2024/2981

4.12.2024

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2024/2981

ze dne 28. listopadu 2024,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o certifikaci evropských peněženek digitální identity

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES ([1]), a zejména na čl. 5c odst. 6 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Podle článku 5c nařízení (EU) č. 910/2014 se certifikace evropských peněženek digitální identity (dále jen „peněženky“) provádí v souladu s požadavky na funkčnost, kybernetickou bezpečnost a ochranu údajů, aby byla zajištěna vysoká úroveň bezpečnosti peněženek a důvěry v ně. Tyto požadavky na certifikaci je třeba harmonizovat ve všech členských státech, aby se zabránilo roztříštěnosti trhu a vytvořil se spolehlivý rámec.

(2) Na všechny činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([2]) a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([3]).

(3) Komise pravidelně posuzuje nové technologie, postupy, normy nebo technické specifikace. V zájmu zajištění co nejvyšší úrovně harmonizace mezi členskými státy při vývoji a certifikaci peněženek se technické specifikace stanovené v tomto nařízení opírají o práci provedenou na základě doporučení Komise (EU) 2021/946 ze dne 3. června 2021 o společném souboru nástrojů Unie pro koordinovaný přístup k rámci pro evropskou digitální identitu ([4]), a zejména o architekturu a referenční rámec, který je jeho součástí. V souladu se 75. bodem odůvodnění nařízení Evropského parlamentu a Rady (EU) 2024/1183 ([5]) by Komise měla toto prováděcí nařízení přezkoumat a v případě potřeby aktualizovat, aby bylo v souladu s globálním vývojem, architekturou a referenčním rámcem a aby byly dodržovány osvědčené postupy na vnitřním trhu.

(4) Za účelem potvrzení shody s požadavky na kybernetickou bezpečnost obsaženými v rámci pro certifikaci by se certifikace řešení peněženky měla odvolávat na evropské systémy certifikace kybernetické bezpečnosti zřízené podle nařízení Evropského parlamentu a Rady (EU) 2019/881 ([6]), pokud jsou k dispozici a jsou relevantní. Pokud uvedené systémy neexistují nebo pokud částečně pokrývají požadavky na kybernetickou bezpečnost, stanoví toto nařízení obecné požadavky na vnitrostátní systémy certifikace, které zahrnují požadavky na funkčnost, kybernetickou bezpečnost a ochranu údajů.

([1]) Úř. věst. L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([3]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).
([4]) Úř. věst. L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu (Úř. věst. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).
([6]) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“ (Úř. věst. L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Podle čl. 5a odst. 11 nařízení (EU) č. 910/2014 musí být peněženky certifikovány vůči vysoké úrovni záruky stanovené v nařízení (EU) č. 910/2014, jakož i v prováděcím nařízení Komise (EU) 2015/1502 ([7]). Této úrovně záruky musí dosáhnout celkové řešení peněženky. Podle tohoto nařízení mohou být některé komponenty řešení peněženky certifikovány vůči nižší úrovni záruky, pokud je to řádně odůvodněno a není tím dotčena vysoká úroveň záruky dosažená celkovým řešením.

(6) Všechny vnitrostátní systémy certifikace by měly určit vlastníka systému, který bude odpovědný za vývoj a údržbu systému certifikace. Vlastníkem systému může být subjekt posuzování shody, subjekt nebo orgán veřejné správy, obchodní sdružení, skupina subjektů posuzování shody nebo jakýkoli jiný vhodný subjekt, který může být odlišný od subjektu provozujícího vnitrostátní systém certifikace.

(7) Předmět certifikace by měl zahrnovat softwarové komponenty řešení peněženky, jako je instance peněženky. Bezpečná kryptografická aplikace peněženky (WSCA), bezpečný kryptografický prostředek peněženky (WSCD) a platformy, na kterých jsou tyto softwarové komponenty spuštěny, ačkoli jsou součástí provozního prostředí, by měly být zahrnuty do předmětu certifikace pouze tehdy, pokud je poskytuje řešení peněženky. V ostatních případech, zejména pokud tyto prostředky a platformy poskytují koncoví uživatelé, by poskytovatelé měli stanovit předpoklady o provozním prostředí řešení peněženky, včetně těchto prostředků a platforem, a zavést opatření, která potvrdí, že tyto předpoklady jsou ověřeny v praxi. Aby byla zajištěna ochrana kritických aktiv prostřednictvím hardwaru a systémového softwaru používaného ke správě a ochraně kryptografických klíčů vytvořených, uložených nebo zpracovávaných bezpečnými kryptografickými prostředky peněženky, musí bezpečné kryptografické prostředky peněženky splňovat vysoké standardy certifikace, jak se odrážejí v mezinárodních normách, jako jsou společná kritéria (v rámci systému EUCC), stanovená v prováděcím nařízení Komise (EU) 2024/482 ([8]), a to prostřednictvím hodnocení EAL4 a pokročilé metodické analýzy zranitelnosti, srovnatelné například s AVA_VAN.5. Tyto certifikační normy by měly být použity nejpozději při certifikaci shody peněženek podle evropského systému certifikace kybernetické bezpečnosti přijatého podle nařízení (EU) 2019/881.

(8) Plně mobilní, bezpečné a uživatelsky přívětivé peněženky jsou podporovány dostupností standardizovaných a certifikovaných řešení odolných proti neoprávněné manipulaci, jako jsou vestavěné zabezpečené prvky, externí zařízení jako například čipové karty nebo vestavěné platformy SIM v mobilních zařízeních. U vnitrostátních prostředků a peněženek elektronické identifikace je důležité zajistit včasný přístup k vestavěným zabezpečeným prvkům a koordinovat úsilí členských států v této oblasti. Skupina pro evropskou spolupráci v oblasti digitální identity zřízená podle čl. 46e odst. 1 nařízení (EU) č. 910/2014 (dále jen „skupina pro spolupráci“) by proto měla pro tento účel zřídit specializovanou podskupinu. Po konzultaci s příslušnými zúčastněnými stranami by se tato podskupina měla dohodnout na společném plánu přístupu k vestavěným zabezpečeným prvkům, který má Komise zvážit pro účely zprávy o přezkumu nařízení (EU) č. 910/2014. Aby se usnadnilo zavádění peněženky na vnitrostátní úrovni, měla by Komise dále ve spolupráci s členskými státy vypracovat a průběžně aktualizovat příručku pro případy použití v rámci architektury a referenčního rámce.

(9) Předmětem certifikace vnitrostátních systémů certifikace by měly být také procesy, které se používají k poskytování a provozování řešení peněženky, a to i v případě, že definování nebo provádění těchto procesů jsou zadány třetím stranám. K prokázání toho, že procesy splňují požadavky systémů, lze jako důkaz použít informace o záruce za předpokladu, že se k určení toho, zda jsou informace o záruce dostatečné, použije analýza závislostí. Informace o záruce mají mnoho různých forem, včetně zpráv a certifikátů shody, které mohou být soukromé, vnitrostátní, evropské nebo mezinárodní, založené na normách nebo technických specifikacích. Cílem analýzy závislostí je posoudit kvalitu dostupných informací o záruce vztahujících se ke komponentům peněženky.

([7]) Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (Úř. věst. L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) Prováděcí nařízení Komise (EU) 2024/482 ze dne 31. ledna 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC) (Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Na základě postupů nastavených za tímto účelem by měla mít skupina pro spolupráci možnost vydávat stanoviska a doporučení k návrhům vnitrostátních systémů certifikace, které jí byly předloženy. Tyto vnitrostátní systémy certifikace by měly být specifické pro danou architekturu peněženky a pro každou specifickou podporovanou architekturu by měly existovat specifické profily.

