Úradný vestník
Európskej únie

SK
Séria L

2024/2981

4.12.2024

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2024/2981

z 28. novembra 2024,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o certifikáciu európskych peňaženiek digitálnej identity

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 5c ods. 6,

keďže:

(1) Podľa článku 5c nariadenia (EÚ) č. 910/2014 sa má certifikácia európskych peňaženiek digitálnej identity (ďalej len „peňaženky“) vykonávať v súlade s požiadavkami na funkčnosť, kybernetickú bezpečnosť a ochranu údajov s cieľom zaistiť vysokú úroveň bezpečnosti a dôveryhodnosti peňaženiek. Tieto požiadavky na certifikáciu je potrebné harmonizovať vo všetkých členských štátoch, aby sa zabránilo fragmentácii trhu a vytvoril sa spoľahlivý rámec.

(2) Na činnosti spracúvania osobných údajov podľa tohto nariadenia sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 ([2]) a v relevantných prípadoch smernica Európskeho parlamentu a Rady 2002/58/ES ([3]).

(3) Komisia pravidelne posudzuje nové technológie, postupy, normy alebo technické špecifikácie. S cieľom zabezpečiť čo najvyššiu úroveň harmonizácie medzi členskými štátmi pri vývoji a certifikácii peňaženiek sa technické špecifikácie stanovené v tomto nariadení opierajú o prácu vykonanú na základe odporúčania Komisie (EÚ) 2021/946 z 3. júna 2021 o spoločnom súbore nástrojov Únie pre koordinovaný prístup k európskemu rámcu digitálnej identity ([4]), a najmä o architektúru a referenčný rámec, ktorý je jeho súčasťou. V súlade s odôvodnením 75 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1183 ([5]) by Komisia mala toto vykonávacie nariadenie podľa potreby preskúmať a aktualizovať, aby bolo v súlade s globálnym vývojom, architektúrou a referenčným rámcom a aby sa na vnútornom trhu dodržiavali najlepšie postupy.

(4) S cieľom osvedčiť súlad s požiadavkami kybernetickej bezpečnosti zahrnutými v certifikačnom rámci by sa certifikácia riešení peňaženky mala odvolávať na európske systémy certifikácie kybernetickej bezpečnosti zriadené podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 ([6]), ak sú k dispozícii a ak sú relevantné. Ak takéto systémy neexistujú alebo ak sa čiastočne vzťahujú na požiadavky kybernetickej bezpečnosti, v tomto nariadení sa stanovujú všeobecné požiadavky vzťahujúce sa na vnútroštátne schémy certifikácie, ktoré zahŕňajú požiadavky na funkčnosť, kybernetickú bezpečnosť a ochranu údajov.

([1]) Ú. v. EÚ L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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).

([3]) 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).

([4]) Ú. v. EÚ L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([5]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity (Ú. v. EÚ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([6]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Podľa článku 5a ods. 11 nariadenia (EÚ) č. 910/2014 majú byť peňaženky certifikované na úrovni zabezpečenia „vysoká“, ako je stanovené v nariadení (EÚ) č. 910/2014, ako aj vo vykonávacom nariadení Komisie (EÚ) 2015/1502 ([7]). Túto úroveň zabezpečenia musí dosiahnuť celkové riešenie peňaženky. Podľa tohto nariadenia môžu byť niektoré komponenty riešenia peňaženky certifikované na nižšej úrovni zabezpečenia, ak je to riadne odôvodnené a bez toho, aby bola dotknutá úroveň zabezpečenia „vysoká“ dosiahnutá celkovým riešením.

(6) Všetky vnútroštátne schémy certifikácie by mali určiť vlastníka schémy, ktorý bude zodpovedný za vývoj a údržbu schémy certifikácie. Vlastníkom schémy môže byť orgán posudzovania zhody, vládny orgán alebo úrad, obchodné združenie, skupina orgánov posudzovania zhody alebo akýkoľvek iný vhodný orgán a môže byť iný ako orgán, ktorý prevádzkuje vnútroštátnu schému certifikácie.

(7) Predmet certifikácie by mal zahŕňať komponenty riešenia peňaženky, ako napr. inštanciu peňaženky. Zabezpečená kryptografická aplikácia peňaženky (ďalej len „WSCA“), zabezpečené kryptografické zariadenie peňaženky (ďalej len „WSCD“) a platformy, na ktorých sa tieto softvérové komponenty vykonávajú, hoci sú súčasťou operačného prostredia, by mali byť zahrnuté do predmetu certifikácie, len ak ich poskytuje riešenie peňaženky. V ostatných prípadoch, a najmä ak tieto zariadenia a platformy poskytujú koncoví používatelia, by poskytovatelia mali stanoviť predpoklady týkajúce sa prevádzkového prostredia riešenia peňaženky vrátane týchto zariadení a platforiem, a zaviesť opatrenia na potvrdenie toho, že tieto predpoklady sa overujú v praxi. S cieľom zabezpečiť ochranu kritických aktív prostredníctvom hardvéru a systémového softvéru používaného na správu a ochranu kryptografických kľúčov vytvorených, uložených alebo spracovaných zariadením WSCD, musí toto zariadenie spĺňať vysoké normy certifikácie, ktoré sa odrážajú v medzinárodných normách, ako napr. spoločné kritériá *Common Criteria* (ďalej len „EUCC“), stanovené vo vykonávacom nariadení Komisie (EÚ) 2024/482 ([8]), hodnotenie EAL4 a pokročilá metodická analýza zraniteľností, napríklad porovnateľná s AVA_VAN.5. Tieto certifikačné normy by sa mali používať najneskôr vtedy, keď sa certifikácia zhody peňaženiek vykonáva podľa európskeho systému certifikácie kybernetickej bezpečnosti prijatého podľa nariadenia (EÚ) 2019/881.

(8) Plne mobilné, bezpečné a používateľsky prívetivé peňaženky využívajú podporu dostupnosti štandardizovaných a certifikovaných riešení odolných voči neoprávnenej manipulácii, ako sú napríklad zabudované zabezpečené prvky, externé zariadenia, ako sú napríklad čipové karty, alebo zabudované platformy SIM v mobilných zariadeniach. Je dôležité zabezpečiť včasný prístup k zabudovaným zabezpečeným prvkom pre vnútroštátne prostriedky elektronickej identifikácie a peňaženky a koordinovať úsilie členských štátov v tejto oblasti. Skupina pre európsku spoluprácu v oblasti digitálnej identity zriadená podľa článku 46e ods. 1 nariadenia (EÚ) č. 910/2014 (ďalej len „skupina pre spoluprácu“) by mala zriadiť podskupinu určenú na tento účel. Táto podskupina by sa mala po konzultácii s príslušnými zainteresovanými stranami dohodnúť na spoločnom pláne prístupu k zabudovaným zabezpečeným prvkom, ktorý má Komisia zvážiť pri správe o preskúmaní nariadenia (EÚ) č. 910/2014. S cieľom uľahčiť zavádzanie peňaženky na vnútroštátnej úrovni by Komisia mala okrem toho v spolupráci s členskými štátmi vypracovať a priebežne aktualizovať príručku pre prípady použitia ako súčasť architektúry a referenčného rámca.

(9) Predmetom certifikácie vnútroštátnych schém certifikácie by mali byť aj procesy, ktoré sa používajú na poskytovanie a prevádzku riešenia peňaženky, a to aj v prípade, že vymedzenie alebo vykonávanie týchto procesov je zadané tretím stranám. Na preukázanie toho, že procesy spĺňajú požiadavky schém, sa ako dôkaz môžu použiť informácie o zabezpečení za predpokladu, že sa na určenie toho, či sú informácie o zabezpečení dostatočné, použije analýza závislosti. Informácie o zabezpečení majú rôzne formy vrátane správ a certifikátov zhody, ktoré môžu byť súkromné, vnútroštátne, európske alebo medzinárodné, založené na normách alebo technických špecifikáciách. Cieľom analýzy závislosti je posúdiť kvalitu dostupných informácií o zabezpečení komponentov peňaženky.

([7]) Vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Ú. v. EÚ L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskeho systému certifikácie kybernetickej bezpečnosti založeného na spoločných kritériách (EUCC) (Ú. v. EÚ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Na základe postupov stanovených na tento účel by skupina pre spoluprácu mala mať možnosť poskytovať stanoviská a odporúčania k návrhom vnútroštátnych schém certifikácie, ktoré jej boli predložené. Tieto vnútroštátne schémy certifikácie by mali byť špecifické pre architektúru peňaženky a pre každú konkrétnu podporovanú architektúru by mali existovať špecifické profily.

(11) S cieľom zabezpečiť spoločné chápanie a harmonizovaný prístup k posudzovaniu najkritickejších rizík, ktoré by mohli ovplyvniť poskytovanie a prevádzku peňaženiek, by sa mal vypracovať register rizík a hrozieb, ktoré by sa mali zohľadniť pri navrhovaní riešení peňaženiek nezávisle od ich konkrétnej architektúry. Pri určovaní rizík, ktoré by sa mali zahrnúť do registra, by sa malo pamätať na ciele kybernetickej bezpečnosti opísané v nariadení (EÚ) č. 910/2014, ako je dôvernosť, integrita a dostupnosť riešenia peňaženky, ako aj ochrana súkromia používateľov a údajov. Náležité zohľadnenie rizík a hrozieb zahrnutých v tomto registri rizík by malo byť súčasťou požiadaviek vnútroštátnych schém certifikácie. S cieľom držať krok s neustále sa vyvíjajúcou panorámou hrozieb by sa mal register rizík viesť a pravidelne aktualizovať v súčinnosti so skupinou pre spoluprácu.

(12) Pri vytváraní schém certifikácie by mali vlastníci schémy vykonať posúdenie rizík s cieľom spresniť riziká a hrozby uvedené v registri a doplniť ich o riziká a hrozby špecifické pre architektúru alebo realizáciu riešenia peňaženky. Pri posúdení rizík by sa malo zvážiť, ako možno príslušné riziká a hrozby vhodne riešiť. Poskytovatelia peňaženky by mali doplniť posúdenie rizík schémy s cieľom identifikovať všetky riziká a hrozby špecifické pre ich realizáciu a navrhnúť vhodné opatrenia na ich riešenie, ktoré certifikačný orgán vyhodnotí.

(13) S cieľom preukázať, že architektúra riešenia peňaženky spĺňa uplatniteľné bezpečnostné požiadavky, by každá schéma alebo profil špecifický pre architektúru mali obsahovať aspoň opis architektúry riešenia peňaženky, zoznam bezpečnostných požiadaviek uplatniteľných na architektúru riešenia peňaženky, plán hodnotenia na potvrdenie, že riešenie peňaženky založené na tejto architektúre spĺňa tieto požiadavky, a posúdenie rizík. Vo vnútroštátnych schémach certifikácie by sa od poskytovateľov peňaženiek malo vyžadovať, aby preukázali, ako návrh riešenia peňaženky, ktoré poskytujú, zodpovedá referenčnej architektúre, a aby podrobne opísali bezpečnostné kontroly a plány validácie konkrétneho riešenia peňaženky. Vnútroštátne schémy certifikácie by mali definovať aj činnosť posudzovania zhody s cieľom overiť, či návrh peňaženky správne odráža referenčnú architektúru vybraného profilu. Vnútroštátne schémy certifikácie by mali spĺňať požiadavky stanovené v článku 51 nariadenia (EÚ) 2019/881 s výnimkou písmen e) a f) uvedeného článku, ktoré sa týkajú logovania.

(14) Pokiaľ ide o certifikáciu produktov, malo by sa umožniť používanie certifikátov zhody vydaných v rámci európskeho systému certifikácie kybernetickej bezpečnosti podľa EUCC a certifikátov zhody vydaných v rámci vnútroštátnych schém certifikácie v kontexte dohody o vzájomnom uznávaní SOG-IS. Okrem toho by sa malo umožniť používanie iných vnútroštátnych schém certifikácie pre menej citlivé komponenty produktov, ako sú napríklad schémy vytvorené podľa normy CEN EN 17640 pre metodiku hodnotenia kybernetickej bezpečnosti s pevne stanoveným časom.

(15) Na jasné, jednoduché a rozpoznateľné označenie toho, že peňaženka bola poskytnutá v súlade s nariadením (EÚ) č. 910/2014, by sa mala používať značka dôvery EÚ pre peňaženku digitálnej identity (ďalej len „značka dôvery“). Mala by sa preto považovať za značku zhody pre riešenie peňaženky certifikované v rámci vnútroštátnych schém certifikácie. Vnútroštátne schémy certifikácie by nemali definovať žiadne iné značky zhody.

(16) S cieľom odradiť od podvodov by vnútroštátne schémy certifikácie mali vymedziť opatrenia, ktoré sa majú prijať v prípade, že sa o certifikáciu v rámci schémy žiada podvodným spôsobom.

(17) Na zabezpečenie účinného riadenia oznámení o zraniteľnostiach by poskytovatelia riešení peňaženky a schéma elektronickej identifikácie, v rámci ktorej sa poskytujú, mali definovať a zaviesť procesy na vyhodnocovanie závažnosti a potenciálneho vplyvu zraniteľností. Vnútroštátne schémy certifikácie by mali stanoviť prahovú hodnotu, po ktorej prekročení treba informovať certifikačný orgán. Takáto požiadavka na oznamovanie by nemala mať vplyv na kritériá stanovené právnymi predpismi o ochrane údajov a orgánmi členských štátov na ochranu údajov pre oznamovanie porušení ochrany osobných údajov. Mohli by sa vytvoriť možné synergie medzi povinným oznamovaním porušenia alebo ohrozenia riešení peňaženky a oznamovaním porušení ochrany osobných údajov podľa nariadenia (EÚ) 2016/679. Posúdením správy o analýze vplyvu na zraniteľnosť, ktoré vykoná certifikačný orgán, by nemalo byť dotknuté vyhodnotenie posúdenia vplyvu na ochranu údajov, ktoré vykoná orgán na ochranu údajov podľa článkov 35 a 36 nariadenia (EÚ) 2016/679.

(18) Poskytovatelia riešení peňaženky a schéma elektronickej identifikácie, v rámci ktorej sa poskytujú, by mali vlastníkovi schémy oznámiť všetky zdôvodnenia výnimiek z posúdenia zraniteľnosti, ktoré sa vyžadujú na vyhodnotenie zariadenia WSCD a aplikácie WSCA, ako sa uvádza v prílohe IV.

(19) Zrušenie certifikátu zhody by mohlo mať závažné dôsledky, napríklad zrušenie všetkých nasadených jednotiek peňaženky. Certifikačné orgány by preto mali zvážiť zrušenie len vtedy, ak neodstránená zraniteľnosť môže významne ovplyvniť spoľahlivosť riešenia peňaženky alebo spoľahlivosť iného riešenia peňaženky.

(20) Mal by sa zaviesť osobitný proces aktualizácie vnútroštátnych schém certifikácie, aby sa zvládol prechod medzi jednotlivými vydaniami schém, najmä pokiaľ ide o opatrenia, ktoré má držiteľ certifikátu prijať v súvislosti s nadchádzajúcimi hodnoteniami, údržbou, opätovnou certifikáciou a osobitnými hodnoteniami.

(21) S cieľom uľahčiť transparentnosť by si poskytovatelia peňaženky mali verejne vymieňať bezpečnostné informácie o svojich riešeniach peňaženky.

(22) Ak sa vnútroštátne schémy certifikácie spoliehajú na informácie o zabezpečení z iných schém alebo zdrojov certifikácie, mala by sa vykonať analýza závislosti s cieľom overiť, či je dokumentácia o zabezpečení, napríklad správy o zabezpečení a certifikáty zhody, dostupná a primeraná pre riešenia peňaženky a schému elektronickej identifikácie, v rámci ktorej sa poskytuje. Základom tejto analýzy závislosti by malo byť posúdenie rizika riešení peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje. Hodnotenie by malo určiť, či dokumentácia o zabezpečení, ktorá je k dispozícii pre dané riešenie peňaženky, a schéma elektronickej identifikácie, v rámci ktorej sa poskytuje, je primeraná na poskytnutie zabezpečenia zodpovedajúceho cieľovej úrovni hodnotenia. Hodnotenie by malo tiež aktualizovať analýzu závislosti alebo ju v prípade potreby úplne prehodnotiť.

(23) Certifikačné orgány by mali vydávať certifikáty zhody vo vnútroštátnych schémach certifikácie spolu s verejne dostupnou certifikačnou správou, ako sa uvádza v článku 5d ods. 2 písm. a) nariadenia (EÚ) č. 910/2014. Súvisiaca správa o posúdení certifikácie by mala byť k dispozícii skupine pre spoluprácu.

