivosti, kot je določeno v Izvedbeni uredbi (EU) 2015/1502;

(h) predstavljajo edine komponente, ki lahko izvajajo kriptografske operacije denarnice in vse druge operacije s kritičnimi sredstvi v okviru izvajanja elektronske identifikacije na visoki ravni zanesljivosti.

2. Kadar se ponudniki denarnic odločijo zagotoviti varno kriptografsko aplikacijo denarnice za vgrajeni varnostni element, svojo tehnično rešitev utemeljijo na tehničnih specifikacijah iz Priloge I ali drugih enakovrednih tehničnih specifikacijah.

Člen 6

Avtentičnost in veljavnost denarnice

1. Ponudniki denarnic zagotovijo, da vsaka enota denarnice vsebuje potrdila o enoti denarnice.

2. Ponudniki denarnic zagotovijo, da potrdila o enoti denarnice iz odstavka 1 vsebujejo javne ključe in da so ustrezni zasebni ključi zaščiteni z varno kriptografsko napravo denarnice.

3. Ponudniki denarnic:

(a) obvestijo uporabnike denarnic o njihovih pravicah in obveznostih v zvezi z njihovo enoto denarnice;

(b) zagotovijo mehanizme, neodvisne od denarnic, za varno identifikacijo in avtentikacijo uporabnikov denarnic;

(c) zagotovijo, da imajo uporabniki denarnic pravico zahtevati preklic potrdil o enoti denarnice z uporabo mehanizmov avtentikacije iz točke (b).

Člen 7

Preklic potrdil o enoti denarnice

1. Ponudniki denarnic so edini subjekti, ki lahko prekličejo potrdila o enoti denarnice za enote denarnice, ki so jih zagotovili.

2. Ponudniki denarnic vzpostavijo javno dostopno politiko, v kateri določijo pogoje in časovni okvir za preklic potrdil o enoti denarnice.

3. Kadar ponudniki denarnic prekličejo potrdila o enoti denarnice, zadevne uporabnike denarnice v 24 urah obvestijo o preklicu njihovih enot denarnice, vključno z razlogom za preklic in posledicami za uporabnika denarnice. Te informacije se zagotovijo na jedrnat in zlahka dostopen način ter vsebujejo jasen in preprost jezik.

4. Kadar ponudniki denarnic prekličejo potrdila o enoti denarnice, javno objavijo status veljavnosti potrdila o enoti denarnice na način, ki ohranja zasebnost, in v potrdilu denarnice opišejo lokacijo teh informacij.

POGLAVJE III

TEMELJNE FUNKCIONALNOSTI IN FUNKCIJE EVROPSKIH DENARNIC ZA DIGITALNO IDENTITETO

Člen 8

Oblike identifikacijskih podatkov osebe in elektronskih potrdil o atributih

Ponudniki denarnic zagotovijo, da rešitve denarnic podpirajo uporabo identifikacijskih podatkov osebe in elektronskih potrdil o atributih, izdanih v skladu s seznamom standardov iz Priloge II.

Člen 9

Evidence transakcij

1. Ne glede na to, ali je transakcija uspešno zaključena ali ne, instance denarnice evidentirajo vse transakcije z na denarnice zanašajočimi se strankami in drugimi denarnicami, vključno z elektronskim podpisom in žigom.

2. Evidentirane informacije vsebujejo vsaj:

(a) čas in kraj transakcije;

(b) naziv, kontaktne podatke in edinstveno identifikacijsko oznako ustrezne na denarnice zanašajoče se stranke ter državo članico, v kateri ima sedež, ali v primeru drugih enot denarnice ustrezne informacije iz potrdila o enoti denarnice;

(c) vrsto ali vrste podatkov, ki se zahtevajo in so predstavljeni v transakciji;

(d) v primeru nezaključenih transakcij, razlog za nezaključitev.

3. Ponudniki denarnic zagotovijo celovitost, avtentičnost in zaupnost evidentiranih informacij.

4. Instance denarnice evidentirajo poročila, ki jih uporabnik denarnice pošlje organom za varstvo podatkov prek svoje enote denarnice.

5. Evidence iz odstavkov 1 in 2 so ponudniku denarnice dostopne, kadar je to potrebno za zagotavljanje storitev denarnice, na podlagi izrecnega predhodnega soglasja uporabnika denarnice.

6. Evidence iz odstavkov 1 in 2 ostanejo dostopne, dokler to zahteva pravo Unije ali nacionalno pravo.

7. Ponudniki denarnic uporabnikom denarnic omogočijo izvoz evidentiranih informacij iz odstavka 2.

Člen 10

Vgrajeno razkritje

1. Ponudniki denarnic zagotovijo, da lahko enote denarnice, ki jih zagotavljajo, obdelajo elektronska potrdila o atributih s skupnimi vgrajenimi politikami razkrivanja iz Priloge III.