(11) Aby bylo zajištěno společné chápání posuzování nejkritičtějších rizik, která by mohla ovlivnit poskytování a fungování peněženek, a harmonizovaný přístup k jejich posuzování, měl by být vypracován registr rizik a hrozeb, které by měly být zohledněny při navrhování řešení peněženek nezávisle na jejich konkrétní architektuře. Při určování rizik, která by měla být zahrnuta do registru, je třeba mít na paměti cíle kybernetické bezpečnosti popsané v nařízení (EU) č. 910/2014, jako je důvěrnost, integrita a dostupnost řešení peněženky, jakož i ochrana soukromí uživatelů a jejich údajů. Řádné zohlednění rizik a hrozeb zahrnutých do tohoto registru rizik by mělo být součástí požadavků vnitrostátních systémů certifikace. Aby byl registr rizik v souladu s neustále se vyvíjejícím prostředím hrozeb, měl by být v součinnosti se skupinou pro spolupráci udržován a pravidelně aktualizován.

(12) Při vytváření systémů certifikace by vlastníci systémů měli provést posouzení rizik s cílem upřesnit rizika a hrozby uvedené v registru a doplnit je o rizika a hrozby specifické pro architekturu nebo zavádění daného řešení peněženky. Posouzení rizik by mělo zvážit, jak lze příslušná rizika a hrozby vhodně ošetřit. Poskytovatelé peněženek by měli doplnit posouzení rizik systému s cílem určit veškerá rizika a hrozby specifické pro jejich zavádění a navrhnout vhodná opatření pro jejich řešení, která vyhodnotí certifikační subjekt.

(13) Aby bylo možné prokázat, že architektura řešení peněženky splňuje příslušné bezpečnostní požadavky, měl by každý systém nebo profil specifický pro danou architekturu obsahovat alespoň popis architektury řešení peněženky, seznam bezpečnostních požadavků vztahujících se na architekturu daného řešení peněženky, plán hodnocení, který potvrdí, že řešení peněženky založené na této architektuře tyto požadavky splňuje, a posouzení rizik. Vnitrostátní systémy certifikace by měly vyžadovat, aby poskytovatelé peněženek prokázali, jak forma jimi poskytovaného řešení peněženky odpovídá referenční architektuře, a podrobně popsali bezpečnostní kontroly a plány ověřování platnosti pro konkrétní řešení peněženky. Vnitrostátní systémy certifikace by měly rovněž definovat činnost posuzování shody, jejímž účelem je ověřit, zda návrh peněženky řádně odráží referenční architekturu vybraného profilu. Vnitrostátní systémy certifikace by měly splňovat požadavky stanovené v článku 51 nařízení (EU) 2019/881, s výjimkou jeho písmen e) a f) týkajících se zaznamenávání.

(14) Pokud jde o certifikaci produktů, mělo by být umožněno používat certifikáty shody vydané v rámci evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC) a certifikáty shody vydané v rámci vnitrostátních systémů certifikace v kontextu dohody výboru SOG-IS o vzájemném uznávání. Kromě toho by mělo být umožněno používat pro méně citlivé komponenty produktů jiné vnitrostátní systémy certifikace, například systémy vytvořené podle normy CEN EN 17640 pro metodiku hodnocení kybernetické bezpečnosti v rámci pevně stanoveného časového období.

(15) Značka důvěry EU pro peněženku digitální identity (dále jen „značka důvěry“) by měla být používána k jasnému, jednoduchému a rozpoznatelnému označení toho, že peněženka byla poskytnuta v souladu s nařízením (EU) č. 910/2014. Proto by měla být u řešení peněženky certifikovaného v rámci vnitrostátních systémů certifikace považována za značku shody. Vnitrostátní systémy certifikace by neměly definovat žádné další značky shody.

(16) S cílem odradit od podvodů by vnitrostátní systémy certifikace měly definovat opatření, která budou přijata v případě, že bude certifikace v rámci systému požadována podvodně.

(17) Aby byla zajištěna účinná správa oznámení o zranitelnostech, měli by poskytovatelé řešení peněženky a systému elektronické identifikace, v jehož rámci se poskytují, určit a zavést postupy pro hodnocení závažnosti a potenciálního dopadu zranitelností. Vnitrostátní systémy certifikace by měly stanovit prahovou hodnotu, po jejímž překročení je třeba informovat certifikační subjekt. Tímto požadavkem na oznámení by neměla být dotčena kritéria stanovená právními předpisy o ochraně údajů a úřady členských států pro ochranu údajů pro oznamování porušení zabezpečení osobních údajů. Mohly by být vytvořeny případné synergie mezi povinným oznamováním narušení nebo ohrožení řešení peněženky a oznamováním porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679. Posouzením zprávy o analýze dopadu na zranitelnost certifikačním subjektem by nemělo být dotčeno posouzení vlivu na ochranu osobních údajů, které provádí úřad pro ochranu osobních údajů podle článků 35 a 36 nařízení (EU) 2016/679.

(18) Poskytovatelé řešení peněženek a systému elektronické identifikace, v jehož rámci jsou poskytována, by měli vlastníkovi systému oznámit veškerá odůvodnění výjimek z posouzení zranitelnosti požadovaného pro hodnocení bezpečného kryptografického prostředku peněženky a bezpečné kryptografické aplikace peněženky, jak je stanoveno v příloze IV.

(19) Zrušení certifikátu shody může mít závažné důsledky, jako například zneplatnění všech jednotek peněženky v oběhu. Certifikační subjekty by proto měly zvážit zrušení pouze v případě, že neodstraněná zranitelnost může významně ovlivnit spolehlivost řešení peněženky nebo spolehlivost jiného řešení peněženky.

(20) Měl by být zaveden zvláštní proces pro aktualizaci vnitrostátních systémů certifikace, který by umožnil zvládnout přechod mezi po sobě jdoucími verzemi systémů, zejména pokud jde o opatření, která má držitel certifikátu přijmout v souvislosti s nadcházejícími hodnoceními, údržbou, recertifikací a zvláštními hodnoceními.

(21) Pro usnadnění transparentnosti by poskytovatelé peněženek měli veřejně sdílet informace o bezpečnosti svých řešeních peněženky.

(22) Pokud se vnitrostátní systémy certifikace spoléhají na informace o záruce z jiných systémů certifikace nebo zdrojů, měla by být provedena analýza závislostí k ověření toho, že jsou dokumenty o záruce, například zprávy o záruce a certifikáty shody, dostupné a přiměřené pro řešení peněženky a systém elektronické identifikace, v jehož rámci jsou poskytována. Základem této analýzy závislostí by mělo být posouzení rizik řešení peněženky a systému elektronické identifikace, v jehož rámci jsou poskytována. Hodnocení by mělo určit, zda dokumenty o záruce dostupné pro dané řešení peněženky a systém elektronické identifikace, v jehož rámci je poskytováno, jsou dostatečné k poskytnutí záruky odpovídající cílové úrovni hodnocení. Hodnocení by mělo rovněž aktualizovat analýzu závislostí nebo ji v případě potřeby zcela přehodnotit.

(23) Certifikační subjekty by měly vydávat certifikáty shody ve vnitrostátních systémech certifikace spolu s veřejně dostupnou zprávou o certifikaci, jak je uvedeno v čl. 5d odst. 2 písm. a) nařízení (EU) č. 910/2014. Související zpráva o posouzení certifikace by měla být zpřístupněna skupině pro spolupráci.

(24) Vnitrostátní systémy certifikace by měly stanovit každoroční hodnocení dozoru s cílem zajistit efektivní fungování procesů spojených se správou a údržbou peněženek, což znamená, aby fungovaly tak, jak je stanoveno v zásadách vymezujících tyto procesy. Posouzení zranitelnosti každé dva roky je požadavek vyplývající z nařízení (EU) č. 910/2014, který má zajistit, aby řešení peněženky i nadále vhodně krylo kybernetická bezpečnostní rizika a hrozby identifikované v registru rizik, včetně případného vývoje v oblasti hrozeb. Pojmy hodnocení dozoru, hodnocení recertifikace a zvláštní hodnocení by měly být v souladu s normou EN ISO/IEC 17021-1:2015.