(24) Vnútroštátne schémy certifikácie by mali stanoviť ročné hodnotenie dohľadu s cieľom zabezpečiť, aby procesy súvisiace so správou a údržbou peňaženiek fungovali účinne, tzn. aby fungovali tak, ako je vymedzené v politikách určujúcich procesy. Dvojročné posúdenie zraniteľnosti je požiadavka vyplývajúca z nariadenia (EÚ) č. 910/2014 s cieľom zabezpečiť, aby riešenie peňaženky naďalej primerane pokrývalo riziká a hrozby kybernetickej bezpečnosti identifikované v registri rizík vrátane akéhokoľvek vývoja panorámy hrozieb. Pojmy hodnotenia dohľadu, hodnotenia na účely opätovnej certifikácie a osobitné hodnotenia by mali byť v súlade s normou EN ISO/IEC 17021-1:2015.

(25) Cyklus certifikácie sa končí uplynutím platnosti certifikátu zhody alebo vydaním nového certifikátu zhody po úspešnom hodnotení na účely opätovnej certifikácie. Hodnotenie na účely opätovnej certifikácie by malo zahŕňať hodnotenie všetkých komponentov predmetu certifikácie vrátane hodnotenia účinnosti a prípadne posúdenia zraniteľnosti. Počas opätovnej certifikácie by malo byť možné opätovne použiť výsledky predchádzajúcich hodnotení komponentov, ktoré sa nezmenili.

(26) Po prijatí európskeho systému certifikácie kybernetickej bezpečnosti by vnútroštátne schémy certifikácie s rovnakým rozsahom pôsobnosti mali prestať vydávať certifikáty po uplynutí vymedzeného prechodného obdobia, ako sa uvádza v článku 57 ods. 1 nariadenia (EÚ) 2019/881.

(27) Vnútroštátne schémy certifikácie by sa mali opierať o existujúce rámce a podľa potreby opätovne používať dôkazy s cieľom zabezpečiť harmonizáciu a interoperabilitu. Členské štáty môžu uzatvárať dohody o cezhraničnom opakovanom použití schém certifikácie alebo ich častí. Európska komisia a agentúra ENISA by mali v spolupráci so skupinou pre spoluprácu podporovať členské štáty pri vývoji a udržiavaní ich vnútroštátnych schém certifikácie, čím sa zabezpečí výmena poznatkov a najlepších postupov.

(28) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([9]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 30. septembra 2024 svoje stanovisko.

(29) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru uvedeného v článku 48 ods. 1 nariadenia (EÚ) č. 910/2014,

PRIJALA TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy a rozsah pôsobnosti

V tomto nariadení sa stanovujú referenčné normy a zavádzajú špecifikácie a postupy na vytvorenie spoľahlivého rámca na certifikáciu peňaženiek, ktoré sa majú pravidelne aktualizovať, aby boli v súlade s vývojom technológií a noriem a s prácou vykonávanou na základe odporúčania (EÚ) 2021/946 o spoločnom súbore nástrojov Únie pre koordinovaný prístup k európskemu rámcu digitálnej identity, a najmä s architektúrou a referenčným rámcom.

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „riešenie peňaženky“ je kombinácia softvéru, hardvéru, služieb, nastavení a konfigurácií vrátane inštancií peňaženky, jednej alebo viacerých zabezpečených kryptografických aplikácií peňaženky a jedného alebo viacerých zabezpečených kryptografických zariadení peňaženky;

2. „vlastník schémy“ je organizácia, ktorá je zodpovedná za vývoj a údržbu schémy certifikácie;

3. „predmet certifikácie“ sú produkty, procesy a služby alebo ich kombinácia, na ktoré sa vzťahujú stanovené požiadavky;

4. „zabezpečená kryptografická aplikácia peňaženky“ je aplikácia, ktorá spravuje kritické aktíva tak, že je prepojená s kryptografickými a nekryptografickými funkciami poskytovanými zabezpečeným kryptografickým zariadením peňaženky a tieto funkcie využíva;

5. „inštancia peňaženky“ je aplikácia nainštalovaná a nakonfigurovaná v zariadení alebo prostredí používateľa peňaženky, ktorá je súčasťou jednotky peňaženky a ktorú používateľ peňaženky používa na interakciu s jednotkou peňaženky;

([9]) 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).

6. „zabezpečené kryptografické zariadenie peňaženky“ je zariadenie odolné voči neoprávnenej manipulácii, poskytujúce prostredie, ktoré je prepojené so zabezpečenou kryptografickou aplikáciou peňaženky a ktoré zabezpečená kryptografická aplikácia peňaženky využíva na ochranu kritických aktív a poskytovanie kryptografických funkcií na účely bezpečného vykonávania kritických operácií;

7. „register rizík“ je záznam informácií relevantných pre proces certifikácie o identifikovaných rizikách;

8. „poskytovateľ peňaženky“ je fyzická alebo právnická osoba, ktorá poskytuje riešenia peňaženky;

9. „certifikačný orgán“ je orgán posudzovania zhody tretej strany, ktorý prevádzkuje schémy certifikácie;

10. „jednotka peňaženky“ je jedinečná konfigurácia riešenia peňaženky, ktorá zahŕňa inštancie peňaženky, zabezpečené kryptografické aplikácie peňaženky a zabezpečené kryptografické zariadenia peňaženky, ktoré poskytovateľ peňaženky poskytuje jednotlivým používateľom peňaženky;

11. „kritické aktíva“ sú aktíva v rámci jednotky peňaženky alebo v súvislosti s ňou, ktoré majú taký mimoriadny význam, že narušenie ich dostupnosti, dôvernosti alebo integrity by malo veľmi vážny, oslabujúci účinok na schopnosť spoliehať sa na jednotku peňaženky;

12. „používateľ peňaženky“ je používateľ, ktorý má kontrolu nad jednotkou peňaženky;

13. „incident“ je incident vymedzený v článku 6 bode 6 smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 ([10]);

14. „zahrnuté pravidlá sprístupňovania informácií“ sú súbor pravidiel zakotvených v elektronickom osvedčení atribútov jeho poskytovateľom, v ktorom sa uvádzajú podmienky, ktoré musí strana spoliehajúca sa na peňaženku splniť, aby mala prístup k elektronickému osvedčeniu atribútov.

KAPITOLA II

VNÚTROŠTÁTNE SCHÉMY CERTIFIKÁCIE

Článok 3

Zavedenie vnútroštátnych schém certifikácie

1. Členské štáty určia vlastníka schémy pre každú vnútroštátnu schému certifikácie.

2. Predmetom certifikácie vymedzenej vo vnútroštátnych schémach certifikácie je poskytovanie a prevádzka riešení peňaženky a schém elektronickej identifikácie, v rámci ktorých sa poskytujú.

3. V súlade s vykonávacím nariadením (EÚ) 2015/1502 zahŕňa predmet certifikácie vo vnútroštátnych schémach certifikácie tieto prvky:

a) softvérové komponenty vrátane nastavení a konfigurácií riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa riešenia peňaženky poskytujú;

b) hardvérové komponenty a platformy, na ktorých bežia softvérové komponenty uvedené v bode b) y a schémou elektronickej identifikácie, v rámci ktorej sa poskytuje, a keď sú potrebné na splnenie požadovanej úrovne zabezpečenia pre tieto softvérové komponenty. Ak hardvérové komponenty a platformy neposkytuje poskytovateľ peňaženky, vnútroštátne schémy certifikácie formulujú predpoklady hodnotenia hardvérových komponentov a platforiem, na základe ktorých možno zabezpečiť odolnosť voči útočníkom s vysokým potenciálom útoku v súlade s vykonávacím nariadením (EÚ) 2015/1502, a špecifikujú hodnotiace činnosti na potvrdenie týchto predpokladov, ako sa uvádza v prílohe IV;

([10]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) procesy, ktoré podporujú poskytovanie a prevádzku riešenia peňaženky vrátane procesu pridávania používateľa, ako je uvedené v článku 5a nariadenia (EÚ) č. 910/2014, zahŕňajúce aspoň registráciu, správu elektronických prostriedkov a organizáciu podľa oddielov 2.1, 2.2 a 2.4 prílohy I k vykonávaciemu nariadeniu (EÚ) 2015/1502.

4. Vnútroštátne schémy certifikácie obsahujú opis konkrétnej architektúry riešení peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje. Ak sa vnútroštátne schémy certifikácie vzťahujú na viac ako jednu konkrétnu architektúru, musia obsahovať profil pre každú konkrétnu architektúru.

5. Pre každý profil musia vnútroštátne schémy certifikácie stanoviť aspoň tieto údaje:

a) osobitnú architektúru riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytujú;

b) bezpečnostné kontroly spojené s úrovňami zabezpečenia stanovenými v článku 8 nariadenia (EÚ) č. 910/2014;

c) plán hodnotenia vypracovaný v súlade s oddielom 7.4.1 normy EN ISO/IEC 17065:2012;

d) bezpečnostné požiadavky potrebné na riešenie rizík a hrozieb kybernetickej bezpečnosti uvedených v registri rizík stanovenom v prílohe I k tomuto nariadeniu až do požadovanej úrovne zabezpečenia a na prípadné splnenie cieľov vymedzených v článku 51 nariadenia (EÚ) 2019/881;

e) mapovanie kontrol uvedených v písmene b) tohto odseku na komponenty architektúry;

f) opis toho, ako bezpečnostné kontroly, mapovanie, bezpečnostné požiadavky a plán hodnotenia uvedené v písmenách b) až c) umožňujú poskytovateľom riešení peňaženky a schéme elektronickej identifikácie, v rámci ktorej sa poskytujú, primerane riešiť riziká a hrozby kybernetickej bezpečnosti identifikované v registri rizík uvedenom v písmene d) až do požadovanej úrovne zabezpečenia na základe posúdenia rizík s cieľom spresniť riziká a hrozby uvedené v registri rizík a doplniť ich o riziká a hrozby špecifické pre architektúru.

6. Plán hodnotenia uvedený v odseku5 písm. c) obsahuje zoznam hodnotiacich činností, ktoré sa majú zahrnúť do hodnotenia riešení peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytujú.

7. Na základe hodnotiacej činnosti uvedenej v odseku 6 sa vyžaduje, aby poskytovatelia riešení peňaženky a schéma elektronickej identifikácie, v rámci ktorej sa poskytujú, poskytovali informácie spĺňajúce požiadavky uvedené v prílohe II.

Článok 4

Všeobecné požiadavky

1. Vnútroštátne schémy certifikácie zahŕňajú požiadavky na funkčnosť, kybernetickú bezpečnosť a ochranu údajov pomocou týchto schém certifikácie, ak sú dostupné a uplatniteľné:

a) európske systémy certifikácie kybernetickej bezpečnosti zriadené podľa nariadenia (EÚ) 2019/881 vrátane EUCC;

b) vnútroštátne schémy certifikácie kybernetickej bezpečnosti, na ktoré sa vzťahuje EUCC, v súlade s článkom 49 vykonávacieho nariadenia (EÚ) 2024/482.

2. Vnútroštátne schémy certifikácie môžu okrem toho odkazovať na (ak sú dostupné a uplatniteľné):

a) iné príslušné vnútroštátne schémy certifikácie;

b) medzinárodné, európske a vnútroštátne normy;

c) technické špecifikácie, ktoré spĺňajú požiadavky stanovené v prílohe II k nariadeniu Európskeho parlamentu a Rady (EÚ) č. 1025/2012 ([11]).

3. Vnútroštátne schémy certifikácie:

a) špecifikujú prvky uvedené v časti 6.5 normy EN ISO/IEC 17067:2013;

b) sa zavádzajú ako schéma typu 6 v súlade s oddielom 5.3.8 normy EN ISO/IEC 17067:2013.

4. Vnútroštátne schémy certifikácie musia spĺňať tieto požiadavky:

a) iba poskytovatelia uvedení v článku 5a ods. 2 nariadenia (EÚ) č. 910/2014 majú nárok na vydanie certifikátov podľa vnútroštátnych schém certifikácie;

b) ako značka zhody sa používa iba značka dôvery;

c) poskytovatelia riešení peňaženky a schéma elektronickej identifikácie, v rámci ktorej sa poskytujú, zahŕňajú pri odkazoch na schému odkazy na nariadenie (EÚ) č. 910/2014 a toto nariadenie;

d) poskytovatelia riešení peňaženky a schéma elektronickej identifikácie, v rámci ktorej sa poskytujú, dopĺňajú posúdenie rizík schémy uvedené v článku 3 ods. 5 písm. f) s cieľom identifikovať riziká a hrozby špecifické pre ich realizáciu a navrhnúť vhodné opatrenia na riešenie všetkých relevantných rizík a hrozieb;

e) sú stanovené povinnosti a právne kroky a obsahujú odkazy na príslušné vnútroštátne právne predpisy, v ktorých sa vymedzujú zodpovednosti a možné právne kroky v prípade podvodného využívania certifikácie v rámci schémy.

5. Posúdenie uvedené v odseku 4 písm. d) sa poskytne certifikačnému orgánu na vyhodnotenie.

Článok 5

Riadenie incidentov a zraniteľností

1. Vnútroštátne schémy certifikácie obsahujú požiadavky na riadenie incidentov a zraniteľností v súlade s odsekmi 2 až 9.

2. Držiteľ certifikátu zhody riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, bez zbytočného odkladu oznámi svojmu certifikačnému orgánu porušenie alebo ohrozenie riešenia peňaženky alebo schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, ktoré by mohlo mať vplyv na jeho súlad s požiadavkami vnútroštátnych schém certifikácie.

3. Držiteľ certifikátu zhody musí zaviesť, udržiavať a uplatňovať politiku a postupy riadenia zraniteľnosti, pričom zohľadňuje postupy stanovené v existujúcich európskych a medzinárodných normách vrátane normy EN ISO/IEC 30111:2019.

4. Držiteľ certifikátu zhody informuje vydávajúci certifikačný orgán o zraniteľnostiach a zmenách, ktoré majú vplyv na riešenie peňaženky, na základe definovaných kritérií týkajúcich sa vplyvu týchto zraniteľností a zmien.

5. Držiteľ certifikátu zhody vypracuje správu o analýze vplyvu na zraniteľnosť pre každú zraniteľnosť, ktorá ovplyvňuje softvérové komponenty riešenia peňaženky. Správa obsahuje tieto informácie:

a) vplyv zraniteľnosti na certifikované riešenie peňaženky;

b) možné riziká spojené s blízkosťou alebo pravdepodobnosťou útoku;

([11]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES a ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) či je možné zraniteľnosť odstrániť dostupnými prostriedkami;

d) v prípade, že zraniteľnosť možno odstrániť dostupnými prostriedkami, možné spôsoby odstránenia zraniteľnosti.

6. Ak sa v odseku 4 vyžaduje oznámenie, držiteľ certifikátu zhody bez zbytočného odkladu zašle certifikačnému orgánu správu o analýze vplyvu na zraniteľnosť uvedenú v odseku 5.

7. Držiteľ certifikátu zhody musí zaviesť, udržiavať a uplatňovať politiku riadenia zraniteľností spĺňajúcu požiadavky stanovené v prílohe I k aktu o kybernetickej odolnosti ([12]).

8. Vo vnútroštátnych schémach certifikácie sa stanovia požiadavky na zverejňovanie zraniteľností, ktoré sa vzťahujú na certifikačné orgány.

9. Držiteľ certifikátu zhody zverejní a zaregistruje všetky verejne známe a odstránené zraniteľnosti v riešení peňaženky alebo v jednom z online úložísk uvedených v prílohe V.

Článok 6

Údržba vnútroštátnych schém certifikácie

1. Vnútroštátne schémy certifikácie obsahujú proces pravidelného preskúmania ich fungovania. Cieľom tohto procesu je potvrdiť ich primeranosť a identifikovať aspekty, ktoré si vyžadujú zlepšenie, pričom sa zohľadní spätná väzba od zainteresovaných strán.

2. Vnútroštátne schémy certifikácie obsahujú ustanovenia týkajúce sa ich údržby. Tento proces zahŕňa aspoň tieto požiadavky:

a) pravidlá riadenia definície a požiadaviek vnútroštátnych schém certifikácie;

b) stanovenie časových harmonogramov vydávania certifikátov po prijatí aktualizovaných verzií vnútroštátnych schém certifikácie, a to pre nové certifikáty zhody, ako aj pre už vydané certifikáty;

c) pravidelné preskúmanie vnútroštátnych schém certifikácie s cieľom zabezpečiť, aby sa požiadavky vnútroštátnych schém certifikácie uplatňovali konzistentným spôsobom, pričom sa zohľadnia aspoň tieto aspekty:

— žiadosti o vysvetlenie adresované vlastníkovi schémy v súvislosti s požiadavkami vnútroštátnych schém certifikácie,

— spätná väzba od zainteresovaných strán a iných zainteresovaných subjektov,

— schopnosť vlastníka vnútroštátnej schémy certifikácie reagovať na žiadosti o informácie;

d) pravidlá monitorovania referenčných dokumentov a postupy vývoja referenčných verzií vnútroštátnych schém certifikácie vrátane aspoň prechodných období;

e) proces na zabezpečenie pokrytia najnovších rizík a hrozieb kybernetickej bezpečnosti uvedených v registri rizík stanovenom v prílohe I k tomuto nariadeniu;

f) proces riadenia ďalších zmien vo vnútroštátnych schémach certifikácie.