2. Instance denarnic so sposobne obdelovati in predstaviti take vgrajene politike razkrivanja iz odstavka 1 v povezavi s podatki, prejetimi od na denarnice zanašajoče se stranke, ki jih je zahtevala.

3. Instance denarnic preverijo, ali na denarnice zanašajoča se stranka izpolnjuje zahteve vgrajene politike razkrivanja, in uporabnika denarnice obvestijo o ugotovitvah.

Člen 11

Kvalificirani elektronski podpisi in žigi

1. Ponudniki denarnic zagotovijo, da lahko uporabniki denarnic prejmejo kvalificirana potrdila za kvalificirane elektronske podpise ali žige, ki so povezana z napravami za ustvarjanje kvalificiranega podpisa ali žiga, ki so glede na instance denarnic lahko lokalne, zunanje ali upravljane na daljavo.

2. Ponudniki denarnic zagotovijo, da je mogoče rešitve denarnic varno povezati z eno od naslednjih vrst naprav za ustvarjanje kvalificiranega podpisa ali žiga: lokalna, zunanja ali na daljavo vodena naprava za ustvarjanje kvalificiranega podpisa ali žiga za namene uporabe kvalificiranih potrdil iz odstavka 1.

3. Ponudniki denarnic zagotovijo, da imajo uporabniki denarnic, ki so fizične osebe, vsaj za nepoklicne namene brezplačen dostop do aplikacij za ustvarjanje podpisa, ki omogočajo ustvarjanje brezplačnih kvalificiranih elektronskih podpisov z uporabo potrdil iz odstavka 1.

Člen 12

Aplikacije za ustvarjanje podpisa

1. Aplikacije za ustvarjanje podpisa, ki jih uporabljajo enote denarnice, lahko zagotovijo ponudniki denarnic, ponudniki storitev zaupanja ali na denarnice zanašajoče se stranke.

2. Aplikacije za ustvarjanje podpisa imajo naslednje funkcije:

(a) podpisovanje ali žigosanje podatkov, ki jih zagotovi uporabnik denarnice;

(b) podpisovanje ali žigosanje podatkov, ki jih zagotovi na denarnice zanašajoča se stranka;

(c) ustvarjanje podpisov ali žigov vsaj v obvezni obliki iz Priloge IV;

(d) obveščanje uporabnikov denarnic o rezultatu postopka ustvarjanja podpisa ali žiga.

3. Aplikacije za ustvarjanje podpisa so lahko vgrajene v instance denarnice ali zunanje. Kadar se aplikacije za ustvarjanje podpisa zanašajo na naprave za ustvarjanje kvalificiranega podpisa na daljavo in so vgrajene v instance denarnic, podpirajo vmesnik za aplikacijsko programiranje iz Priloge IV.

Člen 13

Izvoz in prenosljivost podatkov

Kadar je to tehnično izvedljivo in razen v primerih kritičnih sredstev, enote denarnice podpirajo varen izvoz in prenosljivost osebnih podatkov uporabnika denarnice, da se mu omogoči prehod na enoto denarnice druge rešitve denarnice na način, ki zagotavlja visoko raven zanesljivosti, kot je določeno v Izvedbeni uredbi (EU) 2015/1502.

Člen 14

Psevdonimi

1. Denarnice podpirajo ustvarjanje psevdonimov za uporabnike denarnic v skladu s tehničnimi specifikacijami iz Priloge V.

2. Enote denarnice na zahtevo na denarnice zanašajoče se stranke podpirajo ustvarjanje psevdonima, ki je specifičen in edinstven zanjo, ter ji ta psevdonim zagotovijo bodisi samostojno bodisi v kombinaciji s kakršnimi koli identifikacijskimi podatki osebe ali elektronskim potrdilom o atributih, ki ga zahteva ta stranka.

POGLAVJE IV

KONČNE DOLOČBE

Člen 15

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 28. novembra 2024

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA I

SEZNAM STANDARDOV IZ ČLENA 5

— SAM.01 Secured Applications for Mobile – Requirements for supporting 3rd party Applets on eSIM and eSE via SAM (varne aplikacije za mobilne telefone – zahteve za podpiranje programčkov tretjih oseb na karticah eSIM in vgrajenih varnostnih elementih prek v varnih aplikacij za mobilne telefone) v1.1 2023, GSMA;

— GPC_GUI_217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM (standard GlobalPlatform – konfiguracija varnih aplikacij za mobilne telefone – tehnična specifikacija za izvajanje varnih aplikacij za mobilne telefone) v1.0 2024-04;

— GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards (standard GlobalPlatform – specifikacija za kartice – tehnična specifikacija za pametne kartice) v2.3.1 2018-03;

— GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management (standard GlobalPlatform – sprememba A – upravljanje tajne vsebine kartic) v1.2 2019-07;

— GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 (standard GlobalPlatform – sprememba D – protokol za varne kanale 03) v1.2 2020-04;

— GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 (standard GlobalPlatform – sprememba F – protokol za varne kanale 11) v1.4 2024-03;

— GPD_SPE_0 75 GlobalPlatform Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices (standard GlobalPlatform – specifikacija za vmesnik Open Mobile API – vmesnik Open Mobile API za mobilne aplikacije za dostop do varnostnih elementov na uporabniških napravah) v3.3 2018-08.

PRILOGA II

SEZNAM STANDARDOV IZ ČLENA 8

— ISO/IEC.18013-5:2021;

— Podatkovni model za preverljive poverilnice 1.1 (Verifiable Credentials Data Model 1.1) iz priporočila Konzorcija za svetovni splet (W3C) z dne 3. marca 2022.

PRILOGA III

SEZNAM SKUPNIH VGRAJENIH POLITIK RAZKRIVANJA IZ ČLENA 10

1. „Brez politike“ pomeni, da se za elektronska potrdila o atributih ne uporablja nobena politika.
2. „Politika samo pooblaščene zanašajoče se stranke“ pomeni, da lahko uporabniki denarnic razkrijejo elektronska potrdila o atributih samo avtenticiranim zanašajočim se strankam, ki so izrecno navedene v politikah razkrivanja.
3. „Specifičen koren zaupanja“ pomeni, da bi morali uporabniki denarnic specifično elektronsko potrdilo o atributih razkriti samo avtenticiranim na denarnice zanašajočim se strankam s potrdili o dostopu za na denarnice zanašajoče se stranke, ki izhajajo iz specifičnega korena (ali seznama specifičnih korenov) ali vmesnih potrdil.

PRILOGA IV

OBLIKE PODPISA IN ŽIGA IZ ČLENA 12

1. Obvezna oblika podpisa ali žiga:

   PAdES (napredni elektronski podpis PDF), kot je določen v standardu ETSI EN 319 142-1 V1.1.1 (2016-04) „Elektronski podpisi in infrastruktura (ESI) – Digitalni podpisi PAdES – 1. del: Gradniki in izhodiščni podpisi PAdES“.

2. Seznam neobveznih oblik podpisa ali žiga:

   (a) XAdES, kot je določen v standardu ETSI EN 319 132-1 V1.2.1 (2022-02) „Elektronski podpisi in infrastrukture (ESI) – Digitalni podpisi XAdES – 1. del: Gradniki in izhodiščni podpisi XAdES“ za podpisovanje oblike XML;

   (b) JAdES, kot je določen v standardu ETSI TS 119 182-1 V1.2.1 (2024-07) „Elektronski podpisi in infrastrukture (ESI) – Digitalni podpisi JAdES – 1. del: Gradniki in izhodiščni podpisi JAdES“ za podpisovanje oblike JSON;

   (c) CAdES (napredni elektronski podpis CMS), kot je določen v standardu ETSI EN 319 122-1 V1.3.1 (2023-06) „Elektronski podpisi in infrastrukture (ESI) – Digitalni podpisi CAdES – 1. del: Gradniki in izhodiščni podpisi CAdES“ za podpisovanje oblike CMS;

   (d) ASiC (pripadajoči vsebnik podpisov), kot je določen v standardu ETSI EN 319 162-1 V1.1.1 (2016-04) „Elektronski podpisi in infrastrukture (ESI) – Pripadajoči vsebniki podpisov (ASiC) – 1. del: Gradniki in izhodiščni podpisi ASiC“ ter standardu ETSI EN 319 162-2 V1.1.1 (2016-04) „Elektronski podpisi in infrastrukture (ESI) – Pripadajoči vsebniki podpisov (ASiC) – 2. del: Dodatni vsebniki ASiC“ za podpisovanje vsebnikov.

3. Vmesnik za aplikacijsko programiranje:

   — Specifikacija v2.0 Cloud Signature Consortium (konzorcij za podpisovanje v oblaku, CSC) z dne 20. aprila 2023.

PRILOGA V

TEHNIČNE SPECIFIKACIJE ZA USTVARJANJE PSEVDONIMOV IZ ČLENA 14

Tehnične specifikacije:

— Spletna avtentikacija, raven 2 (Web Authentication, Level 2), iz priporočila Konzorcija za svetovni splet (W3C) z dne 8. aprila 2021, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.