(25) Certifikační cyklus končí uplynutím platnosti certifikátu shody nebo vydáním nového certifikátu shody po úspěšném hodnocení recertifikace. Hodnocení recertifikace by mělo zahrnovat hodnocení všech komponentů předmětu certifikace, včetně hodnocení účinnosti a případně posouzení zranitelnosti. Při recertifikaci by mělo být možné znovu použít výsledky předchozích hodnocení komponentů, které se nezměnily.

(26) Po přijetí evropského systému certifikace kybernetické bezpečnosti by vnitrostátní systémy certifikace se stejným rozsahem působnosti měly po uplynutí přechodného období stanoveného v čl. 57 odst. 1 nařízení (EU) 2019/881 přestat vydávat certifikáty.

(27) Vnitrostátní systémy certifikace by se za účelem zajištění harmonizace a interoperability měly opírat o stávající rámce a podle potřeby opakovaně používat důkazy. Členské státy mohou uzavírat dohody o přeshraničním opakovaném použití systémů certifikace nebo jejich částí. Evropská komise a agentura ENISA by měly ruku v ruce se skupinou pro spolupráci podporovat členské státy při vývoji a údržbě jejich vnitrostátních systémů certifikace a zajistit sdílení znalostí a osvědčených postupů.

(28) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([9]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 30. září 2024.

(29) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru uvedeného v čl. 48 odst. 1 nařízení (EU) č. 910/2014,

PŘIJALA TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět a oblast působnosti

Toto nařízení stanoví referenční normy a zavádí specifikace a postupy pro vytvoření spolehlivého rámce pro certifikaci peněženek, který bude pravidelně aktualizován, aby byl v souladu s vývojem technologií a norem a s prací prováděnou na základě doporučení (EU) 2021/946 o společném souboru nástrojů Unie pro koordinovaný přístup k rámci pro evropskou digitální identitu, a zejména s architekturou a referenčním rámcem.

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

1) „řešením peněženky“ kombinace softwaru, hardwaru, služeb, nastavení a konfigurací, včetně instancí peněženky, jedné nebo více bezpečných kryptografických aplikací peněženky a jednoho nebo více bezpečných kryptografických prostředků peněženky;

2) „vlastníkem systému“ organizace, která je odpovědná za vývoj a údržbu systému certifikace;

3) „předmětem certifikace“ produkty, procesy a služby nebo jejich kombinace, na které se vztahují stanovené požadavky;

4) „bezpečnou kryptografickou aplikací peněženky“ aplikace, která spravuje kritická aktiva prostřednictvím propojení s kryptografickými a nekryptografickými funkcemi poskytovanými bezpečným kryptografickým prostředkem peněženky a jejich využívání;

5) „instancí peněženky“ aplikace nainstalovaná a nakonfigurovaná v zařízení nebo prostředí uživatele peněženky, která je součástí jednotky peněženky a kterou uživatel peněženky používá k interakci s jednotkou peněženky;

([9]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6) „bezpečným kryptografickým prostředkem peněženky“ prostředek odolný proti neoprávněné manipulaci, který poskytuje prostředí propojené s bezpečnou kryptografickou aplikací peněženky a používaný touto aplikací k ochraně kritických aktiv a poskytování kryptografických funkcí pro bezpečné provádění kritických operací;

7) „registrem rizik“ záznam informací o zjištěných rizicích, které jsou důležité pro proces certifikace;

8) „poskytovatelem peněženky“ fyzická nebo právnická osoba, která poskytuje řešení peněženky;

9) „certifikačním subjektem“ subjekt pro posouzení shody třetí stranou, který provozuje systémy certifikace;

10) „jednotkou peněženky“ jedinečná konfigurace řešení peněženky, která zahrnuje instance peněženky, bezpečné kryptografické aplikace peněženky a bezpečné kryptografické prostředky peněženky, které poskytovatel peněženky poskytuje jednotlivému uživateli peněženky;

11) „kritickými aktivy“ aktiva v rámci jednotky peněženky nebo ve vztahu k ní, která jsou tak mimořádně důležitá, že ohrožení jejich dostupnosti, důvěrnosti nebo integrity by mělo velmi vážný a oslabující účinek na schopnost spoléhat se na jednotku peněženky;

12) „uživatelem peněženky“ uživatel, který má jednotku peněženky pod kontrolou;

13) „incidentem“ incident ve smyslu čl. 6 bodu 6 směrnice Evropského parlamentu a Rady (EU) 2022/2555 ([10]);

14) „vloženými zásadami zpřístupňování informací“ soubor pravidel, který je součástí elektronického potvrzení atributů jeho poskytovatelem a ve kterém jsou uvedeny podmínky, jež musí strana spoléhající se na peněženku splnit, aby získala přístup k elektronickému potvrzení atributů.

KAPITOLA II

VNITROSTÁTNÍ SYSTÉMY CERTIFIKACE

Článek 3

Zavedení vnitrostátních systémů certifikace

1. Členské státy přidělí vlastníka ke každému vnitrostátnímu systému certifikace.

2. Předmětem certifikace definovaným ve vnitrostátních systémech certifikace je poskytování a fungování řešení peněženky a systémů elektronické identifikace, v jejichž rámci se poskytují.

3. V souladu s prováděcím nařízením (EU) 2015/1502 zahrnuje předmět certifikace ve vnitrostátních systémech certifikace tyto prvky:

a) softwarové komponenty, včetně nastavení a konfigurace řešení peněženky a systému elektronické identifikace, v jehož rámci jsou řešení peněženky poskytována;

b) hardwarové komponenty a platformy, na kterých běží softwarové komponenty uvedené v bodě (b) nebo se na ně spoléhají při kritických operacích v případech, kdy jsou poskytovány přímo nebo nepřímo řešením peněženky a systémem elektronické identifikace, v jehož rámci je poskytováno, a kdy jsou vyžadovány pro splnění požadované úrovně záruky těchto softwarových komponentů. Pokud hardwarové komponenty a platformy neposkytuje poskytovatel peněženky, vnitrostátní systémy certifikace stanoví předpoklady pro hodnocení hardwarových komponentů a platforem, podle něhož lze zajistit odolnost proti útočníkům s vysokým potenciálem útoku v souladu s prováděcím nařízením (EU) 2015/1502, a stanoví hodnoticí činnosti k potvrzení těchto předpokladů, jak je uvedeno v příloze IV;

([10]) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) procesy, které podporují poskytování a fungování řešení peněženky, včetně procesu zapojení uživatelů podle článku 5a nařízení (EU) č. 910/2014, a které zahrnují alespoň přihlášení, správu prostředků pro elektronickou identifikaci a organizaci podle oddílu 2.1, 2.2 a 2.4 přílohy I prováděcího nařízení (EU) 2015/1502.

4. Vnitrostátní systémy certifikace musí obsahovat popis konkrétní architektury řešení peněženky a systému elektronické identifikace, v jehož rámci jsou poskytována. Pokud vnitrostátní systémy certifikace pokrývají více než jednu konkrétní architekturu, musí obsahovat profil pro každou jednotlivou architekturu.