([12]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Ú. v. EÚ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Vnútroštátne schémy certifikácie obsahujú požiadavky na vykonávanie hodnotení aktuálne certifikovaných produktov v určitom období po revízii schémy alebo po vydaní nových špecifikácií alebo noriem, alebo ich nových verzií, ktoré musia byť v súlade s riešeniami peňaženky a so schémou elektronickej identifikácie, v rámci ktorej sa poskytujú.

KAPITOLA III

POŽIADAVKY TÝKAJÚCE SA VLASTNÍKOV SCHÉMY

Článok 7

Všeobecné požiadavky

1. Vlastníci schémy vyvíjajú a udržiavajú vnútroštátne schémy certifikácie a riadia ich operácie.

2. Vlastníci schémy môžu všetky svoje úlohy alebo ich časť subdodávateľsky zadať tretej strane. Pri uzatváraní subdodávateľských zmlúv so súkromnou stranou vlastníci schémy zmluvne stanovia úlohy a povinnosti všetkých strán. Vlastníci schémy sú naďalej zodpovední za všetky subdodávateľsky zadané činnosti vykonávané ich subdodávateľmi.

3. Vlastníci schémy vykonávajú svoje monitorovacie činnosti, ak je to vhodné, aspoň na základe týchto informácií:

a) informácie od certifikačných orgánov, vnútroštátnych akreditačných orgánov a príslušných orgánov dohľadu nad trhom;

b) informácie vyplývajúce z vlastných auditov a vyšetrovaní alebo auditov a vyšetrovaní iného orgánu;

c) sťažnosti a odvolania prijaté podľa článku 15.

4. Vlastníci schémy informujú skupinu pre spoluprácu o revíziách vnútroštátnych schém certifikácie. Toto oznámenie poskytne skupine pre spoluprácu primerané informácie, aby mohla vydávať odporúčania vlastníkom schémy a stanoviská k aktualizovaným vnútroštátnym schémam certifikácie.

KAPITOLA IV

POŽIADAVKY TÝKAJÚCE SA POSKYTOVATEĽOV RIEŠENÍ PEŇAŽENKY A SCHÉMY ELEKTRONICKEJ IDENTIFIKÁCIE, V RÁMCI KTOREJ SA POSKYTUJÚ

Článok 8

Všeobecné požiadavky

1. Vnútroštátne schémy certifikácie obsahujú požiadavky na kybernetickú bezpečnosť založené na posúdení rizík každej konkrétnej podporovanej architektúry. Cieľom týchto požiadaviek na kybernetickú bezpečnosť je riešiť identifikované riziká a hrozby kybernetickej bezpečnosti, ako sa uvádza v registri rizík v prílohe I.

2. V súlade s článkom 5a ods. 23 nariadenia (EÚ) č. 910/2014 sa vo vnútroštátnych schémach certifikácie vyžaduje, aby riešenia peňaženiek a schémy elektronickej identifikácie, v rámci ktorých sa poskytujú, boli odolné voči útočníkom s vysokým potenciálom útoku pre úroveň zabezpečenia „vysoká“, ako sa uvádza vo vykonávacom nariadení (EÚ) 2015/1502.

3. Vo vnútroštátnych schémach certifikácie sa stanovia bezpečnostné kritériá, ktoré zahŕňajú tieto požiadavky:

a) v relevantných prípadoch akt o kybernetickej odolnosti alebo požiadavky spĺňajúce bezpečnostné ciele stanovené v článku 51 nariadenia (EÚ) 2019/881;

b) zavedenie a vykonávanie politík a postupov týkajúcich sa riadenia rizík spojených s prevádzkou riešenia peňaženky vrátane identifikácie a hodnotenia rizík a zmierňovania identifikovaných rizík;

c) zavedenie a vykonávanie politík a postupov týkajúcich sa riadenia zmien a riadenia zraniteľností v súlade s článkom 5 tohto nariadenia;

d) zavedenie a vykonávanie politík a postupov riadenia ľudských zdrojov vrátane požiadaviek na odbornosť, spoľahlivosť, skúsenosti, odbornú prípravu v oblasti bezpečnosti a kvalifikáciu pracovníkov zapojených do vývoja alebo prevádzky riešenia peňaženky;

e) požiadavky týkajúce sa prevádzkového prostredia riešenia peňaženky, a to aj vo forme predpokladov týkajúcich sa bezpečnosti zariadení a platforiem, na ktorých sú prevádzkované softvérové komponenty riešenia peňaženky, vrátane zariadenia WSCD, a v prípade potreby a relevantnosti požiadavky na posudzovanie zhody s cieľom potvrdiť, že tieto predpoklady sú overené na príslušných zariadeniach a platformách;

f) pre každý predpoklad, ktorý nie je podložený certifikátom zhody alebo inými prijateľnými informáciami o zabezpečení, opis mechanizmu, ktorý poskytovateľ peňaženky používa na vynútenie tohto predpokladu, ako aj odôvodnenie, že tento mechanizmus je dostatočný na zabezpečenie overenia tohto predpokladu;

g) zavedenie a vykonávanie opatrení na zabezpečenie používania aktuálne certifikovanej verzie riešenia peňaženky.

4. Vnútroštátne schémy certifikácie obsahujú funkčné požiadavky týkajúce sa mechanizmov aktualizácie pre každý softvérový komponent riešení peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytujú, v prípade operácií uvedených v prílohe III.

5. Vo vnútroštátnych schémach certifikácie sa vyžaduje, aby žiadateľ o certifikáciu poskytol alebo inak sprístupnil certifikačnému orgánu tieto informácie a dokumentáciu:

a) dôkazy týkajúce sa informácií uvedených v prílohe IV bode 1, v prípade potreby vrátane podrobností o riešení peňaženky a jej zdrojovom kóde vrátane:

— *informácií o architektúre:* pre každý komponent riešenia peňaženky (vrátane komponentov produktu, procesu a služby) opis jeho základných bezpečnostných vlastností vrátane jeho vonkajších závislostí,

— *úrovní kontroly a zabezpečenia:* pre každú bezpečnostnú kontrolu riešenia peňaženky opis kontroly a požadovanú úroveň zabezpečenia na základe prílohy k vykonávaciemu nariadeniu (EÚ) 2015/1502, v ktorej sa stanovuje viacero technických špecifikácií a postupov, ktoré sa vzťahujú na rôzne kontroly vykonávané prostriedkami elektronickej identifikácie,

— *mapovania kontrol na komponenty architektúry:* opis toho, ako sú kontroly peňaženky realizované pomocou rôznych komponentov riešenia peňaženky, na základe zdôvodnenia, prečo sa vyžaduje daná úroveň zabezpečenia a ako je realizovaná kontrola so všetkými požadovanými bezpečnostnými aspektmi na príslušnej úrovni,

— *odôvodnenia a opodstatnenia pokrytia rizika:* opodstatnenie:

— mapovania kontrol na komponenty,

— vhodnosti navrhovaného plánu hodnotenia na primerané pokrytie všetkých kontrol,

— pokrytia poskytovaného kontrolami rizík a hrozieb kybernetickej bezpečnosti identifikovaných v registri rizík, ktoré sú doplnené kontrolami rizík a hrozieb špecifických pre realizáciu, a to na primeranej úrovni zabezpečenia;

b) informácie uvedené v prílohe V;

c) úplný zoznam certifikátov zhody a iných informácií o zabezpečení použitých ako dôkaz počas hodnotiacich činností;

d) všetky ostatné informácie dôležité pre hodnotiace činnosti.

KAPITOLA V

POŽIADAVKY TÝKAJÚCE SA CERTIFIKAČNÝCH ORGÁNOV

Článok 9

Všeobecné požiadavky

1. Certifikačné orgány sú akreditované vnútroštátnymi akreditačnými orgánmi vymenovanými podľa nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 ([13]) v súlade s normou EN ISO/IEC 17065:2012 za predpokladu, že spĺňajú požiadavky stanovené vo vnútroštátnych schémach certifikácie v súlade s odsekom 2.

2. Na účely akreditácie musia certifikačné orgány spĺňať všetky tieto požiadavky na spôsobilosť:

a) podrobná a technická znalosť príslušných architektúr riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, ako aj hrozieb a rizík súvisiacich s týmito architektúrami;

b) znalosť dostupných bezpečnostných riešení a ich vlastností podľa prílohy k vykonávaciemu nariadeniu (EÚ) 2015/1502;

c) znalosť činností vykonávaných na základe certifikátov zhody uplatňovaných na komponenty riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, ako predmetu certifikácie;

d) podrobná znalosť uplatniteľnej vnútroštátnej schémy certifikácie zriadenej v súlade s kapitolou II.

3. Certifikačné orgány vykonávajú svoje činnosti dohľadu najmä na základe týchto informácií:

a) informácie od vnútroštátnych akreditačných orgánov a príslušných orgánov dohľadu nad trhom;

b) informácie vyplývajúce z vlastných auditov a vyšetrovaní alebo auditov a vyšetrovaní iného orgánu;

c) sťažnosti a odvolania prijaté podľa článku 15.

Článok 10

Využívanie subdodávateľov

Certifikačné orgány môžu vykonávanie hodnotiacich činností, ako sú stanovené v článku 13, subdodávateľsky zadať tretím stranám. Ak sú hodnotiace činnosti zadané subdodávateľom, vo vnútroštátnych schémach certifikácie sa stanoví:

1. že všetci subdodávatelia certifikačného orgánu vykonávajúci hodnotiace činnosti musia, ak je to uplatniteľné a vhodné pre vykonávané činnosti, spĺňať požiadavky harmonizovaných noriem, ako sú EN ISO/IEC 17025:2017 pre skúšanie, EN ISO/IEC 17020:2012 pre inšpekciu, EN ISO/IEC 17021-1:2015 pre audit a EN ISO/IEC 17029:2019 pre validáciu a overovanie;

2. že certifikačné orgány musia prevziať zodpovednosť za všetky hodnotiace činnosti subdodávateľsky zadané iným orgánom a preukázať, že počas svojej akreditácie prijali primerané opatrenia, a to aj tým, že sa v prípade potreby opierajú o akreditáciu svojich subdodávateľov;

3. miera, v akej je nutné získať predchádzajúci súhlas s využitím subdodávateľov od vlastníkov schémy alebo klienta, ktorého riešenie peňaženky sa certifikuje v rámci schémy certifikácie.

([13]) Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Článok 11

Oznámenie dozornému orgánu

Certifikačné orgány oznamujú dozornému orgánu uvedenému v článku 46a ods. 1 nariadenia (EÚ) č. 910/2014 vydanie, pozastavenie platnosti a zrušenie certifikátov zhody riešení peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytujú.

Článok 12

Riadenie incidentov a zraniteľností

1. Certifikačné orgány bez zbytočného odkladu pozastavia platnosť certifikátu zhody riešení peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytujú, po tom, ako potvrdia, že oznámené porušenie alebo ohrozenie bezpečnosti má vplyv na súlad riešenia peňaženky alebo schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, s požiadavkami vnútroštátnych schém certifikácie.

2. Certifikačné orgány zrušia certifikát zhody, ktorého platnosť bola pozastavená v dôsledku porušenia alebo ohrozenia bezpečnosti, ktorému sa včas nezabránilo.

3. Certifikačné orgány zrušia certifikáty zhody, ak zistená zraniteľnosť nebola včas odstránená primerane jej závažnosti a potenciálnemu vplyvu v súlade s článkom 5c ods. 4 a článkom 5e ods. 2 nariadenia (EÚ) č. 910/2014.

KAPITOLA VI

POSTUPY PRI POSUDZOVANÍ ZHODY

Článok 13

Hodnotiace činnosti

1. Vnútroštátne schémy certifikácie obsahujú metódy a postupy, ktoré majú orgány posudzovania zhody používať pri vykonávaní svojich hodnotiacich činností v súlade s normou EN ISO/IEC 17065:2012 a ktoré sa vzťahujú aspoň na tieto aspekty:

a) metódy a postupy na vykonávanie hodnotiacich činností vrátane tých, ktoré sa týkajú zariadenia WSCD, ako sa uvádza v prílohe IV;

b) audit realizácie riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, na základe registra rizík stanoveného v prílohe I a v prípade potreby doplneného o riziká špecifické pre realizáciu;

c) činnosti funkčného testovania založené na skúšobných zostavách, ktoré sú vymedzené podľa technických špecifikácií alebo noriem, ak sú dostupné a vhodné;

d) posúdenie existencie a vhodnosti procesov údržby vrátane aspoň riadenia verzií, riadenia aktualizácií a riadenia zraniteľnosti;

e) posúdenie prevádzkovej účinnosti procesov údržby vrátane aspoň riadenia verzií, riadenia aktualizácií a riadenia zraniteľnosti;

f) analýza závislostí poskytnutá poskytovateľom peňaženky vrátane metodiky na posúdenie prijateľnosti informácií o zabezpečení, ktorá zahŕňa prvky uvedené v prílohe VI;

g) posúdenie zraniteľnosti na primeranej úrovni vrátane:

— preskúmania návrhu riešenia peňaženky a prípadne jej zdrojového kódu;

— testovanie odolnosti riešenia peňaženky voči útočníkom s vysokým potenciálom útoku pre úroveň zabezpečenia „vysoká“ podľa oddielu 2.2.1 prílohy k vykonávaciemu nariadeniu (EÚ) 2015/1502;

h) posúdenie vývoja prostredia hrozieb a jeho vplyvu na pokrytie rizík riešením peňaženky s cieľom určiť, ktoré hodnotiace činnosti sú potrebné pre rôzne komponenty riešenia peňaženky.

2. Vnútroštátne schémy certifikácie obsahujú hodnotenie s cieľom určiť, či realizácia riešení peňaženky a schéma elektronickej identifikácie, v rámci ktorej sa tieto riešenia peňaženky poskytujú, zodpovedajú architektúre stanovenej v článku 3 ods. 5 písm. a), ako aj hodnotenie s cieľom určiť, či plán hodnotenia navrhnutý spolu s realizáciou zodpovedá plánu hodnotenia uvedenému v článku 3 ods. 5 písm. c).

3. Vo vnútroštátnych schémach certifikácie sa stanovia pravidlá výberu vzorky, aby sa predišlo opakovaniu rovnakých hodnotiacich činností a aby sa zaistilo zameranie na činnosti, ktoré sú špecifické pre daný variant. Tieto pravidlá výberu vzorky umožňujú, aby sa funkčné a bezpečnostné testy vykonávali len na vzorke variantov cieľového komponentu riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, a na vzorke cieľových zariadení. V rámci vnútroštátnych schém certifikácie sa od všetkých certifikačných orgánov vyžaduje, aby používanie výberu vzorky zdôvodnili.

4. V rámci vnútroštátnych schém certifikácie sa vyžaduje, aby certifikačný orgán vyhodnotil aplikáciu WSCA na základe metód a postupov stanovených v prílohe IV.

Článok 14

Certifikačné činnosti

1. Vo vnútroštátnych schémach certifikácie sa stanoví činnosť osvedčovania na účely vydania certifikátu zhody v súlade s oddielom V písm. a) normy EN ISO/IEC 17067:2013, tabuľka 1, vrátane týchto aspektov:

a) obsah certifikátu zhody, ako sa uvádza v prílohe VII;

b) spôsob, akým sa majú výsledky hodnotenia uviesť vo verejnej certifikačnej správe, vrátane aspoň zhrnutia predbežného plánu auditu a validácie, ako sa uvádza v prílohe VIII;

c) obsah výsledkov hodnotenia uvedených v správe o posúdení certifikácie vrátane prvkov stanovených v prílohe VIII.

2. Správa o posúdení certifikácie môže byť k dispozícii skupine pre spoluprácu a Komisii.

Článok 15

Sťažnosti a odvolania

Vnútroštátne schémy certifikácie obsahujú postupy alebo odkazy na platné vnútroštátne právne predpisy, ktoré definujú mechanizmus účinného podávania a vybavovania sťažností a odvolaní v súvislosti s vykonávaním schémy certifikácie alebo vydaným certifikátom zhody. Tieto postupy zahŕňajú informovanie sťažovateľa o priebehu konania a o prijatom rozhodnutí, a informovanie sťažovateľa o práve na účinný súdny prostriedok nápravy. Vo vnútroštátnych schémach certifikácie sa vyžaduje, aby sa všetky sťažnosti a odvolania, ktoré certifikačný orgán nevyriešil alebo nemohol vyriešiť, zaslali vlastníkovi schémy na posúdenie a vyriešenie.

Článok 16

Činnosti dohľadu

1. Vo vnútroštátnych schémach certifikácie sa vyžaduje, aby certifikačné orgány vykonávali činnosti dohľadu pozostávajúce z hodnotenia procesov v rámci dohľadu kombinovaných s náhodnými skúškami alebo kontrolami.