5. Pro každý profil musí vnitrostátní systémy certifikace stanovit alespoň tyto požadavky:

a) konkrétní architekturu řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno;

b) bezpečnostní kontroly spojené s úrovněmi záruky stanovenými v článku 8 nařízení (EU) č. 910/2014;

c) plán hodnocení vypracovaný v souladu s oddílem 7.4.1 normy EN ISO/IEC 17065:2012;

d) bezpečnostní požadavky nezbytné k řešení kybernetických bezpečnostních rizik a hrozeb uvedených v registru rizik stanoveném v příloze I tohoto nařízení, a to až do požadované úrovně záruky, a případně ke splnění cílů vymezených v článku 51 nařízení (EU) 2019/881;

e) přiřazení kontrol uvedených v písmenu (b) tohoto odstavce ke komponentům architektury;

f) popis toho, jak bezpečnostní kontroly, přiřazení kontrol, bezpečnostní požadavky a plán hodnocení uvedené v písmenech (b) až (c) umožňují poskytovatelům řešení peněženek a systému elektronické identifikace, v jehož rámci jsou poskytována, odpovídajícím způsobem řešit kybernetická bezpečnostní rizika a hrozby identifikované v registru rizik podle písmena (d), a to až do požadované úrovně záruky na základě posouzení rizik s cílem upřesnit rizika a hrozby uvedené v registru a doplnit je o rizika a hrozby specifické pro architekturu.

6. Plán hodnocení uvedený v odst. 5 písm. (c) obsahuje seznam hodnoticích činností, které mají být zahrnuty do hodnocení řešení peněženky a systému elektronické identifikace, v jehož rámci jsou poskytována.

7. V rámci hodnoticí činnosti uvedené v odstavci 6 se od poskytovatelů řešení peněženky a systému elektronické identifikace, v jehož rámci se poskytují, požaduje, aby poskytli informace splňující požadavky uvedené v příloze II.

Článek 4

Obecné požadavky

1. Vnitrostátní systémy certifikace pokrývají požadavky na funkčnost, kybernetickou bezpečnost a ochranu údajů, a to s využitím následujících systémů certifikace, jsou-li k dispozici a použitelné:

a) evropské systémy certifikace kybernetické bezpečnosti zřízené podle nařízení (EU) 2019/881, včetně systému EUCC;

b) vnitrostátní systémy certifikace kybernetické bezpečnosti, na něž se vztahuje systém EUCC, v souladu s článkem 49 prováděcího nařízení (EU) 2024/482.

2. Vnitrostátní systémy certifikace mohou navíc odkazovat na (jsou-li k dispozici a použitelné):

a) další příslušné vnitrostátní systémy certifikace;

b) mezinárodní, evropské a vnitrostátní normy;

c) technické specifikace, které splňují požadavky stanovené v příloze II nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ([11]).

3. Vnitrostátní systémy certifikace:

a) určí prvky uvedené v oddíle 6.5 normy EN ISO/IEC 17067:2013;

b) jsou zavedeny v souladu s oddílem 5.3.8 normy EN ISO/IEC 17067:2013 jako systém typu 6.

4. Vnitrostátní systémy certifikace musí splňovat tyto požadavky:

a) k vydávání certifikátů v rámci vnitrostátních systémů certifikace jsou způsobilí pouze poskytovatelé uvedení v čl. 5a odst. 2 nařízení (EU) č. 910/2014;

b) jako značka shody se používá pouze značka důvěry;

c) poskytovatelé řešení peněženky a systému elektronické identifikace, v jehož rámci jsou poskytována, uvádějí v souvislosti s tímto systémem odkazy na nařízení (EU) č. 910/2014 a toto nařízení;

d) poskytovatelé řešení peněženek a systému elektronické identifikace, v jehož rámci jsou poskytována, doplňují posouzení rizik systému podle čl. 3 odst. 5 písm. f) s cílem určit rizika a hrozby specifické pro jejich zavádění a navrhnout ke všem relevantním rizikům a hrozbám vhodná opatření pro jejich řešení;

e) jsou stanoveny odpovědnosti a právní kroky zahrnující odkazy na platné vnitrostátní právní předpisy, jež definují odpovědnosti a možné právní kroky, pokud je certifikace v rámci systému používána podvodně.

5. Posouzení uvedené v odst. 4 písm. (d) je sdíleno s certifikačním subjektem pro účely hodnocení.

Článek 5

Řízení incidentů a zranitelností

1. Vnitrostátní systémy certifikace obsahují požadavky na řízení incidentů a zranitelností v souladu s odstavci 2 až 9.

2. Držitel certifikátu shody řešení peněženky a systému elektronické identifikace, v jehož rámci se poskytují, oznámí svému certifikačnímu subjektu bez zbytečného odkladu veškerá porušení nebo ohrožení řešení peněženky nebo systému elektronické identifikace, v jehož rámci je poskytováno, která mají pravděpodobný dopad na jejich soulad s požadavky vnitrostátních systémů certifikace.

3. Držitel certifikátu shody musí zavést, udržovat a uplatňovat zásady a postupy pro řízení zranitelností, přičemž zohlední postupy stanovené ve stávajících evropských a mezinárodních normách, včetně normy EN ISO/IEC 30111:2019.

4. Držitel certifikátu shody oznámí vydávajícímu certifikačnímu subjektu zranitelnosti a změny, které mají vliv na řešení peněženky, a to na základě definovaných kritérií dopadu těchto zranitelností a změn.

5. Držitel certifikátu shody vypracuje zprávu o analýze dopadu zranitelností pro každou zranitelnost, která ovlivňuje softwarové komponenty řešení peněženky. Zpráva musí obsahovat tyto informace:

a) dopad zranitelnosti na certifikované řešení peněženky;

b) možná rizika spojená s blízkostí nebo pravděpodobností útoku;

([11]) Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského 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 kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) zda lze zranitelnost odstranit dostupnými prostředky;

d) pokud lze zranitelnost odstranit dostupnými prostředky, možné způsoby jejího odstranění.

6. Pokud je oznámení požadováno podle odstavce 4, předá držitel certifikátu shody zprávu o analýze dopadu zranitelností uvedenou v odstavci 5 certifikačnímu subjektu bez zbytečného odkladu.

7. Držitel certifikátu shody musí zavést, udržovat a uplatňovat zásady řízení zranitelností splňující požadavky stanovené v příloze I aktu o kybernetické odolnosti ([12]).

8. Vnitrostátní systémy certifikace stanoví požadavky na zveřejňování zranitelností vztahující se na certifikační subjekty.

9. Držitel certifikátu shody zveřejní a zaregistruje každou veřejně známou a odstraněnou zranitelnost v řešení peněženky nebo v jednom z online úložišť uvedených v příloze V.

Článek 6

Údržba vnitrostátních systémů certifikace

1. Vnitrostátní systémy certifikace obsahují proces pro pravidelné přezkoumávání jejich provozu. Cílem tohoto procesu je potvrdit jejich přiměřenost a určit aspekty, které vyžadují zlepšení, s přihlédnutím ke zpětné vazbě od zúčastněných stran.

2. Vnitrostátní systémy certifikace obsahují ustanovení týkající se jejich údržby. Tento proces zahrnuje alespoň tyto požadavky:

a) pravidla pro správu definic a požadavků vnitrostátních systémů certifikace;

b) stanovení lhůt pro vydávání certifikátů po přijetí aktualizovaných verzí vnitrostátních systémů certifikace, a to jak pro nové certifikáty shody, tak pro dříve vydané certifikáty;

c) pravidelný přezkum vnitrostátních systémů certifikace s cílem zajistit konzistentní uplatňování požadavků vnitrostátních systémů certifikace, s přihlédnutím alespoň k těmto aspektům:

— žádosti o vysvětlení adresované vlastníkovi systému v souvislosti s požadavky vnitrostátního systému certifikace,

— zpětná vazba od zúčastněných stran a dalších dotčených stran,

— reakce vlastníka vnitrostátního systému certifikace na žádosti o informace;

d) pravidla pro sledování referenčních dokumentů a postupy pro vývoj referenčních verzí vnitrostátních systémů certifikace, zahrnující alespoň přechodná období;

e) postup k zajištění toho, aby byla pokryta nejnovější kybernetická bezpečnostní rizika a hrozby uvedené v registru rizik stanoveném v příloze I tohoto nařízení;

f) proces řízení dalších změn ve vnitrostátních systémech certifikace.

([12]) Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti) (Úř. věst. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Vnitrostátní systémy certifikace obsahují požadavky na provádění hodnocení aktuálně certifikovaných výrobků v rámci určitého období po revizi systému nebo po vydání nových specifikací nebo norem nebo jejich nových verzí, s nimiž musí být řešení peněženky a systém elektronické identifikace, v jehož rámci jsou poskytována, v souladu.

KAPITOLA III

POŽADAVKY TÝKAJÍCÍ SE VLASTNÍKŮ SYSTÉMŮ

Článek 7

Obecné požadavky

1. Vlastníci systémů vytvářejí a udržují systémy certifikace a řídí jejich operace.

2. Vlastníci systému mohou všechny své úkoly nebo jejich část zadat třetí straně jako subdodavateli. V případě zadání subdodávek třetí straně stanoví vlastníci systémů povinnosti a odpovědnosti všech stran smluvně. Vlastníci systémů zůstávají odpovědní za všechny subdodavatelské činnosti prováděné jejich subdodavateli.

3. Vlastníci systémů provádějí své případné monitorovací činnosti alespoň na základě těchto informací:

a) informací od certifikačních subjektů, vnitrostátních akreditačních orgánů a příslušných orgánů dozoru nad trhem;

b) informací vyplývajících z vlastních auditů a šetření nebo auditů a šetření jiného orgánu;

c) stížností a odvolání podle článku 15.

4. Vlastníci systémů informují o revizích vnitrostátních systémů certifikace skupinu pro spolupráci. Toto oznámení poskytne skupině pro spolupráci dostatečné informace pro vydání doporučení vlastníkům systémů a stanovisek k aktualizovaným vnitrostátním systémům certifikace.

KAPITOLA IV

POŽADAVKY TÝKAJÍCÍ SE POSKYTOVATELŮ ŘEŠENÍ PENĚŽENKY A SYSTÉMU ELEKTRONICKÉ IDENTIFIKACE, V JEHOŽ RÁMCI JSOU POSKYTOVÁNA

Článek 8

Obecné požadavky

1. Vnitrostátní systémy certifikace obsahují požadavky na kybernetickou bezpečnost založené na posouzení rizik každé konkrétní podporované architektury. Cílem těchto požadavků na kybernetickou bezpečnost je odstranit identifikované kybernetické bezpečnostní hrozby a rizika, jak jsou stanoveny v registru rizik uvedeném v příloze I.

2. V souladu s čl. 5a odst. 23 nařízení (EU) č. 910/2014 vnitrostátní systémy certifikace požadují, aby řešení peněženky a systémy elektronické identifikace, v jejichž rámci jsou poskytována, byly pro vysokou úroveň záruky odolné proti útočníkům s vysokým potenciálem útoku, jak je stanoveno v prováděcím nařízením (EU) 2015/1502.

3. Vnitrostátní systémy certifikace stanoví bezpečnostní kritéria, která zahrnují tyto požadavky:

a) akt o kybernetické odolnosti, je-li to relevantní, nebo požadavky splňující bezpečnostní cíle stanovené v článku 51 nařízení (EU) 2019/881;

b) stanovení a uplatňování zásad a postupů týkajících se řízení rizik spojených s fungováním řešení peněženky, včetně identifikace a posouzení rizik a zmírňování identifikovaných rizik;

c) stanovení a uplatňování zásad a postupů týkajících se řízení změn a řízení zranitelností v souladu s článkem 5 tohoto nařízení;

d) stanovení a uplatňování zásad a postupů v oblasti řízení lidských zdrojů, včetně požadavků na odbornost, spolehlivost, zkušenosti, bezpečnostní školení a kvalifikaci pracovníků podílejících se na vývoji nebo fungování řešení peněženky;

e) požadavky týkající se provozního prostředí řešení peněženky, včetně předpokladů o bezpečnosti zařízení a platforem, na kterých jsou provozovány softwarové komponenty řešení peněženky, včetně bezpečných kryptografických prostředků peněženky, a v příslušných případech požadavky na posouzení shody, jejichž cílem je potvrdit, že jsou tyto předpoklady ověřeny na příslušných zařízeních a platformách;

f) pro každý předpoklad, který není podložen certifikátem shody nebo jinými přijatelnými informacemi o záruce, popis mechanismu, který poskytovatel peněženky používá k prosazení předpokladu, a také odůvodnění, že tento mechanismus je dostatečný k zajištění ověření předpokladu;

g) stanovení a provádění opatření, která zajistí používání aktuálně certifikované verze řešení peněženky.

4. Vnitrostátní systémy certifikace obsahují pro operace uvedené v příloze III funkční požadavky týkající se mechanismů aktualizace každého softwarového komponentu řešení peněženky a systému elektronické identifikace, v jehož rámci jsou poskytována.

5. Vnitrostátní systémy certifikace požadují, aby žadatel o certifikaci certifikačnímu subjektu poskytl nebo jinak zpřístupnil tyto informace a dokumenty:

a) důkazy týkající se informací uvedených v bodě 1 přílohy IV, v případě potřeby včetně podrobností o řešení peněženky a jejím zdrojovém kódu, zahrnujících mimo jiné:

— *informace o architektuře:* pro každý komponent řešení peněženky (včetně komponentů produktu, procesu a služby) popis jeho základních bezpečnostních vlastností, včetně jeho externích závislostí,

— *kontroly a úrovně záruky:* pro každou bezpečnostní kontrolu řešení peněženky popis kontroly a požadovanou úroveň záruky na základě přílohy prováděcího nařízení (EU) 2015/1502, která stanoví řadu technických specifikací a postupů, jež se týkají různých kontrol prováděných prostředky pro elektronickou identifikaci,

— *přiřazení kontrol ke komponentům architektury:* popis toho, jak jsou kontroly peněženky prováděny pomocí různých komponentů řešení peněženky, založený na důvodech vysvětlujících, proč je požadována daná úroveň zabezpečení, a jak jsou kontroly prováděny se všemi požadovanými bezpečnostními aspekty na příslušné úrovni,

— *důvody a odůvodnění krytí rizik:* odůvodnění:

— přiřazení kontrol ke komponentům;

— vhodnosti navrhovaného plánu hodnocení tak, aby vhodně zahrnoval všechny kontroly;

— pokrytí kontrolami kybernetických bezpečnostních rizik a hrozeb identifikovaných v registru rizik, doplněné kontrolami rizik a hrozeb specifickými pro provádění, na příslušné úrovni záruk.

b) informace uvedené v příloze V;

c) úplný seznam certifikátů shody a dalších informací o záruce použitých jako důkaz během hodnoticích činností;

d) veškeré další informace důležité pro hodnoticí činnosti.

KAPITOLA V

POŽADAVKY TÝKAJÍCÍ SE CERTIFIKAČNÍCH SUBJEKTŮ

Článek 9

Obecné požadavky

1. Certifikační subjekty jsou akreditovány vnitrostátními akreditačními orgány jmenovanými podle nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ([13]) v souladu s normou EN ISO/IEC 17065:2012, pokud splňují požadavky stanovené ve vnitrostátních systémech certifikace podle odstavce 2.

2. Pro účely akreditace musí certifikační subjekty splňovat všechny následující požadavky na způsobilost:

a) podrobnou a technickou znalost příslušných architektur řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno, jakož i hrozeb a rizik souvisejících s těmito architekturami;

b) znalost dostupných bezpečnostních řešení a jejich vlastností podle přílohy prováděcího nařízení (EU) 2015/1502;

c) znalosti činností prováděných na základě certifikátů shody, které se vztahují na komponenty daného řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno, přičemž jsou předmětem certifikace;

d) podrobná znalost použitelného vnitrostátního systému certifikace zřízeného v souladu s kapitolou II.