2. Vnútroštátne schémy certifikácie obsahujú požiadavky, aby vlastníci schém monitorovali dodržiavanie povinností certifikačných orgánov podľa nariadenia (EÚ) č. 910/2014 a prípadne podľa vnútroštátnych schém certifikácie.

3. Vnútroštátne schémy certifikácie obsahujú požiadavky, aby certifikačné orgány monitorovali:

a) dodržiavanie povinností držiteľov certifikátu zhody vydaného v rámci vnútroštátnych schém certifikácie týkajúcich sa certifikácie podľa nariadenia (EÚ) č. 910/2014 a podľa vnútroštátnych schém certifikácie;

b) súlad certifikovaného riešenia peňaženky s požiadavkami stanovenými vo vnútroštátnych schémach certifikácie.

Článok 17

Dôsledky nesúladu

Vo vnútroštátnych schémach certifikácie sa stanovia dôsledky nesúladu certifikovaného riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, s požiadavkami stanovenými v tomto nariadení. Tieto dôsledky zahŕňajú tieto aspekty:

1. povinnosť certifikačného orgánu informovať držiteľa certifikátu zhody a požiadať držiteľa certifikátu zhody o vykonanie nápravných opatrení;

2. povinnosť certifikačného orgánu informovať ostatné príslušné orgány dohľadu nad trhom, ak sa nesúlad týka príslušných právnych predpisov Únie;

3. podmienky vykonávania nápravných opatrení držiteľom certifikátu zhody;

4. podmienky pozastavenia platnosti certifikátu zhody certifikačným orgánom a obnovenia platnosti certifikátu zhody po odstránení nesúladu;

5. podmienky zrušenia certifikátu zhody certifikačným orgánom;

6. dôsledky nedodržania požiadaviek vnútroštátnej schémy certifikácie certifikačným orgánom.

KAPITOLA VII

ŽIVOTNÝ CYKLUS CERTIFIKÁCIE

Článok 18

Životný cyklus certifikácie

1. Platnosť certifikátov zhody vydaných v rámci vnútroštátnych schém certifikácie podlieha pravidelným hodnotiacim činnostiam certifikačného orgánu vykonávaným v súlade s požiadavkami stanovenými v prílohe IX.

2. Vnútroštátne schémy certifikácie obsahujú proces opätovnej certifikácie riešení peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytujú, na žiadosť držiteľa certifikátu zhody pred uplynutím platnosti pôvodného certifikátu zhody. Tento proces opätovnej certifikácie zahŕňa úplné hodnotenie riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, vrátane posúdenia zraniteľnosti, podľa zásad stanovených v prílohe IX.

3. Vnútroštátne schémy certifikácie obsahujú proces riadenia zmien v certifikovanom riešení peňaženky a v schéme elektronickej identifikácie, v rámci ktorej sa poskytuje. Tento proces zahŕňa pravidlá na určenie, či sa má na zmenu vzťahovať osobitné hodnotenie uvedené v odseku 4 alebo overenie prevádzkovej účinnosti procesov údržby podľa prílohy IV.

4. Vnútroštátne schémy certifikácie musia obsahovať proces osobitných hodnotení v súlade s normou EN ISO/IEC 17065:2012. Tento proces osobitných hodnotení zahŕňa výber činností, ktoré sa majú vykonať na riešenie konkrétneho problému, ktorý bol podnetom na osobitné hodnotenie.

5. Vo vnútroštátnych schémach certifikácie sa stanovia pravidlá týkajúce sa zrušenia certifikátu zhody.

KAPITOLA VIII

ZAZNAMENÁVANIE ÚDAJOV A OCHRANA INFORMÁCIÍ

Článok 19

Uchovávanie záznamov

1. Vnútroštátne schémy certifikácie obsahujú požiadavky na certifikačné orgány týkajúce sa systému záznamov pre všetky relevantné informácie, ktoré vznikli v súvislosti s činnosťami posudzovania zhody, ktoré vykonávajú, vrátane údajov vydaných a prijatých poskytovateľmi riešení peňaženky a schémami elektronickej identifikácie, v rámci ktorých sa poskytujú. Záznamy takýchto informácií sa uchovávajú bezpečným spôsobom. Záznamy sa môžu uchovávať elektronicky a zostávajú prístupné tak dlho, ako sa to vyžaduje v právnych predpisoch Únie alebo vo vnútroštátnych právnych predpisoch, a najmenej päť rokov po zrušení alebo uplynutí platnosti príslušného certifikátu zhody.

2. Vo vnútroštátnych schémach certifikácie sa stanovia požiadavky, aby držiteľ certifikátu zhody na účely tohto nariadenia a najmenej päť rokov po zrušení alebo uplynutí platnosti príslušného certifikátu zhody bezpečne uchovával tieto informácie:

a) záznamy o informáciách poskytnutých certifikačnému orgánu alebo niektorému z jeho subdodávateľov počas procesu certifikácie;

b) vzorky hardvérových komponentov, ktoré boli zahrnuté do rozsahu certifikácie pre riešenie peňaženky.

3. Vo vnútroštátnych schémach certifikácie sa vyžaduje, aby držiteľ certifikátu zhody na požiadanie sprístupnil informácie uvedené v odseku 1 certifikačnému orgánu alebo orgánu dohľadu uvedenému v článku 46a ods. 1 nariadenia (EÚ) č. 910/2014.

Článok 20

Ochrana informácií

V rámci vnútroštátnych schém certifikácie sú všetky osoby alebo organizácie, ktorým je umožnený prístup k informáciám pri výkone činností v rámci vnútroštátnej schémy certifikácie, povinné zaistiť bezpečnosť a ochranu obchodných tajomstiev a iných dôverných informácií, ako aj zachovanie práv duševného vlastníctva a prijať potrebné a vhodné technické a organizačné opatrenia na zabezpečenie tejto dôvernosti.

KAPITOLA IX

ZÁVEREČNÉ USTANOVENIA

Článok 21

Prechod na európsky systém certifikácie kybernetickej bezpečnosti

Toto nariadenie podlieha preskúmaniu po prijatí prvého európskeho systému certifikácie kybernetickej bezpečnosti pre riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorých sa poskytujú, s cieľom zohľadniť prínos takéhoto európskeho systému certifikácie kybernetickej bezpečnosti k celkovej certifikácii riešení peňaženky a schém elektronickej identifikácie, v rámci ktorých sa poskytujú.

Článok 22

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 28. novembra 2024

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA I

REGISTER RIZÍK PRE EURÓPSKE PEŇAŽENKY DIGITÁLNEJ IDENTITY

Úvod

V registri rizík sú opísané hlavné riziká a hrozby v oblasti bezpečnosti a ochrany súkromia, ktoré sa týkajú peňaženiek a ktoré musia byť riadne zohľadnené v každej architektúre a realizácii peňaženiek. **Hlavné riziká** (oddiel I) súvisia s používaním peňaženiek používateľmi a spoliehajúcimi sa stranami a sú spojené s priamymi hrozbami zameranými na aktíva peňaženiek. Okrem toho je identifikovaných niekoľko **systémových rizík** (oddiel II) pre peňaženky, ktoré by zvyčajne vyplývali z kombinácie hrozieb vzťahujúcich sa na celý systém peňaženky.

Typ rizika	ID rizika	Názvy súvisiacich rizík
Hlavné riziká pre peňaženky	R1	Vytvorenie alebo používanie existujúcej elektronickej totožnosti
	R2	Vytvorenie alebo používanie falošnej elektronickej totožnosti
	R3	Vytvorenie alebo používanie falošných atribútov
	R4	Krádež totožnosti
	R5	Krádež údajov
	R6	Zverejnenie údajov
	R7	Manipulácia s údajmi
	R8	Strata údajov
	R9	Neoprávnená transakcia
	R10	Manipulácia s transakciami
	R11	Popretie
	R12	Zverejnenie údajov o transakciách
	R13	Prerušenie prevádzky
	R14	Sledovanie
Systémové riziká	SR1	Hromadné sledovanie
	SR2	Poškodenie dobrého mena
	SR3	Nedodržiavanie právnych predpisov

V registri sa identifikujú aj **technické hrozby** (oddiel III) zamerané na realizáciu riešenia peňaženky. Tieto hrozby sa týkajú vysokých rizík v tom zmysle, že každá z nich by sa mohla použiť na spustenie mnohých ďalších vysokých rizík.

Typ hrozby	ID hrozby	Názvy súvisiacich hrozieb	Podkategórie hrozieb
Technická hrozba	TT1	Fyzické útoky	1.1. *Krádež*
			1.2. *Únik informácií*
			1.3. *Neoprávnená manipulácia*
	TT2	Chyby a nesprávne konfigurácie	2.1. *Chyby pri správe systému IT*
			2.2. *Chyby na úrovni aplikácie alebo chyby pri používaní*
			2.3. *Chyby v čase vývoja a nesprávne konfigurácie systému*

Typ hrozby	ID hrozby	Názvy súvisiacich hrozieb	Podkategórie hrozieb
	TT3	Používanie nespoľahlivých zdrojov	3.1. *Chybné používanie alebo konfigurácia komponentov peňaženky*
	TT4	Poruchy a výpadky	4.1. *Porucha alebo nefunkčnosť vybavenia, zariadení alebo systémov*
			4.2. *Strata zdrojov*
			4.3. *Strata podporných služieb*
	TT5	Škodlivé konanie	5.1. *Zachytávanie informácií*
			5.2. *Phishing a spoofing*
			5.3. *Prehrávanie správ*
			5.4. *Útok hrubou silou*
			5.5. *Zraniteľnosti softvéru*
			5.6. *Útoky na dodávateľský reťazec*
			5.7. *Škodlivý softvér*
			5.8. *Predpovedanie náhodných čísel*

Nakoniec sú v registri uvedené **priame hrozby pre peňaženky** a každá z nich je spojená s (neúplným) výberom rizík (oddiel IV).

ODDIEL I

Hlavné riziká pre peňaženky

R1. Vytvorenie alebo používanie existujúcej elektronickej totožnosti

Vytvorenie alebo používanie existujúcej elektronickej totožnosti je definované ako vytvorenie elektronickej totožnosti v peňaženke, ktorá existuje v reálnom svete a je pridelená inému používateľovi. Toto riziko vo svojej podstate vedie k riziku krádeže totožnosti (R4) a riziku neoprávnených transakcií (R9).

R2. Vytvorenie alebo používanie falošnej elektronickej totožnosti

Vytvorenie alebo používanie falošnej elektronickej totožnosti je definované ako vytvorenie elektronickej totožnosti v peňaženke, ktorá neexistuje v reálnom svete.

R3. Vytvorenie alebo používanie falošných atribútov

Vytvorenie alebo používanie falošných atribútov je definované ako vytvorenie alebo používanie atribútov, ktoré nemožno validovať, aby ich vydal deklarovaný poskytovateľ, a nemožno im dôverovať.

R4. Krádež totožnosti

Krádež totožnosti je definovaná ako neoprávnené získanie jednotky peňaženky alebo strata autentifikačných faktorov, čo umožňuje vydávať sa za určitú osobu.

R5. Krádež údajov

Krádež údajov je definovaná ako neoprávnené extrahovanie údajov. Krádež údajov sa spája aj s hrozbami, ako je zachytenie údajov (neoprávnené zachytenie údajov pri prenose) a dešifrovanie údajov (neoprávnené dekódovanie zašifrovaných údajov), ktoré môžu v niektorých prípadoch viesť k zverejneniu údajov (R6).

R6. Zverejnenie údajov

Zverejnenie údajov je definované ako neoprávnené odhalenie osobných údajov vrátane osobitných kategórií osobných údajov. Veľmi podobné je riziko porušenia ochrany súkromia, ak sa posudzuje skôr z hľadiska ochrany súkromia než z hľadiska bezpečnosti.

R7. Manipulácia s údajmi

Manipulácia s údajmi je definovaná ako neoprávnená zmena údajov.

R8. Strata údajov

Strata údajov je definovaná ako situácia, keď sa údaje uložené v peňaženke stratia v dôsledku zneužitia alebo škodlivého konania. Toto riziko je často sekundárnym rizikom manipulácie s údajmi (R7) alebo prerušenia prevádzky (R13), keď nie je možné obnoviť všetky údaje alebo ich časť.

R9. Neoprávnená transakcia

Neoprávnené transakcie sú definované ako prevádzkové činnosti vykonávané bez povolenia alebo vedomia používateľa peňaženky. V mnohých prípadoch môže neoprávnená transakcia viesť ku krádeži totožnosti (R4) alebo zverejneniu údajov (R6). Týka sa to aj neoprávnených transakcií, napríklad zneužitia kryptografických kľúčov.

R10. Manipulácia s transakciami

Manipulácia s transakciami je definovaná ako neoprávnená zmena operácií v peňaženke. Manipulácia s transakciami je útokom na integritu a súvisí s porušením integrity údajov.

R11. Popretie

Popretie je definované ako situácia, keď zainteresovaná strana môže poprieť vykonanie činnosti alebo účasť na transakcii a ostatné zainteresované strany nemajú náležité dôkazy, ktoré by to vyvrátili.

R12. Zverejnenie údajov o transakciách

Zverejnenie údajov o transakciách je definované ako zverejnenie informácií o transakcii medzi zainteresovanými stranami.

R13. Prerušenie prevádzky

Prerušenie prevádzky je definované ako prerušenie alebo zhoršenie bežnej prevádzky peňaženky. Špecifickým druhom prerušenia prevádzky je zablokovanie používateľa, ktoré je definované ako situácia, keď používateľ nemôže pristupovať k svojmu účtu alebo peňaženke.

R14. Sledovanie

Sledovanie alebo monitorovanie je definované ako neoprávnené sledovanie alebo pozorovanie činností, komunikácie alebo údajov používateľa peňaženky. Sledovanie často súvisí s inferenciou, ktorá je definovaná ako vyvodzovanie citlivých alebo osobných informácií zo zdanlivo neškodných údajov.

ODDIEL II

Systémové riziká

Tieto riziká sa v zozname hrozieb nepoužívajú, pretože sú zvyčajne dôsledkom viacerých hrozieb, ktoré sa opakujú tak, že ohrozujú celý systém.

SR1. Hromadné sledovanie

Hromadné sledovanie je definované ako sledovanie alebo pozorovanie činností mnohých používateľov prostredníctvom komunikácie alebo údajov z ich peňaženky. Hromadné sledovanie sa často spája so sledovaním (R14) a inferenciou v globálnom meradle, pri ktorej sa kombinujú informácie o mnohých používateľoch s cieľom odvodiť citlivé alebo osobné údaje o používateľoch alebo identifikovať štatistické trendy, ktoré možno použiť na navrhovanie ďalších útokov.

SR2. Poškodenie dobrého mena

Poškodenie dobrého mena je definované ako škoda spôsobená dobrému menu organizácie alebo vládneho orgánu. Poškodenie dobrého mena vyplýva aj z iných rizík, keď o porušení alebo incidente informujú médiá a vykreslia organizáciu v nepriaznivom svetle. Poškodenie dobrého mena môže viesť k ďalším rizikám, ako je strata dôvery vyplývajúca z odôvodnených pochybností používateľa a strata ekosystému, keď sa zrúti celý ekosystém.

SR3. Nedodržiavanie právnych predpisov

Nedodržiavanie právnych predpisov je definované ako situácia, keď nie je možné dodržiavať príslušné zákony, predpisy alebo normy. V kontexte peňaženky, keďže bezpečnosť a ochrana súkromia v rámci riešenia sú zákonnými požiadavkami, všetky hrozby pravdepodobne povedú k určitému druhu nedodržiavania právnych predpisov.

ODDIEL III

Technické hrozby

Nie všetky technické hrozby sú spojené s konkrétnymi rizikami pre peňaženky, pretože mnohé z nich sú prostriedkom, ktorý by sa dal použiť na realizáciu útokov zodpovedajúcich mnohým rôznym rizikám.

TT1. Fyzické útoky

1.1. *Krádež*

Krádež je definovaná ako odcudzenie zariadenia, ktoré môže zmeniť správne fungovanie peňaženky (v prípade, že je zariadenie odcudzené a jednotka peňaženky nie je primerane chránená). To môže prispieť k mnohým rizikám vrátane krádeže totožnosti (R4), krádeže údajov (R5) a neoprávnených transakcií (R9).

1.2. *Únik informácií*

Únik informácií je definovaný ako neoprávnený prístup k informáciám, ich odhalenie alebo zdieľanie po získaní fyzického prístupu k peňaženke. To môže prispieť najmä k zverejneniu údajov (R6) a krádeži údajov (R5).

1.3. *Neoprávnená manipulácia*

Neoprávnená manipulácia je definovaná ako narušenie integrity jedného alebo viacerých komponentov jednotky peňaženky alebo narušenie integrity komponentov, na ktoré sa jednotka peňaženky spolieha, napr. používateľského zariadenia alebo jeho operačného systému. To môže prispieť najmä k manipulácii s údajmi (R7), strate údajov (R8) a manipulácii s transakciami (R10). Ak sa neoprávnená manipulácia zameriava na softvérové komponenty, môže prispieť k mnohým rizikám.