3. Certifikační subjekty provádějí činnosti dozoru zejména na základě těchto informací:

a) informací od vnitrostátních akreditačních orgánů a příslušných orgánů dozoru nad trhem;

b) informací vyplývajících z vlastních auditů a šetření nebo auditů a šetření jiného orgánu;

c) stížností a odvolání podle článku 15.

Článek 10

Subdodavatelé

Certifikační subjekty mohou podle článku 13 zadat hodnoticí činnosti třetím stranám. Pokud jsou hodnoticí činnosti zadávány subdodavatelům, stanoví vnitrostátní systémy certifikace tyto požadavky:

1) všichni subdodavatelé certifikačního subjektu provádějící hodnoticí činnosti musí podle potřeby a vhodnosti pro prováděné činnosti splňovat požadavky harmonizovaných norem, jako je EN ISO/IEC 17025:2017 pro zkoušení, EN ISO/IEC 17020:2012 pro inspekci, EN ISO/IEC 17021-1:2015 pro audit a EN ISO/IEC 17029:2019 pro validaci [ověřování platnosti] a ověřování;

2) certifikační subjekty musí převzít odpovědnost za všechny hodnoticí činnosti zadané jiným subjektům a prokázat, že během své akreditace přijaly vhodná opatření, včetně případného spoléhání se na vlastní akreditaci svých subdodavatelů;

3) do jaké míry je třeba získat předchozí souhlas s potřebami v oblasti externího zajišťování služeb od vlastníků systémů nebo klienta, jehož řešení peněženky je certifikováno v rámci certifikačního systému.

([13]) Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Článek 11

Oznámení orgánu dohledu

Certifikační subjekty oznámí vydání, pozastavení a zrušení certifikátů shody řešení peněženky a systému elektronické identifikace, v jehož rámci jsou řešení peněženky poskytována, orgánu dohledu uvedenému v čl. 46a odst. 1 nařízení (EU) č. 910/2014.

Článek 12

Řízení incidentů a zranitelností

1. Certifikační subjekty bez zbytečného odkladu pozastaví platnost certifikátu shody řešení peněženky a systému elektronické identifikace, v jehož rámci jsou poskytována, poté, co potvrdí, že oznámené narušení nebo ohrožení bezpečnosti má vliv na soulad řešení peněženky nebo systému elektronické identifikace, v jehož rámci jsou poskytována, s požadavky vnitrostátních systémů certifikace.

2. Certifikační subjekty zruší certifikát shody, jehož platnost byla pozastavena v důsledku narušení nebo ohrožení bezpečnosti, které nebylo včas odstraněno.

3. Certifikační subjekty v souladu s čl. 5c odst. 4 a čl. 5e odst. 2 nařízení (EU) č. 910/2014 zruší certifikáty shody, pokud zjištěná zranitelnost nebyla včas odstraněna úměrně její závažnosti a potenciálnímu dopadu.

KAPITOLA VI

ČINNOSTI POSUZOVÁNÍ SHODY

Článek 13

Hodnoticí činnosti

1. Vnitrostátní systémy certifikace obsahují metody a postupy, které mají subjekty posuzování shody používat při provádění svých hodnoticích činností v souladu s normou EN ISO/IEC 17065:2012 a které zahrnují alespoň tyto aspekty:

a) metody a postupy pro provádění hodnoticích činností, včetně těch, které se týkají bezpečného kryptografického prostředku peněženky, jak je stanoveno v příloze IV;

b) audit zavedení řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno, na základě registru rizik uvedeného v příloze I a v případě potřeby doplněného o rizika specifická pro zavádění;

c) testování funkčnosti, pokud je to možné a vhodné, na základě sad testů definovaných podle technických specifikací nebo norem;

d) posouzení existence a vhodnosti procesů údržby, včetně alespoň správy verzí, správy aktualizací a řízení zranitelností;

e) posouzení operační účinnosti procesů údržby, včetně alespoň správy verzí, správy aktualizací a řízení zranitelností;

f) analýzu závislostí, kterou poskytne poskytovatel peněženky, včetně metodiky pro posouzení přijatelnosti informací o záruce, jež zahrnuje prvky uvedené v příloze VI;

g) posouzení zranitelnosti na příslušné úrovni, včetně:

— přezkumu formy řešení peněženky a případně jeho zdrojového kódu,

— testování odolnosti řešení peněženky proti útočníkům s vysokým potenciálem útoku pro „vysokou“ úroveň záruky podle bodu 2.2.1 přílohy prováděcího nařízení (EU) 2015/1502;

h) posouzení vývoje prostředí hrozeb a jeho dopadu na pokrytí rizik řešením peněženky s cílem určit, které hodnoticí činnosti jsou u různých komponentů řešení peněženky zapotřebí.

2. Vnitrostátní systémy certifikace obsahují hodnocení, které má určit, zda zavedená řešení peněženky a systém elektronické identifikace, v jehož rámci jsou tato řešení peněženky poskytována, odpovídají architektuře stanovené v čl. 3 odst. 5 písm. a), jakož i hodnocení, jehož cílem je určit, zda plán hodnocení navržený společně s zavedením odpovídá plánu hodnocení uvedenému v čl. 3 odst. 5 písm. c).

3. Vnitrostátní systémy certifikace stanoví pravidla pro výběr vzorků s cílem zabránit opakování stejných hodnoticích činností a zaměřit se na činnosti, které jsou specifické pro danou variantu. Tato pravidla pro výběr vzorků umožňují provádět testy funkčnosti a bezpečnosti pouze na vzorku variant cílového komponentu řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno, a na vzorku cílových zařízení. Vnitrostátní systémy certifikace požadují, aby všechny certifikační subjekty odůvodnily použití výběru vzorků.

4. Vnitrostátní systémy certifikace požadují, aby certifikační subjekt provedl hodnocení bezpečné kryptografické aplikace peněženky na základě metod a postupů stanovených v příloze IV.

Článek 14

Certifikační činnosti

1. Vnitrostátní systémy certifikace stanoví pro účely vydání certifikátu shody potvrzení v souladu s oddílem V písm. a) normy EN ISO/IEC 17067:2013, tabulka 1, včetně těchto aspektů:

a) obsah certifikátu shody stanovený v příloze VII;

b) jak mají být výsledky hodnocení uvedeny ve veřejné zprávě o certifikaci, včetně alespoň shrnutí předběžného plánu auditu a ověřování platnosti, jak je stanoveno v příloze VIII;

c) obsah výsledků hodnocení uvedených ve zprávě o posouzení certifikace, včetně prvků uvedených v příloze VIII.

2. Zpráva o posouzení certifikace může být zpřístupněna skupině pro spolupráci a Komisi.

Článek 15

Stížnosti a odvolání

Vnitrostátní systémy certifikace obsahují postupy nebo odkazy na příslušné vnitrostátní právní předpisy, které definují mechanismus účinného podávání a vyřizování stížností a odvolání v souvislosti s prováděním systému certifikace nebo vydaným certifikátem shody. Tyto postupy zahrnují poskytnutí informací stěžovateli o pokroku v řešení stížnosti a o přijatém rozhodnutí, jakož i o jeho právu na účinnou soudní ochranu. Vnitrostátní systémy certifikace vyžadují, aby všechny stížnosti a odvolání, které nevyřešil nebo nemohl vyřešit certifikační subjekt, byly zaslány k posouzení a vyřešení vlastníkovi systému.

Článek 16

Činnosti dozoru

1. Vnitrostátní systémy certifikace vyžadují, aby certifikační subjekty prováděly činnosti dozoru spočívající v hodnocení procesů dozoru v kombinaci s namátkovými testy nebo inspekcemi.

2. Vnitrostátní systémy certifikace obsahují požadavky na vlastníky systémů, aby monitorovali soulad certifikačních subjektů s povinnostmi vyplývajícími z nařízení (EU) č. 910/2014 a případně z vnitrostátních systémů certifikace.

3. Vnitrostátní systémy certifikace obsahují požadavky na certifikační subjekty, aby monitorovaly tyto skutečnosti:

a) soulad držitelů certifikátu shody vydaného v rámci vnitrostátních systémů certifikace s jejich povinnostmi týkajícími se certifikace a vyplývajícími z nařízení (EU) č. 910/2014 a vnitrostátních systémů certifikace;

b) soulad certifikovaného řešení peněženky s požadavky stanovenými ve vnitrostátních systémech certifikace.

Článek 17

Důsledky nesouladu

Vnitrostátní systémy certifikace stanoví důsledky nesouladu certifikovaného řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno, s požadavky stanovenými v tomto nařízení. Tyto důsledky obsahují následující aspekty:

1) povinnost certifikačního subjektu informovat držitele certifikátu shody a požádat držitele certifikátu shody o provedení nápravných opatření;

2) povinnost certifikačního subjektu informovat ostatní příslušné orgány dozoru nad trhem, pokud se nesoulad týká příslušných právních předpisů Unie;

3) podmínky pro provedení nápravných opatření držitelem certifikátu shody;

4) podmínky pro pozastavení platnosti certifikátu shody certifikačním subjektem a pro obnovení jeho platnosti po odstranění nesouladu;

5) podmínky pro zrušení certifikátu shody certifikačním subjektem;

6) důsledky nesouladu ze strany certifikačního subjektu s požadavky vnitrostátního systému certifikace.

KAPITOLA VII

ŽIVOTNÍ CYKLUS CERTIFIKACE

Článek 18

Životní cyklus certifikace

1. Platnost certifikátů shody vydaných v rámci vnitrostátních systémů certifikace je předmětem pravidelných hodnoticích činností prováděných certifikačním subjektem v souladu s požadavky stanovenými v příloze IX.

2. Vnitrostátní systémy certifikace obsahují proces pro recertifikaci řešení peněženky a systému elektronické identifikace, v jehož rámci jsou poskytována, na žádost držitele certifikátu shody před uplynutím platnosti původního certifikátu shody. Tento proces recertifikace zahrnuje úplné hodnocení řešení peněženky a systému elektronické identifikace, v jehož rámci jsou poskytována, včetně posouzení zranitelnosti, podle zásad stanovených v příloze IX.

3. Vnitrostátní systémy certifikace obsahují proces pro řízení změn v certifikovaném řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno. Tento proces zahrnuje pravidla pro určení, zda se na změnu má vztahovat zvláštní hodnocení podle odstavce 4 nebo ověření operační účinnosti procesů údržby podle přílohy IV.

4. Vnitrostátní systémy certifikace obsahují proces pro zvláštní hodnocení v souladu s normou EN ISO/IEC 17065:2012. Tento proces pro zvláštní hodnocení zahrnuje výběr činností, které mají být provedeny za účelem řešení konkrétního problému, který vyvolal dané zvláštní hodnocení.

5. Vnitrostátní systémy certifikace stanoví pravidla týkající se zrušení certifikátu shody.

KAPITOLA VIII

VEDENÍ ZÁZNAMŮ A OCHRANA INFORMACÍ

Článek 19

Uchovávání záznamů

1. Vnitrostátní systémy certifikace obsahují požadavky na certifikační subjekty týkající se systému záznamů všech relevantních informací vytvořených v souvislosti s činnostmi posuzování shody, které vykonávají, včetně údajů vydaných a přijatých poskytovateli řešení peněženky a systémů elektronické identifikace, v jejichž rámci jsou poskytována. Záznamy těchto informací se uchovávají bezpečným způsobem. Záznamy mohou být uchovávány v elektronické podobě a musí zůstat přístupné po dobu vyžadovanou právem Unie nebo členských států, nejméně však po dobu pěti let po zrušení nebo uplynutí platnosti příslušného certifikátu shody.

2. Vnitrostátní systémy certifikace stanoví požadavky na držitele certifikátu shody, aby pro účely tohoto nařízení a nejméně po dobu pěti let po zrušení nebo uplynutí platnosti příslušného certifikátu shody bezpečně uchovával tyto informace:

a) záznamy o informacích poskytnutých certifikačnímu subjektu nebo jakémukoliv z jeho subdodavatelů během certifikačního procesu;

b) vzorky hardwarových komponentů, které byly zahrnuty do rozsahu certifikace pro dané řešení peněženky.

3. Vnitrostátní systémy certifikace vyžadují, aby držitel certifikátu shody na požádání zpřístupnil informace uvedené v odstavci 1 certifikačnímu subjektu nebo orgánu dohledu uvedenému v čl. 46a odst. 1 nařízení (EU) č. 910/2014.

Článek 20

Ochrana informací

V rámci vnitrostátních systémů certifikace jsou všechny osoby nebo organizace, kterým je poskytnut přístup k informacím při výkonu činností v rámci vnitrostátního systému certifikace, povinny zajistit bezpečnost a ochranu obchodního tajemství a jiných důvěrných informací, jakož i zachování práv duševního vlastnictví, a přijmout nezbytná a vhodná technická a organizační opatření k zajištění této důvěrnosti.

KAPITOLA IX

ZÁVĚREČNÁ USTANOVENÍ

Článek 21

Přechod na evropský systém certifikace kybernetické bezpečnosti

Toto nařízení podléhá přezkumu po přijetí prvního evropského systému certifikace kybernetické bezpečnosti pro řešení peněženky a systémy elektronické identifikace, v jejichž rámci jsou poskytována, s cílem zohlednit přínos tohoto evropského systému certifikace kybernetické bezpečnosti k celkové certifikaci řešení peněženky a systémů elektronické identifikace, v jejichž rámci jsou poskytována.

Článek 22

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 28. listopadu 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

REGISTR RIZIK PRO EVROPSKÉ PENĚŽENKY DIGITÁLNÍ IDENTITY

Úvod

Registr rizik popisuje hlavní rizika a hrozby pro bezpečnost a soukromí, které se týkají peněženek a které musí být řádně řešeny v každé architektuře a každém zavedení peněženky. **Rizika na vysoké úrovni** (oddíl I) souvisejí s používáním peněženek uživateli a spoléhajícími se stranami a jsou spojena s přímými hrozbami zaměřenými na aktiva peněženek. Kromě toho je u peněženek identifikováno několik **rizik na úrovni systému** (oddíl II), která obvykle vyplývají z kombinace hrozeb týkajících se celého systému peněženek.

Druh rizika	ID rizika	Názvy souvisejících rizik
Rizika pro peněženky na vysoké úrovni	R1	Vytvoření nebo použití existující elektronické identity
	R2	Vytvoření nebo použití falešné elektronické identity
	R3	Vytvoření nebo použití falešných atributů
	R4	Krádež identity
	R5	Krádež údajů
	R6	Zpřístupnění údajů
	R7	Manipulace s údaji
	R8	Ztráta údajů
	R9	Neoprávněná transakce
	R10	Manipulace s transakcemi
	R11	Popření
	R12	Zpřístupnění údajů o transakcích
	R13	Narušení služby
	R14	Dozor
Rizika související se systémem	SR1	Velkoobchodní dozor
	SR2	Poškození dobré pověsti
	SR3	Nesoulad s právními předpisy

Registr rovněž identifikuje **technické hrozby** (oddíl III) zaměřené na zavedení řešení peněženky. Tyto hrozby souvisejí s riziky na vysoké úrovni v tom smyslu, že každá z nich by mohla vyvolat mnoho rizik na vysoké úrovni.