TT2. Chyby a nesprávne konfigurácie

2.1. *Chyby pri správe systému IT*

Chyby pri správe systému IT sú definované ako únik, zdieľanie alebo poškodenie informácií spôsobené nesprávnym používaním aktív IT používateľmi (nedostatočná informovanosť o funkciách aplikácie) alebo nesprávnou konfiguráciou alebo správou aktív IT.

2.2. *Chyby na úrovni aplikácie alebo chyby pri používaní*

Chyby na úrovni aplikácie alebo chyby pri používaní sú definované ako nefunkčnosť aplikácie spôsobená chybou v samotnej aplikácii alebo chybou niektorého z používateľov (používateľov peňaženky a spoliehajúcich sa strán).

2.3. *Chyby v čase vývoja a nesprávne konfigurácie systému*

Chyby v čase vývoja a nesprávna konfigurácia systému sú definované ako nefunkčnosť alebo zraniteľnosti spôsobené nesprávne vyvinutými alebo nakonfigurovanými aktívami IT alebo obchodnými procesmi (nevhodné špecifikácie produktov IT, nevhodná použiteľnosť, nezabezpečené rozhrania, nesprávne toky politík a postupov, chyby v návrhu).

TT3. Používanie nespoľahlivých zdrojov

Používanie nespoľahlivých zdrojov je definované ako činnosť vedúca k neúmyselnej škode spôsobenej zle definovanými vzťahmi dôvery, napríklad dôverou v poskytovateľa tretej strany bez dostatočného zabezpečenia.

3.1. *Chybné používanie alebo konfigurácia komponentov peňaženky*

Chybné používanie alebo konfigurácia komponentov peňaženky sú definované ako neúmyselné poškodenie komponentov peňaženky v dôsledku chybného použitia alebo nesprávnej konfigurácie požívateľmi peňaženky alebo nedostatočne vyškolenými vývojármi, alebo v dôsledku nedostatočného prispôsobenia sa zmenám v panoráme hrozieb, typicky použitím zraniteľných komponentov tretích strán alebo platforiem v prevádzke.

TT4. Poruchy a výpadky

4.1. *Porucha alebo nefunkčnosť vybavenia, zariadení alebo systémov*

Porucha alebo nefunkčnosť vybavenia je definovaná ako neúmyselné poškodenie aktív IT v dôsledku poruchy alebo nefunkčnosti vybavenia vrátane infraštruktúry poskytovateľa a zariadení používateľa.

4.2. *Strata zdrojov*

Strata zdrojov je definovaná ako výpadok alebo nefunkčnosť v dôsledku nedostupnosti týchto zdrojov, napr. dielov potrebných na údržbu.

4.3. *Strata podporných služieb*

Strata podporných služieb je definovaná ako výpadok alebo nefunkčnosť z dôvodu nedostupnosti podporných služieb potrebných na riadnu prevádzku systému vrátane sieťového pripojenia infraštruktúry poskytovateľa a zariadenia používateľa.

TT5. Škodlivé konanie

5.1. *Zachytávanie informácií*

Zachytávanie informácií je definované ako zachytenie nesprávne zabezpečených informácií pri prenose vrátane útokov typu *man-in-the-middle*.

5.2. *Phishing a spoofing*

Phishing je definovaný ako získavanie informácií od používateľa prostredníctvom klamlivej interakcie, čo sa často spája s falšovaním legitímnych komunikačných prostriedkov a webových sídiel. Tieto hrozby sú zamerané na používateľa a zvyčajne prispievajú ku krádeži totožnosti (R4) a neoprávneným transakciám (R9), často prostredníctvom krádeže údajov (R5) alebo zverejnenia údajov (R6).

5.3. *Prehrávanie správ*

Prehrávanie správ je definované ako opätovné použitie už zachytených správ na vykonanie neoprávnených transakcií, často na úrovni protokolu. Táto technická hrozba prispieva najmä k neoprávneným transakciám, ktoré potom môžu viesť k ďalším rizikám v závislosti od transakcie.

5.4. *Útok hrubou silou*

Útok hrubou silou je definovaný ako narušenie bezpečnosti a často aj dôvernosti vykonávaním veľkého počtu interakcií až dovtedy, kým odozvy neposkytnú cenné informácie.

5.5. *Zraniteľnosti softvéru*

Hrozba súvisiaca so zraniteľnosťou softvéru je narušenie bezpečnosti zneužitím zraniteľnosti softvéru v komponentoch peňaženky alebo v softvérových a hardvérových komponentoch použitých pri realizácii peňaženky vrátane zverejnených zraniteľností a nezverejnených zraniteľností (nultého dňa).

5.6. *Útoky na dodávateľský reťazec*

Útok na dodávateľský reťazec je definovaný ako narušenie bezpečnosti prostredníctvom útokov spáchaných na dodávateľa poskytovateľa peňaženky alebo jej používateľov s cieľom umožniť ďalšie útoky na samotnú peňaženku.

5.7. *Škodlivý softvér*

Škodlivý softvér je definovaný ako narušenie bezpečnosti prostredníctvom škodlivých aplikácií, ktoré vykonávajú nežiaduce a nelegitímne činnosti v peňaženke.

5.8. *Predpovedanie náhodných čísel*

Predpovedanie náhodných čísel je definované ako umožnenie útokov hrubou silou prostredníctvom čiastočného alebo úplného predpovedania generovaných náhodných čísel.

ODDIEL IV

Hrozby pre peňaženky

V tomto poslednom oddiele je uvedený výber typických scenárov hrozieb špecifických pre peňaženky, ktoré sú priradené ku kľúčovým súvisiacim hlavným rizikám, ktoré sú uvedené vyššie. V tomto zozname sa uvádzajú hrozby, ktoré je potrebné pokryť, nejde však o vyčerpávajúci zoznam hrozieb, keďže tie do značnej miery závisia od architektúry vybraného riešenia peňaženky a od vývoja prostredia hrozieb. Okrem toho v posúdení rizík a navrhovaných opatreniach môže byť poskytovateľ peňaženky zodpovedný len za tie komponenty, ktoré patria do rozsahu pôsobnosti certifikácie (*).

ID *Identifikátor*	Opis hrozby *Opis zistenej hrozby (')*	Názov rizika *Súvisiace riziká*
TR1	Útočník môže zrušiť pseudonymy bez opodstatneného dôvodu.	Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR2	Útočník môže vydávať falošné elektronické totožnosti, ktoré neexistujú.	Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR3	Útočník môže začať vydávať neautorizované osobné identifikačné údaje (PID).	Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR4	Útočník môže prinútiť správcu, aby do zoznamu dôveryhodných poskytovateľov PID zadal nesprávneho poskytovateľa PID.	Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR5	Útočník môže obísť službu preukazovania totožnosti na diaľku.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR6	Útočník môže obísť službu fyzického preukazovania totožnosti.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR7	Útočník môže obísť služby preukazovania totožnosti súvisiace s použitím (kvalifikovaného) certifikátu na diaľku.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR8	Útočník môže získať prístup k peňaženke, ktorá nie je viazaná na osobu.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR9	Útočník môže prekonať technické a procedurálne kontroly a vytvoriť nesprávne PID.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR10	Útočník môže aktivovať novú peňaženku na neplatnom zariadení WSCD.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)
TR11	Útočník môže obísť službu preukazovania totožnosti súvisiacu s použitím existujúcich prostriedkov elektronickej identifikácie.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Krádež totožnosti (R4)/Neoprávnená transakcia (R9)
TR12	Útočník môže obísť overenie poskytovateľa PID, že peňaženka je pod kontrolou používateľa, a nechať si vydať PID do spreneverenej peňaženky pod kontrolou útočníka.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Krádež totožnosti (R4)/Neoprávnená transakcia (R9)

ID *Identifikátor*	Opis hrozby *Opis zistenej hrozby (')*	Názov rizika *Súvisiace riziká*
TR13	Útočník môže získať platné PID do neplatnej jednotky peňaženky.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Krádež totožnosti (R4)/Neoprávnená transakcia (R9)
TR14	Poskytovateľ PID môže vydávať falošné totožnosti, ak je totožnosť spojená s existujúcou osobou.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Krádež totožnosti (R4)/Neoprávnená transakcia (R9)
TR15	Útočník môže prepojiť PID s nesprávnou peňaženkou, pretože poskytovateľ PID nie je schopný prepojiť PID so správnou peňaženkou.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Krádež totožnosti (R4)/Neoprávnená transakcia (R9)
TR16	Útočník môže dosiahnuť, že používateľ schváli aktiváciu novej jednotky/inštancie peňaženky, ktorá je pod kontrolou útočníka – čím útočník následne získa kontrolu aj nad osvedčeniami.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Vytvorenie alebo používanie falošnej elektronickej totožnosti (R2)/Krádež totožnosti (R4)/Neoprávnená transakcia (R9)
TR17	Útočník môže vydať PID iného štátu, aby získal prístup k údajom/digitálnym aktívam cieľových občanov.	Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)/Krádež totožnosti (R4)/Neoprávnená transakcia (R9)
TR18	Útočník môže prekonať technické a procedurálne kontroly a vytvoriť falošné (kvalifikované) elektronické osvedčenia atribútov [(Q)EAA].	Vytvorenie alebo používanie falošných atribútov (R3)
TR19	Útočník môže predložiť (Q)EEA, ktoré mu neboli platne vydané.	Vytvorenie alebo používanie falošných atribútov (R3)
TR20	Útočník môže zaútočiť na kryptografický mechanizmus prepojenia peňaženky medzi PID a (Q)EEA, ktoré by mu nemalo byť vydané.	Vytvorenie alebo používanie falošných atribútov (R3)
TR21	Útočník môže použiť (Q)EEA v peňaženke, hoci fyzický náprotivok (Q)EEA je neplatný alebo jeho platnosť uplynula.	Vytvorenie alebo používanie falošných atribútov (R3)
TR22	Útočník môže obísť overenie poskytovateľa (Q)EEA, že peňaženka je pod kontrolou používateľa, a nechať si vydať (Q)EEA do spreneverenej peňaženky pod kontrolou útočníka.	Vytvorenie alebo používanie falošných atribútov (R3)
TR23	Útočník môže sfalšovať elektronické osvedčenia atribútov.	Vytvorenie alebo používanie falošných atribútov (R3)
TR24	Útočník môže do peňaženky vložiť sfalšované elektronické osvedčenia atribútov.	Vytvorenie alebo používanie falošných atribútov (R3)
TR25	Peňaženka môže predložiť atribúty spoliehajúcej sa strane bez schválenia používateľom.	Zverejnenie údajov (R6)
TR26	Môže dôjsť k predloženiu PID, (Q)EEA alebo pseudonymov nesprávnej spoliehajúcej sa strane.	Zverejnenie údajov (R6)
TR27	Útočník môže iniciovať škodlivé obnovenie elektronického osvedčenia atribútov.	Zverejnenie údajov (R6)
TR28	Útočník môže prinútiť používateľa, aby neoprávnene schválil žiadosť o elektronické osvedčenia atribútov (phishing alebo iné).	Zverejnenie údajov (R6)

ID *Identifikátor*	Opis hrozby *Opis zistenej hrozby (')*	Názov rizika *Súvisiace riziká*
TR29	Útočník môže prezradiť atribúty z peňaženky a identifikovať používateľa peňaženky v situácii, keď identifikácia nie je potrebná/povolená.	Zverejnenie údajov (R6)
TR30	Útočník môže prekonať technické a procedurálne kontroly na extrahovanie údajov.	Zverejnenie údajov (R6)
TR31	Môže dôjsť k vyzradeniu žiadosti útočníkovi.	Zverejnenie údajov (R6)
TR32	Útočník môže získať poznatky o zahrnutých pravidlách sprístupňovania informácií o atribútoch a predložiť atribúty obsiahnuté v aktuálnej žiadosti jednotiek peňaženky.	Zverejnenie údajov (R6)
TR33	Útočník môže extrahovať logy alebo ich časti.	Zverejnenie údajov (R6)
TR34	Útočník sa môže dozvedieť, či je peňaženka nainštalovaná v rovnakom zariadení, ktoré používa, alebo v inom zariadení, a získať o nej informácie.	Zverejnenie údajov (R6)
TR35	Útočník môže získať znalostný faktor používaný na autentifikáciu používateľa v aplikácii WSCA.	Zverejnenie údajov (R6)
TR36	Elektronické osvedčenie atribútov o osobe, ktoré sa predkladá vo viacerých transakciách so spoliehajúcou sa stranou alebo medzi rôznymi spoliehajúcimi sa stranami, neúmyselne umožňuje prepojiť viaceré transakcie s príslušnou osobou.	Zverejnenie údajov (R6)
TR37	Verejný zoznam zrušených osvedčení/spoliehajúcich sa strán môže obsahovať informácie o tom, ako používateľ používa svoje osvedčenie (napr. lokalita, IP adresa…).	Zverejnenie údajov (R6)
TR38	Spoliehajúce sa strany môžu ovplyvniť integritu logov, keďže nedokážu preukázať súhlas používateľa so zdieľanými atribútmi.	Zverejnenie údajov (R6)
TR39	Útočník môže nezákonne sledovať používateľov peňaženky pomocou jedinečných/vysledovateľných identifikátorov.	Zverejnenie údajov (R6)/Sledovanie (R14)
TR40	Spoliehajúca sa strana tvorená viacerými jednotkami/subjektmi, z ktorých každý má určený odlišný rozsah toho, čo môže požadovať/spracúvať, môže požadovať a spracúvať údaje, na ktoré nemá zákonné dôvody.	Zverejnenie údajov (R6)/Neoprávnená transakcia (R9)
TR41	Útočník môže narušiť kontrolu integrity a pravosti PID v peňaženke tak, aby bola kontrola zakaždým úspešná.	Manipulácia s údajmi (R7)
TR42	Útočník môže obísť alebo narušiť vykonávanie kontrol v peňaženke, ktorými sa overuje integrita a pravosť požadovaných atribútov, a to tak, aby bola kontrola zakaždým úspešná.	Manipulácia s údajmi (R7)
TR43	Útočník môže obísť alebo narušiť vykonávanie kontrol v peňaženke, ktorými sa overujú všetky požadované atribúty patriace rovnakému používateľovi, a to tak, aby bola kontrola zakaždým úspešná.	Manipulácia s údajmi (R7)
TR44	Útočník môže obísť alebo narušiť vykonávanie kontrol v peňaženke, ktorými sa overuje, či sú PID platné a či ich vydal dôveryhodný poskytovateľ PID, a to tak, aby bola kontrola zakaždým úspešná.	Manipulácia s údajmi (R7)

ID *Identifikátor*	Opis hrozby *Opis zistenej hrozby (*)*	Názov rizika *Súvisiace riziká*
TR45	Útočník môže obísť alebo narušiť vykonávanie kontrol v peňaženke, ktorými sa overuje, či je (Q)EEA platné a či ho vydal kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý je registrovaný na vydanie daného (Q)EEA, a to tak, aby bola kontrola zakaždým úspešná.	Manipulácia s údajmi (R7)
TR46	Útočník môže obísť alebo narušiť vykonávanie kontrol v peňaženke, ktorými sa overuje, či poskytovateľ PID zrušil dané PID, a to tak, aby bola kontrola zakaždým úspešná.	Manipulácia s údajmi (R7)
TR47	Útočník môže obísť alebo narušiť vykonávanie kontrol v peňaženke, ktorými sa overuje, či poskytovateľ (Q)EEA zrušil dané (Q)EEA, a to tak, aby bola kontrola zakaždým úspešná.	Manipulácia s údajmi (R7)
TR48	Útočník môže upraviť obsah zálohovania a obnovy údajov, ktoré by mali byť výlučne pod kontrolou používateľa.	Manipulácia s údajmi (R7)/Strata údajov (R8)
TR49	Útočník môže v prípade určitej inštancie peňaženky upraviť históriu transakcií z logov aktivít.	Manipulácia s údajmi (R7)/Strata údajov (R8)
TR50	Útočník môže odpočúvať počas spojenia z peňaženky k spoliehajúcim sa stranám.	Krádež údajov (R5)/Zverejnenie údajov (R6)
TR51	Útočník môže presvedčiť používateľa, aby poskytol osobné údaje (t. j. PID, elektronické osvedčenia atribútov, pseudonymy, elektronické podpisy, logy a iné údaje) útočníkovi alebo tretej strane, ktorej ich používateľ nemal v úmysle poskytnúť.	Krádež údajov (R5)/Zverejnenie údajov (R6)
TR52	Útočník môže v prípade určitej inštancie peňaženky prečítať históriu transakcií z logov aktivít.	Krádež údajov (R5)/Zverejnenie údajov (R6)
TR53	Útočník môže exportovať alebo extrahovať materiál kryptografického kľúča mimo zariadenia WSCD.	Krádež údajov (R5)/Zverejnenie údajov (R6)/Neoprávnená transakcia (R9)
TR54	Útočník môže prečítať obsah zálohovania a obnovy údajov, ktoré by mali byť výlučne pod kontrolou používateľa.	Krádež údajov (R5)/Zverejnenie údajov (R6)
TR55	Útočník môže obísť metódu autentifikácie používateľa, aby použil pseudonym vygenerovaný jednotkou peňaženky.	Krádež totožnosti (R4)
TR56	Útočník môže používateľom navrhnúť aplikáciu, ktorá imituje konkrétnu legitímnu peňaženku.	Krádež totožnosti (R4)
TR57	Útočník môže exportovať údaje peňaženky vrátane PID, (Q) EEA alebo logov.	Krádež totožnosti (R4)
TR58	Útočník môže exportovať materiál kryptografickej väzby.	Krádež totožnosti (R4)
TR59	Útočník môže prevziať totožnosť prostredníctvom kryptografických kľúčov peňaženky.	Krádež totožnosti (R4)
TR60	Útočník môže duplikovať osobnú jednotku peňaženky iného používateľa v jeho osobnom zariadení a použiť ju.	Krádež totožnosti (R4)/Vytvorenie alebo používanie existujúcej elektronickej totožnosti (R1)

ID *Identifikátor*	Opis hrozby *Opis zistenej hrozby (')*	Názov rizika *Súvisiace riziká*
TR61	Orgány iného štátu môžu požiadať používateľa, aby ukázal a/alebo poskytol všetky údaje o peňaženke, v situácii, keď je blízko, napríklad pri prekročení hranice daného štátu.	Krádež totožnosti (R4)/Sledovanie (R14)
TR62	Používateľ nemôže prenášať svoje logy transakcií po zlyhaní zariadenia používateľa, čo vedie k strate vysledovateľnosti predchádzajúcich transakcií v novej peňaženke.	Popretie (R11)
TR63	Používateľ nemôže obnoviť svoje logy transakcií po zlyhaní zariadenia používateľa, čo vedie k strate vysledovateľnosti v novej peňaženke.	Popretie (R11)
TR64	Spoliehajúce sa strany môžu mať ťažkosti s preukazovaním súhlasu s elektronickými podpismi na diaľku.	Popretie (R11)
TR65	Útočník môže počas pripojenia k spoliehajúcim sa stranám zahltiť spojenie (-ia) žiadosťami.	Prerušenie prevádzky (R13)
TR66	Útočník môže zahltiť službu poskytovania stavu pripojeniami k spoliehajúcim sa stranám.	Prerušenie prevádzky (R13)
TR67	Útočník môže dosiahnuť, že predloženie atribútu sa bude javiť ako spochybnené/popreté, hoci sa v predložení atribútu uvádza jeho platnosť.	Prerušenie prevádzky (R13)
TR68	Útočník môže zrušiť PID bez opodstatneného dôvodu.	Prerušenie prevádzky (R13)
TR69	Útočník môže zrušiť PID bez súhlasu používateľa.	Prerušenie prevádzky (R13)
TR70	Útočník môže zrušiť (Q)EEA bez opodstatneného dôvodu.	Prerušenie prevádzky (R13)
TR71	Útočník môže zrušiť (Q)EEA bez súhlasu používateľa.	Prerušenie prevádzky (R13)
TR72	Útočník môže spustiť viacero žiadostí o identifikáciu bez toho, aby boli rozpoznané ako zámerne ojedinelé žiadosti.	Prerušenie prevádzky (R13)
TR73	Útočník môže odoslať viacero žiadostí bez následnej transakcie.	Prerušenie prevádzky (R13)
TR74	Útočník môže umožniť spoliehajúcej sa strane požiadať o identifikáciu bez zodpovedajúcej identifikácie (odozvy) a úplnej kontroly.	Prerušenie prevádzky (R13)
TR75	Útočník môže poslať odozvu na žiadosť po uplynutí jej časového limitu alebo v podobných situáciách, ktoré vedú k prerušeniu prevádzky.	Prerušenie prevádzky (R13)
TR76	Spoliehajúca sa strana môže poslať viacero neplatných žiadostí.	Prerušenie prevádzky (R13)
TR77	Útočník môže poslať poskytovateľovi peňaženky viacero neplatných žiadostí.	Prerušenie prevádzky (R13)
TR78	Útočník môže spôsobiť, že členský štát nebude môcť vylúčiť nedôveryhodného poskytovateľa PID zo zoznamu dôveryhodných poskytovateľov PID.	Prerušenie prevádzky (R13)
TR79	Útočník môže zabrániť pozastaveniu platnosti alebo zrušeniu peňaženky.	Prerušenie prevádzky (R13)

ID *Identifikátor*	Opis hrozby *Opis zistenej hrozby (')*	Názov rizika *Súvisiace riziká*
TR80	Útočník môže zablokovať transakcie spoliehajúcich sa strán, používateľov a/alebo poskytovateľa PID.	Prerušenie prevádzky (R13)
TR81	Útočník môže vypnúť alebo zneprístupniť zariadenie WSCD.	Prerušenie prevádzky (R13)
TR82	Útočník môže znemožniť poskytovateľovi PID zrušiť PID alebo pozastaviť ich platnosť.	Prerušenie prevádzky (R13)/Neoprávnená transakcia (R9)
TR83	Spoliehajúca sa strany môže odvodiť údaje o totožnosti používateľa nad rámec údajov, ktoré sú jej známe.	Sledovanie (R14)
TR84	Skupina kolúzne spolupracujúcich spoliehajúcich sa strán alebo poskytovateľov PID môže odvodiť údaje o totožnosti používateľa nad rámec údajov, ktoré sú im známe.	Sledovanie (R14)
TR85	Útočník môže sledovať a vystopovať používateľa pomocou osobných identifikačných údajov používateľa v prípade, keď sa identifikácia používateľa nevyžaduje.	Sledovanie (R14)
TR86	Útočník môže nakombinovať „falošné“ predloženie (Q)EEA.	Manipulácia s transakciami (R10)
TR87	Útočník môže aktivovať/prevziať peňaženku na diaľku (napr. bankovú aplikáciu zahŕňajúcu žiadosť o autentifikáciu alebo osvedčenie) bez výslovného súhlasu alebo výlučnej kontroly používateľa v situáciách, keď používateľ nevie o spoliehajúcej sa strane (napr. spí) alebo ju nemôže vidieť.	Manipulácia s transakciami (R10)
TR88	Útočníci môžu zmeniť metadáta žiadosti (názov služby, použitie atď.).	Manipulácia s transakciami (R10)
TR89	Útočníci môžu zmeniť informácie o odozve (stav služby, príležitosť atď.).	Manipulácia s transakciami (R10)
TR90	Útočníci môžu zmeniť informácie o atribútoch žiadosti (cez dotazovanie atď.).	Manipulácia s transakciami (R10)
TR91	Spoliehajúca sa strana môže prehrať prvky z predchádzajúcej relácie v inej relácii.	Manipulácia s transakciami (R10)
TR92	Útočník môže nahradiť alebo upraviť PID počas ich prenosu od poskytovateľa PID do jednotky peňaženky.	Manipulácia s transakciami (R10)
TR93	Útočník môže nahradiť alebo upraviť PID počas ich prenosu z jednotky peňaženky do spoliehajúcej sa strany online.	Manipulácia s transakciami (R10)
TR94	Útočník môže nahradiť alebo upraviť PID počas ich prenosu z jednotky peňaženky do spoliehajúcej sa strany offline.	Manipulácia s transakciami (R10)
TR95	Útočník môže vydať PID bez súhlasu používateľa.	Neoprávnená transakcia (R9)
TR96	Útočník môže použiť zrušené alebo neplatné zahrnuté pravidlá sprístupňovania informácií, prípadne bez vedomia spoliehajúcich sa strán.	Neoprávnená transakcia (R9)
TR97	Útočník môže peňaženku oklamať, aby overila nesprávne elektronické podpisy.	Neoprávnená transakcia (R9)
TR98	Útočník môže peňaženku použiť mimo kontroly používateľa.	Neoprávnená transakcia (R9)

ID *Identifikátor*	Opis hrozby *Opis zistenej hrozby (*[1]*)*	Názov rizika *Súvisiace riziká*
TR99	Útočník môže presvedčiť používateľa, aby autentifikoval a schválil transakcie s útočníkom alebo neoprávnenou treťou stranou.	Neoprávnená transakcia (R9)
TR100	Útočník môže prinútiť používateľa elektronicky sa podpísať bez toho, aby mu predložil obsah, alebo po predložení nesprávneho obsahu.	Neoprávnená transakcia (R9)
TR101	Útočník môže obísť kontrolu prístupu k účtu používateľa u poskytovateľa peňaženky.	Neoprávnená transakcia (R9)
TR102	Útočník sa môže počas pripojenia k spoliehajúcim sa stranám vydávať za spoliehajúcu sa stranu.	Neoprávnená transakcia (R9)/Zverejnenie údajov (R6)
TR103	Používateľ za spojením spoliehajúca sa strana – prehliadač môže byť iný ako používateľ za spojením spoliehajúca sa strana – peňaženka.	Neoprávnená transakcia (R9)/Zverejnenie údajov (R6)/Krádež totožnosti (R4)
TR104	Útočník môže presvedčiť používateľa, aby svoju peňaženku bezdôvodne zrušil.	Neoprávnená transakcia (R9)/Prerušenie prevádzky (R13)
TR105	Útočník môže vykonať útoky typu *man-in-the-middle*.	Neoprávnená transakcia (R9)/Zverejnenie údajov (R6)/Sledovanie (R14)
TR106	Útočník môže predložiť neplatné alebo zrušené atribúty z peňaženky, ktorá sa pravidelne nepripája k sieti.	Vplyv na rôzne riziká
TR107	Útočník môže odcudziť informácie používateľa sfalšovaním peňaženky.	Vplyv na rôzne riziká
TR108	Útočník sa môže vydávať za používateľa prehratím/imitovaním žiadosti o údaje (napr. pri autentifikácii), ktorá sa javí ako platná.	Vplyv na rôzne riziká
TR109	Útočník môže prehrať zahrnuté pravidlá sprístupňovania informácií vo vzťahu k používateľovi a napodobniť tak schválenú žiadosť.	Vplyv na rôzne riziká
TR110	Útočník môže po narušení alebo ohrození bezpečnosti zneužiť, že používatelia peňaženky nemajú nedostatok informácií, alebo zneužiť neprimerané oneskorenie.	Vplyv na rôzne riziká
TR111	Útočník môže upraviť predtým nainštalovanú legitímnu inštanciu peňaženky a pridať do nej škodlivé funkcie.	Vplyv na rôzne riziká
TR112	Útočník môže upraviť legitímnu inštanciu peňaženky a ponúknuť ju používateľom ako legitímnu.	Vplyv na rôzne riziká
TR113	Útočník môže premôcť samotný mechanizmus autentifikácie používateľa, aby obišiel autentifikáciu používateľa peňaženky.	Vplyv na rôzne riziká
TR114	Útočník môže počas nasadenia peňaženky do zariadenia používateľa vložiť do jej kódu škodlivý kód alebo zadné dvierka.	Vplyv na rôzne riziká
TR115	Útočník môže počas vývoja peňaženky vložiť do jej kódu škodlivý kód alebo zadné dvierka.	Vplyv na rôzne riziká
TR116	Útočník môže neoprávnene manipulovať s generovaním náhodných čísel a znížiť ich entropiu natoľko, aby umožnil útoky.	Vplyv na rôzne riziká

ID *Identifikátor*	Opis hrozby *Opis zistenej hrozby (')*	Názov rizika *Súvisiace riziká*
TR117	Útočník môže manipulovať so zariadeniami používateľov v dodávateľskom reťazci tak, aby obsahovali kód alebo konfigurácie, ktoré nespĺňajú podmienky používania peňaženky.	Vplyv na rôzne riziká
TR118	Útočník môže aktivovať jednotku peňaženky, pričom používa sfalšované zariadenie WSCD kontrolované útočníkmi.	Vplyv na rôzne riziká
TR119	Útočník môže čítať informácie odoslané do aplikácie WSCA a/alebo zariadenia WSCD.	Vplyv na rôzne riziká
TR120	Útočník môže do aplikácie WSCA odoslať ľubovoľné informácie.	Vplyv na rôzne riziká
TR121	Útočník môže ukradnúť informácie zachytením výmeny medzi aplikáciou WSCA a zariadením WSCD.	Vplyv na rôzne riziká
TR122	Útočník môže do zariadenia WSCD odoslať ľubovoľné informácie.	Vplyv na rôzne riziká
TR123	Útočník môže odoslať informácie do zariadenia WSCD, čím obíde aplikáciu WSCA.	Vplyv na rôzne riziká
TR124	Útočník môže pomocou phishingu naviesť používateľov do falošnej webovej aplikácie na správu peňaženky a PID.	Vplyv na rôzne riziká
TR125	Útočník môže nahradiť kľúče peňaženky inými kľúčmi a vytvoriť tak správy, ktoré sa použijú pri inom útoku.	Vplyv na rôzne riziká
TR126	Útočník môže zmeniť alebo zničiť kľúče peňaženky, čím sa niektoré funkcie peňaženky stanú nepoužiteľnými.	Vplyv na rôzne riziká
TR127	Útočník môže ovládať škodlivý softvér na prístup k údajom uloženým v peňaženke.	Vplyv na rôzne riziká
TR128	Útočník môže získať prístup k dôkazom vygenerovaným v peňaženke.	Vplyv na rôzne riziká
TR129	Poskytovatelia peňaženky môžu získať prístup k objektom v peňaženke.	Vplyv na rôzne riziká
TR130	Poskytovatelia peňaženky môžu získať prístup k dôkazom vygenerovaným v peňaženke.	Vplyv na rôzne riziká
TR131	Útočník môže ukradnúť odomknuté zariadenie peňaženky.	Vplyv na rôzne riziká
TR132	Útočník môže manipulovať so systémom tak, aby zabránil zaznamenávaniu určitých udalostí.	Vplyv na rôzne riziká
TR133	Útočník môže zachytiť komunikáciu medzi inštanciou peňaženky a aplikáciou WSCA alebo prehrať/imitovať používateľa (napr. zneužitím mechanizmu autentifikácie).	Vplyv na rôzne riziká

PRÍLOHA II

KRITÉRIÁ NA POSÚDENIE PRIJATEĽNOSTI INFORMÁCIÍ O ZABEZPEČENÍ

Názov	Predmet	Body, ktorým treba venovať pozornosť
EUCC	Výrobky IKT	O vydavateľovi: žiadne (akreditované certifikačné orgány) O rozsahu pôsobnosti: — Skontrolovať profil ochrany a cieľ zabezpečenia — Skontrolovať úroveň zabezpečenia hodnotenia a rozšírenia O zabezpečení: — Skontrolovať obmedzenia v používateľskej dokumentácii — V prípade zloženia sa môže vyžadovať prístup k hodnotiacej technickej správe
EUCS (ak je k dispozícii)	Cloudové služby	O vydavateľovi: žiadne (akreditované certifikačné orgány) O rozsahu pôsobnosti: — Skontrolovať opis cloudovej služby — Skontrolovať úroveň hodnotenia a profily rozšírenia O zabezpečení: — Skontrolovať informácie o transparentnosti a v prípade potreby informácie o zložení
Systémy Common Criteria (spoločné kritériá) prevádzkované v EÚ vrátane systémov SOG-IS	Výrobky IKT	O vydavateľovi: žiadne (členské štáty) O rozsahu pôsobnosti: — Skontrolovať profil ochrany a cieľ zabezpečenia — Skontrolovať úroveň zabezpečenia hodnotenia a rozšírenia O zabezpečení: — Skontrolovať obmedzenia v používateľskej dokumentácii — V prípade zloženia sa môže vyžadovať prístup k hodnotiacej technickej správe
EN 17640:2018 (FITCEM vrátane CSPN, BSZ, LINCE, BSZA)	Výrobky IKT	O vydavateľovi: — Skontrolovať schému a požiadavky na certifikačné orgány O rozsahu pôsobnosti: — Skontrolovať opis výrobku — Skontrolovať bezpečnostné vyhlásenia — Skontrolovať úroveň zabezpečenia O zabezpečení: — Skontrolovať vykonané činnosti a zistenia v správe
Schémy certifikácie zariadení na vyhotovenie kvalifikovaného podpisu v súlade s článkom 30 nariadenia (EÚ) č. 910/2014	QSCD	O vydavateľovi: — Skontrolovať schému a požiadavky na certifikačné orgány O rozsahu pôsobnosti: — Skontrolovať opis výrobku — Skontrolovať bezpečnostné vyhlásenia — Skontrolovať úroveň zabezpečenia O zabezpečení: — Skontrolovať vykonané činnosti

Názov	Predmet	Body, ktorým treba venovať pozornosť
EN ISO/IEC 27001:2022	ISMS	O vydavateľovi: žiadne (akreditované certifikačné orgány) O rozsahu pôsobnosti: — Skontrolovať opis systému riadenia — Skontrolovať vyhlásenie o uplatniteľnosti O zabezpečení: — Skontrolovať vykonané činnosti
SOC2	Organizácie	O vydavateľovi: — Skontrolovať ich štatút certifikovaného účtovníka O rozsahu pôsobnosti: — Skontrolovať vyhlásenie o riadení a opis kontrol — Skontrolovať vyhlásenie o uplatniteľnosti O zabezpečení: — Skontrolovať zistenia v správe — V prípade potreby skontrolovať preklenovacie listy
MDSCert (GSMA) (ak je k dispozícii)	Mobilné zariadenia	O vydavateľovi: — Skontrolovať požiadavky na certifikačné orgány O rozsahu pôsobnosti: — Skontrolovať úroveň bezpečnosti zabezpečenia — Skontrolovať požiadavky schémy O zabezpečení: — Skontrolovať činnosti a zistenia v správe
Ostatné schémy	Akýkoľvek komponent	O schéme: — Skontrolovať relevantnosť a ustanovenia schémy O vydavateľovi: — Skontrolovať požiadavky na certifikačné orgány O rozsahu pôsobnosti: — Skontrolovať požiadavky schémy — Skontrolovať bezpečnostný cieľ alebo podobný dokument opisujúci funkčné požiadavky na bezpečnosť a požiadavky na zabezpečenie — Skontrolovať opis produktu a vybrané funkčné požiadavky na bezpečnosť O zabezpečení: — Skontrolovať činnosti a zistenia v správe

PRÍLOHA III

FUNKČNÉ POŽIADAVKY NA RIEŠENIA PEŇAŽENKY

Podľa článku 5a ods. 4, 5, 8 a 14 nariadenia (EÚ) č. 910/2014 funkčné kritériá, ktoré musí spĺňať certifikované riešenie peňaženky a schéma elektronickej identifikácie, na základe ktorej sa poskytuje, zahŕňajú funkčné požiadavky na operácie uvedené vo:

1. vykonávacom nariadení Komisie (EÚ) 2024/2979 ([1]), ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o integritu a základné funkcie;
2. vykonávacom nariadení Komisie (EÚ) 2024/2982 ([2]), 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;
3. vykonávacom nariadení Komisie (EÚ) 2024/2977 ([3]), 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.

([1]) 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 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) 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 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/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).

PRÍLOHA IV

METÓDY A POSTUPY HODNOTIACICH ČINNOSTÍ

1. **Audit realizácie riešenia peňaženky**

Činnosť posudzovania zhody pozostáva z výberu konkrétnych hodnotiacich činností.

Vo vnútroštátnych schémach certifikácie sa špecifikuje hodnotiaca činnosť na posúdenie poskytnutých informácií, ktorá zahŕňa aspoň tieto aspekty:

a) analýza poskytnutých informácií s cieľom potvrdiť, že sú vhodné pre jednu z architektúr špecifikovaných vo vnútroštátnych schémach certifikácie;

b) analýza pokrytia rizík a hrozieb kybernetickej bezpečnosti uvedených v registri rizík v prílohe I opísanými bezpečnostnými kontrolami.

Analýza uvedená v písmenách a) až b) sa opiera o logické dôvody a odôvodnenie poskytnuté poskytovateľom peňaženky.

2. **Hodnotiace činnosti súvisiace so zabezpečeným kryptografickým zariadením peňaženky**

1. Nevyžaduje sa, aby boli kritické operácie vrátane kryptografických výpočtov plne implementované v zariadení WSCD. Časť implementovaná v zariadení WSCD, keď funguje ako súčasť riešenia peňaženky, však musí zaručiť ochranu kritických operácií, ktoré vykonáva, pred útokmi útočníkov s vysokým potenciálom útoku v súlade s vykonávacím nariadením Komisie (EÚ) 2015/1502 ([1]).

2. Zariadenie WSCD alebo jeho časť môže byť predmetom certifikácie, ak ho poskytne držiteľ certifikátu alebo žiadateľ, alebo mimo jeho rozsahu, ak je zabudované do zariadenia poskytnutého koncovým používateľom. Vo vnútroštátnych schémach certifikácie sa okrem toho špecifikujú hodnotiace činnosti na overenie vhodnosti zariadenia WSCD v týchto dvoch prípadoch:

   a) ak aplikácia WSCA závisí od konkrétneho zariadenia WSCD (t. j. ak ju treba hodnotiť ako zložený produkt založený na zariadení WSCD), potom sa pri hodnotení aplikácie WSCA vyžaduje prístup k doplňujúcim informáciám súvisiacim s certifikáciou zariadenia WSCD, najmä vrátane jeho hodnotiacej technickej správy;

   b) ak sa v rámci architektúry zvažovanej v schéme používa niekoľko zariadení WSCD alebo ak sa niektoré operácie s kritickými aktívami vykonávajú mimo zariadenia WSCD, potom vnútroštátne schémy certifikácie zahŕňajú hodnotiace činnosti, aby sa zabezpečilo, že celkové riešenie ponúka očakávanú úroveň bezpečnosti.

3. Nevyhnutným predpokladom certifikácie v rámci vnútroštátnych schém certifikácie je, že zariadenie WSCD sa posúdi podľa požiadaviek úrovne zabezpečenia „vysoká“, ako je stanovené vo vykonávacom nariadení (EÚ) 2015/1502.

   a) Ak sú splnené podmienky uvedené v článku 3 ods. 3 písm. b), hodnotenie zariadenia WSCD alebo jeho časti zahŕňa posúdenie zraniteľnosti podľa normy EN ISO/IEC 15408-3:2022 na úrovni AVA_VAN.5, ako sa uvádza v prílohe I k vykonávaciemu nariadeniu Komisie (EÚ) 2024/482 ([2]), pokiaľ certifikačný orgán riadne neodôvodní, že bezpečnostné charakteristiky aplikácie WSCA umožňujú použiť nižšiu úroveň posúdenia pri zachovaní rovnakej celkovej úrovne zabezpečenia „vysoká“, ako sa uvádza vo vykonávacom nariadení (EÚ) 2015/1502.

([1]) Vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Ú. v. EÚ L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([2]) Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskeho systému certifikácie kybernetickej bezpečnosti založeného na spoločných kritériách (EUCC) (Ú. v. EÚ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

4. Okrem toho v dokumentácii týkajúcej sa každej konkrétnej architektúry vnútroštátne schémy certifikácie formulujú predpoklady pre toto hodnotenie zariadenia WSCD, na základe ktorých možno zabezpečiť odolnosť voči útočníkom s vysokým potenciálom útoku v súlade s vykonávacím nariadením (EÚ) 2015/1502, a špecifikujú hodnotiace činnosti na potvrdenie týchto predpokladov a na potvrdenie po vydaní certifikátu, že predpoklady sú stále overené. Vo vnútroštátnych schémach sa tiež vyžaduje, aby kandidáti na certifikáciu spresnili tieto predpoklady pre ich špecifickú realizáciu a opísali opatrenia zavedené na zaručenie overenia predpokladov počas celého životného cyklu certifikácie.

5. Vnútroštátne schémy certifikácie vo všetkých prípadoch zahŕňajú hodnotiacu činnosť s cieľom overiť, či sú informácie o zabezpečení, ktoré sú k dispozícii pre zariadenie WSCD, vhodné na účely riešenia peňaženky, a to prostredníctvom analýzy informácií o zabezpečení, ako je bezpečnostný cieľ pre certifikáty EUCC vrátane týchto činností:

   a) overenie, či je rozsah hodnotenia vhodný, čo napríklad v prípade certifikátov EUCC znamená overenie, či bezpečnostný cieľ potvrdzuje súlad s jedným z profilov ochrany odporúčaných v EUCC;

   b) overenie, či sú predpoklady o operačnom prostredí zlučiteľné s riešením peňaženky, čo napríklad v prípade certifikátov EUCC znamená, že tieto predpoklady možno nájsť v bezpečnostnom cieli;

   c) overenie, že odporúčania v používateľskej príručke alebo dokumentácii sú zlučiteľné s podmienkami, za ktorých sa má zariadenie WSCD používať v riešení peňaženky;

   d) overenie, či sú predpoklady týkajúce sa zariadenia WSCD uvedené vo vnútroštátnej schéme certifikácie overené a zahrnuté v informáciách o zabezpečení.

6. V prípadoch, keď niektoré overenia nie sú úplne presvedčivé, sa vo vnútroštátnych schémach certifikácie vyžaduje, aby certifikačné orgány špecifikovali kompenzačné požiadavky na zabezpečenú kryptografickú aplikáciu peňaženky (WSCA) založenú na zariadení WSCD, ktoré sa majú zahrnúť do hodnotenia aplikácie WSCA. Ak to nie je možné, vnútroštátne schémy certifikácie budú považovať zariadenie WSCD za nevyhovujúce, čo znamená, že riešeniu peňaženky sa nevydá certifikát zhody.

3. **Hodnotiace činnosti súvisiace so zabezpečenou kryptografickou aplikáciou peňaženky (WSCA)**

1. Vo vnútroštátnych schémach certifikácie sa vyžaduje, aby sa aplikácia WSCA ako súčasť riešenia peňaženky hodnotila podľa požiadaviek minimálnej úrovne zabezpečenia „vysoká“, ako je stanovené vo vykonávacom nariadení (EÚ) 2015/1502.

2. Toto hodnotenie obsahuje posúdenie zraniteľnosti podľa normy EN ISO/IEC 15408-3:2022 na úrovni AVA_VAN.5, ako sa uvádza v prílohe I k vykonávaciemu nariadeniu (EÚ) 2024/482, pokiaľ certifikačný orgán riadne neodôvodní, že bezpečnostné charakteristiky aplikácie WSCA umožňujú použiť nižšiu úroveň posúdenia pri zachovaní rovnakej celkovej úrovne zabezpečenia „vysoká“, ako sa uvádza vo vykonávacom nariadení (EÚ) 2015/1502.

3. Ak WSCA neposkytuje poskytovateľ peňaženky, vnútroštátne schémy certifikácie formulujú predpoklady pre toto hodnotenie zariadenia WSCA, na základe ktorých možno zabezpečiť odolnosť voči útočníkom s vysokým potenciálom útoku v súlade s vykonávacím nariadením Komisie (EÚ) 2015/1502, a špecifikujú hodnotiace činnosti na potvrdenie týchto predpokladov a na potvrdenie po vydaní certifikátu, že predpoklady sú stále overené. Vo vnútroštátnych schémach sa tiež vyžaduje, aby kandidáti na certifikáciu spresnili tieto predpoklady pre ich špecifickú realizáciu a opísali opatrenia zavedené na zaručenie overenia predpokladov počas celého životného cyklu certifikácie.

4. Vnútroštátne schémy certifikácie vo všetkých prípadoch zahŕňajú hodnotiacu činnosť s cieľom overiť, či sú informácie o zabezpečení, ktoré sú k dispozícii pre aplikáciu WSCA, vhodné na účely riešenia peňaženky, a to prostredníctvom analýzy informácií o zabezpečení, ako je bezpečnostný cieľ pre certifikáty EUCC vrátane týchto činností:

   a) overenie, či je rozsah hodnotenia vhodný, čo napríklad v prípade certifikátov EUCC znamená overenie, či bezpečnostný cieľ potvrdzuje súlad s jedným z profilov ochrany odporúčaných v EUCC;

   b) overenie, či sú predpoklady o operačnom prostredí zlučiteľné s riešením peňaženky, čo napríklad v prípade certifikátov EUCC znamená, že tieto predpoklady možno nájsť v bezpečnostnom cieli;

c) overenie, že odporúčania v používateľskej príručke alebo dokumentácii sú zlučiteľné s podmienkami, za ktorých sa má aplikácia WSCA používať v riešení peňaženky;

d) overenie, či sú predpoklady týkajúce sa aplikácie WSCA uvedené vo vnútroštátnej schéme certifikácie overené a zahrnuté v informáciách o zabezpečení.

5. Vo vnútroštátnych schémach certifikácie sa vyžaduje, aby hodnotenie aplikácie WSCA zahŕňalo všetky bezpečnostné kontroly vykonávané touto aplikáciou WSCA.

4. **Hodnotiace činnosti týkajúce sa zariadenia koncového používateľa**

Keďže v registri rizík, ako sa uvádza v prílohe I k tomuto nariadeniu, sa identifikujú riziká, ktoré priamo súvisia s bezpečnosťou zariadenia koncového používateľa, vo vnútroštátnych schémach certifikácie sa špecifikujú bezpečnostné požiadavky na zariadenia koncového používateľa. Keďže však tieto zariadenia poskytuje koncový používateľ, a nie poskytovateľ peňaženky, na tieto požiadavky sa budú vzťahovať predpoklady.

Riešenie peňaženky musí ku každému predpokladu zahŕňať mechanizmus, ktorým sa pri každej jednotke peňaženky overí, či príslušné zariadenie koncového používateľa daný predpoklad spĺňa. Takéto mechanizmy sa považujú za bezpečnostné kontroly a sú zahrnuté do hodnotiacich činností, aby sa preukázala ich vhodnosť a účinnosť na príslušnej úrovni zabezpečenia.

Ďalej sú uvedené dva príklady:

a) zariadenie koncového používateľa môže obsahovať certifikované zariadenie WSCD, čo je potrebné preukázať. Typicky by sa to uskutočnilo použitím kryptografického mechanizmu na overenie, či je v certifikovanom zariadení WSCD prítomné kryptografické tajomstvo, ktoré je dostupné iba v certifikovanom zariadení WSCD. V tomto prípade by sa toto kryptografické tajomstvo malo považovať za kritické aktívum a mala by sa naň vzťahovať certifikácia zariadenia WSCD a/alebo aplikácie WSCA;

b) typickou požiadavkou pre zariadenia koncového používateľa by bolo, že zariadenia musia dostávať bezpečnostné aktualizácie. Keďže táto požiadavka súvisí s inštanciou peňaženky, na mechanizmus používaný na overenie dostupnosti bezpečnostných aktualizácií sa musia vzťahovať iba hodnotiace činnosti na úrovni zabezpečenia vhodné pre danú inštanciu peňaženky, najmä preto, že bude pravdepodobne integrovaný do inštancie peňaženky.

5. **Hodnotiace činnosti týkajúce sa inštancie peňaženky**

1. Pri hodnotení inštancie peňaženky sa zohľadnia tieto dve hlavné výzvy:

   a) inštancia peňaženky bude pravdepodobne existovať v súbore variantov tej istej základnej aplikácie, pričom každý variant sa bude špecializovať na určitú kategóriu zariadení koncového používateľa;

   b) rôzne varianty inštancie peňaženky budú pravdepodobne potrebovať časté aktualizácie, aby bolo možné sledovať vývoj základnej bezpečnostnej platformy, napríklad pri zistení zraniteľností, ktoré si vyžadujú zmeny v aplikáciách.

2. Pri hodnotení inštancie peňaženky sa musia zohľadňovať tieto špecifické výzvy. Jedným z priamych dôsledkov je, že rámec spoločných kritérií nemusí byť vhodný vo všetkých prípadoch. Preto sa v prípade potreby zvážia alternatívne metodiky hodnotenia. V rámci vnútroštátnych schém certifikácie sa zváži používanie metodiky EN 17640:2018 v týchto prípadoch:

   a) ako súčasť samotnej schémy;

   b) prostredníctvom vnútroštátnych schém založených na metodike;

   c) prostredníctvom vnútroštátnych schém založených na podobných zásadách, ale vytvorených pred vypracovaním metodiky EN 17640:2018.

3. Okrem toho, keďže vykonávanie úplného špecializovaného hodnotenia každého variantu môže mať obmedzenú pridanú hodnotu, v rámci vnútroštátnych schém certifikácie sa zváži špecifikovanie kritérií umožňujúcich výber vzorky, aby sa predišlo opakovaniu rovnakých hodnotiacich činností a aby sa zaistilo zameranie na činnosti, ktoré sú špecifické pre daný variant. V rámci vnútroštátnych schém certifikácie sa od všetkých certifikačných orgánov vyžaduje, aby používanie výberu vzorky zdôvodnili.

4. Vnútroštátne schémy certifikácie zahŕňajú aktualizácie inštancie peňaženky v celkovom procese riadenia zmien špecifikovanom pre riešenie peňaženky. Stanovia tiež pravidlá o postupoch, ktoré musí vykonať poskytovateľ peňaženky pri každej aktualizácii (napr. analyzovanie vplyvu zmien na bezpečnostné kontroly), a o hodnotiacich činnostiach, ktoré má vykonať certifikačný orgán pri aktualizáciách podľa špecifikovaných podmienok (napr. posúdenie prevádzkovej účinnosti upravenej bezpečnostnej kontroly). Proces riadenia zmien je jedným z procesov, ktorých prevádzkovú účinnosť je potrebné každoročne kontrolovať v súlade s článkom 18 ods. 3.

6. **Hodnotiace činnosti súvisiace so službami a procesmi využívanými pri poskytovaní a prevádzke riešenia peňaženky**

1. Na hodnotenie služieb a procesov, ktoré zohrávajú úlohu pri poskytovaní a prevádzke riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, hodnotiaci tím zhromažďuje dôkazy vykonávaním hodnotiacich činností, ktoré môžu zahŕňať činnosti auditu, kontroly, overovania a validácie.

2. Certifikačný orgán potvrdí dostatočnosť a vhodnosť dôkazov, ktoré poskytujú dostatočné uistenie, že služby a procesy spĺňajú certifikačné požiadavky, a to potvrdením:

   a) presnosti informácií uvedených v opise procesov a služieb;

   b) vhodnosti návrhu a kontrol procesov a služieb na splnenie hodnotiacich kritérií;

   c) prevádzkovej účinnosti vykonávania týchto kontrol počas stanoveného obdobia pred hodnotením.

3. Presnosť opisu a prevádzkovú účinnosť vykonávania kontrol možno považovať za ciele overovania príslušných tvrdení poskytovateľa peňaženky (t. j. potvrdenie spravodlivosti udalostí, ktoré už nastali, alebo výsledkov, ktoré sa už dosiahli) v zmysle normy ISO/IEC 17000:2020, zatiaľ čo vhodnosť návrhu a kontrol služieb a procesov na splnenie kritérií hodnotenia možno považovať za cieľ validácie príslušného tvrdenia poskytovateľa peňaženky v zmysle normy ISO/IEC 17000:2020 (t. j. potvrdenie hodnovernosti, pokiaľ ide o zamýšľané budúce použitie alebo predpokladaný výsledok).

4. Vzhľadom na to, že riešenie peňaženky nemôže fungovať pred certifikáciou, prevádzkovú účinnosť nemožno potvrdiť na základe skutočnej prevádzky riešenia. Preto sa to musí potvrdiť pomocou dôkazov získaných počas skúšok alebo pilotnej prevádzky.

5. Pre určité špecifické služby a procesy už môžu existovať vnútroštátne schémy certifikácie, napríklad pre registráciu používateľov. Vnútroštátne schémy certifikácie zvážia využitie takýchto schém, ak je to vhodné.

7. **Hodnotiace činnosti súvisiace so službami IKT využívanými pri poskytovaní a prevádzke riešenia peňaženky**

1. Niektoré architektúry peňaženky sa môžu pri poskytovaní a prevádzke riešenia peňaženky spoliehať na špecializované služby IKT vrátane cloudových služieb a tieto služby môžu poskytovať hosting pre citlivé údaje, ako aj citlivé operácie. V takom prípade sa vo vnútroštátnych schémach certifikácie špecifikujú bezpečnostné požiadavky pre tieto služby IKT.

2. Existuje už mnoho schém certifikácie pre služby IKT, cloudové služby a iné zdroje informácií o zabezpečení vrátane tých, ktoré sú uvedené v prílohe II. Vnútroštátne schémy certifikácie sa opierajú o tieto existujúce mechanizmy, ak sú dostupné a uplatniteľné, prostredníctvom jedného z týchto mechanizmov:

   a) zavedie sa povinné používanie konkrétnej schémy alebo výberu schém špecifikovaním podmienok, za ktorých sa majú služby IKT alebo cloudové služby posudzovať pomocou týchto schém;

   b) výber posúdenia sa ponechá na poskytovateľovi peňaženky a využije sa činnosť analýzy závislostí, pomocou ktorej sa zanalyzuje vhodnosť informácií o zabezpečení získaných prostredníctvom týchto posúdení.

3. V oboch prípadoch musia vnútroštátne schémy certifikácie špecifikovať dodatočné hodnotiace činnosti potrebné na analýzu alebo doplnenie informácií získaných prostredníctvom týchto schém.

PRÍLOHA V

ZOZNAM VEREJNE DOSTUPNÝCH INFORMÁCIÍ O PEŇAŽENKÁCH

1. Informácie, ktoré sa zverejňujú podľa článku 8 ods. 5, obsahujú aspoň tieto informácie:

   a) akékoľvek obmedzenia používania riešenia peňaženky;

   b) usmernenia a odporúčania poskytovateľa peňaženky na pomoc koncovým používateľom s bezpečnou konfiguráciou, inštaláciou, nasadením, prevádzkou a údržbou peňaženiek;

   c) obdobie, počas ktorého sa bude koncovým používateľom poskytovať bezpečnostná podpora, a to najmä pokiaľ ide o dostupnosť aktualizácií, ktoré sa týkajú kybernetickej bezpečnosti;

   d) kontaktné informácie výrobcu alebo poskytovateľa a akceptované metódy na prijímanie informácií o zraniteľnosti od koncových používateľov a výskumných pracovníkov v oblasti bezpečnosti;

   e) odkaz na online archívy so zoznamom verejne dostupných zraniteľností súvisiacich s peňaženkami a na akékoľvek relevantné upozornenia týkajúce sa kybernetickej bezpečnosti.

2. Informácie uvedené v odseku 1 sa sprístupnia jasným, komplexným a ľahko dostupným spôsobom na verejne prístupnom mieste každej osobe, ktorá chce použiť riešenie peňaženky.

PRÍLOHA VI

METODIKA POSÚDENIA PRIJATEĽNOSTI INFORMÁCIÍ O ZABEZPEČENÍ

1. **Posúdenie dostupnosti dokumentácie o zabezpečení**

Hodnotitelia vypracujú zoznam dokumentácie o zabezpečení pre každý príslušný komponent riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje. Hodnotitelia potom posúdia celkovú relevantnosť každej dokumentácie o zabezpečení pre preskúmanie závislosti.

Pri analýze sa berú do úvahy tieto aspekty:

1. o samotnej dokumentácii o zabezpečení:

   a) typ dokumentácie o zabezpečení so všetkými požadovanými podrobnosťami,

      (príkladmi takýchto dokumentov sú certifikáty zhody podľa normy EN ISO/IEC 27001:2022 alebo typu 1 alebo typu 2 pre správy ISAE);

   b) zahrnuté obdobie alebo obdobie platnosti,

      [toto obdobie môže byť doplnené preklenovacím listom (dokument pokrývajúci časové obdobie medzi dátumom ukončenia vykazovaného obdobia aktuálnej správy ISAE a vydaním novej správy ISAE) alebo podobným vyhlásením];

   c) platný rámec (napr. existujúca norma);

   d) či dokumentácia o zabezpečení obsahuje mapovanie podľa požiadaviek schémy;

2. o odbornej spôsobilosti a nestrannosti vydavateľa správy o zabezpečení:

   a) názov certifikačného orgánu a, ak je k dispozícii, meno hlavného hodnotiteľa;

   b) dôkazy o spôsobilosti certifikačného orgánu a hodnotiteľa (napr. akreditácia, osobná certifikácia atď.);

   c) dôkaz o nestrannosti certifikačného orgánu a hodnotiteľa (napr. akreditácia atď.).

2. **Posudzovanie zabezpečenia súvisiaceho s individuálnymi požiadavkami**

Hodnotitelia overia, či možno na základe dostupnej dokumentácie o zabezpečení vzťahujúcej sa na riešenie peňaženky a schému elektronickej identifikácie, v rámci ktorej sa poskytuje, primerane určiť, že riešenie peňaženky spĺňa očakávania týkajúce sa individuálnych požiadaviek schémy certifikácie.

Toto posúdenie sa vykoná v prípade každého relevantného komponentu riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje, sformulovaním predpokladu o bezpečnostných kontrolách riešenia peňaženky.

Pri každom takomto predpoklade hodnotiaci tím určí, či je zabezpečenie uvedené v dostupnej dokumentácii o zabezpečení primerané alebo nie.

Záver o primeranosti zabezpečenia sa zakladá na týchto aspektoch:

1. požadované informácie sú v dokumentácii o zabezpečení dostupné s očakávanou úrovňou zabezpečenia;

2. informácie dostupné v dokumentácii o zabezpečení nepokrývajú celý rozsah požiadavky, ale dodatočné kontroly alebo kompenzačné kontroly (t. j. interné kontroly, ktoré znižujú riziko existujúceho alebo potenciálneho nedostatku v kontrole) implementované v riešení peňaženky alebo v schéme elektronickej identifikácie, v rámci ktorej sa poskytuje, umožňujú hodnotiteľom určiť, či sú informácie primerané;

3. informácie dostupné v dokumentácii o zabezpečení neponúkajú očakávanú úroveň zabezpečenia, ale kontroly implementované na posúdenie a monitorovanie poskytovateľa peňaženky umožňujú hodnotiteľom určiť, či sú informácie primerané;
4. ak sa v dokumentácii o zabezpečení uvádzajú prvky nesúladu v návrhu alebo implementácii kontrol uplatnených s cieľom splniť predpoklad, nápravné opatrenia navrhnuté a implementované poskytovateľom peňaženky a preskúmané jeho hodnotiteľmi musia byť primerané, aby zaručili, že daný predpoklad je skutočne splnený.

PRÍLOHA VII

OBSAH CERTIFIKÁTU ZHODY

1. Jedinečný identifikátor pridelený certifikačným orgánom, ktorý vydáva certifikát zhody.

2. Informácie týkajúce sa certifikovaného riešenia peňaženky a schém elektronickej identifikácie, v rámci ktorých sa poskytuje, a o držiteľovi certifikátu zhody vrátane:
   a) názvu riešenia peňaženky;
   b) názvu schém elektronickej identifikácie, v rámci ktorých sa dané riešenie peňaženky poskytuje;
   c) verzie riešenia peňaženky, ktorá bola hodnotená;
   d) mena/názvu, adresy a kontaktných údajov držiteľa certifikátu zhody;
   e) odkazu na webové sídlo držiteľa certifikátu zhody s informáciami, ktoré sa musia zverejniť.

3. Informácie týkajúce sa hodnotenia a certifikácie riešenia peňaženky a schém elektronickej identifikácie, v rámci ktorých sa poskytuje, vrátane:
   a) názvu, adresy a kontaktných údajov certifikačného orgánu, ktorý vydal certifikát zhody;
   b) ak sa líši od certifikačného orgánu, názvu orgánu posudzovania zhody, ktorý hodnotenie vykonal, spolu s informáciou o jeho akreditácii;
   c) mena/názvu vlastníka schémy;
   d) odkazu na nariadenie (EÚ) č. 910/2014 a na toto nariadenie;
   e) odkazu na certifikačnú správu súvisiacu s certifikátom zhody;
   f) odkazu na správu o posúdení certifikácie súvisiacu s certifikátom zhody;
   g) odkazu na normy použité na hodnotenie vrátane ich verzií;
   h) dátumu vydania certifikátu zhody;
   i) obdobia platnosti certifikátu zhody.

PRÍLOHA VIII

OBSAH VEREJNEJ CERTIFIKAČNEJ SPRÁVY A SPRÁVY O POSÚDENÍ CERTIFIKÁCIE

1. Verejná certifikačná správa musí obsahovať aspoň tieto aspekty:
   a) zhrnutie;
   b) identifikáciu riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje;
   c) opis riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa poskytuje;
   d) bezpečnostné informácie, ktoré sa majú zverejniť, ako je opísané v prílohe V, alebo odkaz na tieto informácie;
   e) zhrnutie predbežného plánu auditu a validácie;
   f) zhrnutie preskúmania a rozhodnutia o certifikácii.

2. Správa o posúdení certifikácie obsahuje aspoň:
   a) opis návrhu riešenia peňaženky, systému identifikácie a procesu registrácie spolu s posúdením rizika a konkrétnym plánom validácie;
   b) opis toho, ako riešenie peňaženky spĺňa požiadavky na úroveň zabezpečenia „vysoká“ a ako to preukazujú výsledky posúdenia certifikácie riešenia peňaženky vykonaného v súlade s týmto nariadením;
   c) opis výsledku posúdenia zhody riešenia peňaženky a schémy elektronickej identifikácie, v rámci ktorej sa príslušné jednotky peňaženky poskytujú, najmä zhody s:
      — požiadavkami stanovenými v článku 5a ods. 4, 5 a 8 nariadenia (EÚ) č. 910/2014,
      — požiadavkami na logické oddelenie stanovené v článku 5a ods. 14 nariadenia (EÚ) č. 910/2014,
      — prípadne s normami a technickými špecifikáciami uvedenými v článku 5a ods. 24 nariadenia (EÚ) č. 910/2014, pričom sa opíše, ako tieto požiadavky súvisia so zodpovedajúcimi normatívnymi požiadavkami stanovenými vo vnútroštátnych schémach certifikácie;
   d) súhrn výsledku plnenia plánu validácie vrátane všetkých zistených nezhôd.

PRÍLOHA IX

HARMONOGRAM POVINNÝCH HODNOTENÍ DOHĽADU

1. V článku 18 sa špecifikujú požiadavky na životný cyklus certifikácie, najmä vykonávanie pravidelných hodnotiacich činností. Tieto činnosti musia obsahovať aspoň:

   a) úplné vyhodnotenie predmetu posudzovania zhody pri počiatočnom hodnotení a pri každom hodnotení na účely opätovnej certifikácie vrátane funkcie aktualizácie akéhokoľvek komponentu výrobku;

   b) posúdenie zraniteľnosti pri počiatočnom hodnotení a pri každom hodnotení na účely opätovnej certifikácie a najmenej každé dva roky pri hodnoteniach dohľadu, ktoré zahŕňa aspoň zmeny v predmete posudzovania zhody a zmeny v prostredí hrozieb od posledného posúdenia zraniteľnosti;

   c) dodatočné činnosti, ako je penetračné testovanie v prípade zvýšenej úrovne rizika alebo objavenia sa nových hrozieb;

   d) hodnotenie prevádzkovej účinnosti procesov údržby aspoň každý rok v rámci hodnotení dohľadu a hodnotení na účely opätovnej certifikácie, ktoré zahŕňa aspoň procesy kontroly verzií, aktualizácie a riadenia zraniteľnosti;

   e) po úspešnom preskúmaní a rozhodnutí o certifikácii, vydanie certifikátu zhody po úvodnom hodnotení a po každom hodnotení na účely opätovnej certifikácie.

2. V tabuľke 1 sa uvádza referenčný harmonogram vychádzajúci zo štvorročného cyklu, pričom:

   a) rok 1 sa začína prvým vydaním certifikátu zhody a

   b) všetky hodnotiace činnosti sa vykonajú do 12 mesiacov od hodnotenia predchádzajúceho roka.

3. Harmonogram uvedený v tabuľke 1 je odporúčaním na zabezpečenie včasnej opätovnej certifikácie a na zabránenie prerušeniam poskytovania riešenia peňaženky. Sú možné aj iné harmonogramy, pokiaľ platnosť certifikátu zhody nepresiahne päť rokov, ako sa stanovuje v článku 5c ods. 4 nariadenia (EÚ) č. 910/2014.

4. Okrem pravidelných hodnotení môže byť na žiadosť certifikačného orgánu alebo držiteľa certifikátu zhody iniciované aj osobitné hodnotenie po významnej zmene predmetu certifikácie alebo prostredia hrozieb.

5. Akékoľvek hodnotenie vrátane hodnotení dohľadu a osobitných hodnotení môže viesť k vydaniu nového certifikátu zhody, najmä v prípade významných zmien predmetu certifikácie, avšak s rovnakým dátumom uplynutia platnosti ako pôvodný certifikát zhody.

Tabuľka 1

Úplný štvorročný cyklus hodnotenia

Čas	Typ hodnotenia	Činnosti
Rok 0	Počiatočné	— Úplné hodnotenie predmetu certifikácie vrátane posúdenia zraniteľnosti — Vrátane funkcie na vykonanie aktualizácií každého softvérového komponentu — Hodnotenie procesov údržby okrem ich prevádzkovej účinnosti — Vydanie certifikátu zhody a začiatok štvorročného cyklu
Rok 1	Dohľad	— Hodnotenie prevádzkovej účinnosti procesov údržby — Minimálne kontrola verzií, aktualizácia, riadenie zraniteľností — Vyhodnotenie zmien, ktoré majú vplyv na bezpečnosť produktu

Čas	Typ hodnotenia	Činnosti
Rok 2	Dohľad	— Posúdenie zraniteľnosti celého riešenia — Hodnotenie prevádzkovej účinnosti procesov údržby — Minimálne kontrola verzií, aktualizácia, riadenie zraniteľností — Vyhodnotenie zmien, ktoré majú vplyv na bezpečnosť produktu
Rok 3	Dohľad	— Hodnotenie prevádzkovej účinnosti procesov údržby — Minimálne kontrola verzií, aktualizácia, riadenie zraniteľností — Vyhodnotenie zmien, ktoré majú vplyv na bezpečnosť produktu
Rok 4	Opätovná certifikácia	1. Úplné hodnotenie predmetu certifikácie vrátane posúdenia zraniteľnosti 2. Zjednodušené hodnotenie funkcií/procesov, ktoré sa nezmenili 3. Vrátane funkcie na vykonanie aktualizácií každého softvérového komponentu 4. Hodnotenie procesov údržby vrátane ich prevádzkovej účinnosti 5. Vydanie nového certifikátu zhody