Druh hrozby	ID hrozby	Názvy souvisejících hrozeb	Podkategorie hrozeb
Technická hrozba	TT1	Fyzické útoky	1.1 *Krádež*
			1.2 *Únik informací*
			1.3 *Neoprávněná manipulace*
	TT2	Chyby a chybné konfigurace	2.1 *Chyby při správě IT systému*
			2.2 *Chyby na úrovni aplikace nebo chyby při používání*
			2.3 *Chyby při vývoji a chybné konfigurace systému*

Druh hrozby	ID hrozby	Názvy souvisejících hrozeb	Podkategorie hrozeb
	TT3	Používání nespolehlivých zdrojů	3.1 *Chybné použití nebo konfigurace komponentů peněženky*
	TT4	Poruchy a výpadky	4.1 *Porucha nebo nefunkčnost vybavení, zařízení nebo systémů*
			4.2 *Ztráta zdrojů*
			4.3 *Ztráta podpůrných služeb*
	TT5	Zlovolné jednání	5.1 *Zachycení informací*
			5.2 *Phishing a spoofing*
			5.3 *Přehrání zpráv*
			5.4 *Útok hrubou silou*
			5.5 *Zranitelnosti softwaru*
			5.6 *Útoky na dodavatelský řetězec*
			5.7 *Malware*
			5.8 *Predikce náhodných čísel*

Nakonec jsou v registru **uvedeny přímé hrozby pro peněženky** a ke každé z nich je přiřazen (neúplný) výběr rizik (oddíl IV).

ODDÍL I

Rizika pro peněženky na vysoké úrovni

R1. Vytvoření nebo použití existující elektronické identity

Vytvoření nebo použití existující elektronické identity je definováno jako vytvoření elektronické identity v peněžence, která existuje v reálném světě a je přiřazena jinému uživateli. Toto riziko ve své podstatě vede k riziku krádeže identity (R4) a neoprávněných transakcí (R9).

R2. Vytvoření nebo použití falešné elektronické identity

Vytvoření nebo použití falešné elektronické identity je definováno jako vytvoření elektronické identity v peněžence, která v reálném světě neexistuje.

R3. Vytvoření nebo použití falešných atributů

Vytvoření nebo použití falešných atributů je definováno jako vytvoření nebo použití atributů, u nichž nelze ověřit, že je vydal deklarovaný poskytovatel, a nelze jim důvěřovat.

R4. Krádež identity

Krádež identity je definována jako neoprávněné získání jednotky peněženky nebo ztráta autentizačních faktorů, které umožňují vydávat se za určitou osobu.

R5. Krádež údajů

Krádež údajů je definována jako neoprávněné získání dat. S krádeží údajů souvisí také hrozby, jako je zachycení údajů (neoprávněné zachycení údajů při přenosu) a dešifrování údajů (neoprávněné dekódování zašifrovaných údajů), které mohou v některých případech vést ke zpřístupnění údajů (R6).

R6. Zpřístupnění údajů

Zpřístupnění údajů je definováno jako neoprávněné zveřejnění osobních údajů včetně zvláštních kategorií osobních údajů. Riziko narušení soukromí je velmi podobné, pokud se posuzuje spíše z hlediska ochrany soukromí než z hlediska bezpečnosti.

R7. Manipulace s údaji

Manipulace s údaji je definována jako neoprávněné pozměnění údajů.

R8. Ztráta údajů

Ztráta údajů je definována jako situace, kdy dojde ke ztrátě údajů uložených v peněžence v důsledku zneužití nebo zlovolného jednání. Toto riziko je často sekundárním rizikem manipulace s údaji (R7) nebo narušení služby (R13), kdy nelze obnovit všechny údaje nebo jejich část.

R9. Neoprávněná transakce

Neoprávněné transakce jsou definovány jako operační činnosti provedené bez souhlasu nebo vědomí uživatele peněženky. V mnoha případech může neoprávněná transakce vést ke krádeži identity (R4) nebo zpřístupnění údajů (R6). Souvisí také s neautorizovanými transakcemi, například se zneužitím kryptografických klíčů.

R10. Manipulace s transakcemi

Manipulace s transakcemi je definována jako neoprávněné pozměnění operací v peněžence. Manipulace s transakcemi je útokem na integritu a souvisí s narušením integrity údajů.

R11. Popření

Popření je definováno jako situace, kdy zúčastněná strana může popřít, že by provedla nějakou činnost nebo se účastnila transakce, a ostatní zúčastněné strany nemají vhodné důkazy, které by její tvrzení vyvrátily.

R12. Zpřístupnění údajů o transakcích

Zpřístupnění údajů o transakcích je definováno jako zveřejnění informací týkajících se informací o transakci mezi zúčastněnými stranami.

R13. Narušení služby

Narušení služby je definováno jako přerušení nebo zhoršení běžného fungování peněženky. Specifickým druhem narušení služby je zablokování uživatele, které je definováno jako nemožnost uživatele přistupovat ke svému účtu nebo peněžence.

R14. Dozor

Dozor nebo monitorování jsou definovány jako neoprávněné sledování nebo pozorování činností, komunikace nebo údajů uživatele peněženky. Dozor je často spojen s inferencí, která je definována jako vyvozování citlivých nebo osobních informací ze zdánlivě neškodných údajů.

ODDÍL II

Rizika související se systémem

Tato rizika nejsou v seznamu hrozeb použita, protože jsou obvykle důsledkem více hrozeb, které se opakují tak, že ohrožují celý systém.

SR1. Velkoobchodní dozor

Velkoobchodní dozor je definován jako sledování nebo pozorování činností mnoha uživatelů prostřednictvím jejich komunikace nebo údajů peněženky. Velkoobchodní dozor je často spojen s dozorem (R14) a inferencí v globálním měřítku, kdy se informace o mnoha uživatelích kombinují s cílem vyvodit citlivé nebo osobní údaje o uživatelích nebo určit statistické trendy, které lze využít k návrhu dalších útoků.

SR2. Poškození dobré pověsti

Poškození dobré pověsti je definováno jako újma způsobená pověsti organizace nebo orgánu veřejné správy. Poškození dobré pověsti může být způsobeno i dalšími riziky, pokud se narušení nebo incident objeví v médiích a vykresluje organizaci v nepříznivém světle. Poškození dobré pověsti může vést k dalším rizikům, jako je ztráta důvěry vyplývající z důvodných pochybností uživatele a ztráta ekosystému, když se celý ekosystém zhroutí.

SR3. Nesoulad s právními předpisy

Nesoulad s právními předpisy je definován jako situace, kdy nemohou být dodrženy příslušné právní předpisy nebo normy. Vzhledem k tomu, že v kontextu peněženky jsou bezpečnost a ochrana soukromí daného řešení právními požadavky, je pravděpodobné, že všechny hrozby povedou k určitému druhu nesouladu s právními předpisy.

ODDÍL III

Technické hrozby

Technické hrozby nejsou všechny spojeny s konkrétními riziky pro peněženky, protože mnohé z nich jsou prostředky, které by mohly být použity k provedení útoků odpovídajících mnoha různým rizikům.

TT1. Fyzické útoky

1.1 *Krádež*

Krádež je definována jako odcizení zařízení, které může ovlivnit správné fungování peněženky (v případě, že je zařízení odcizeno a jednotka peněženky není dostatečně chráněna). To může přispět k mnoha rizikům, včetně krádeže identity (R4), krádeže údajů (R5) a neoprávněných transakcí (R9).

1.2 *Únik informací*

Únik informací je definován jako neoprávněný přístup k informacím, jejich zveřejnění nebo sdílení po fyzickém přístupu k peněžence. To může přispět zejména ke zpřístupnění údajů (R6) a krádeži údajů (R5).

1.3 *Neoprávněná manipulace*

Neoprávněná manipulace je definována jako narušení integrity jednoho nebo více komponentů jednotky peněženky nebo komponentů, na které se jednotka peněženky spoléhá, např. uživatelského zařízení nebo jeho operačního systému. To může přispět zejména k manipulaci s údaji (R7), ztrátě údajů (R8) a manipulaci s transakcemi (R10). Pokud neoprávněná manipulace cílí na softwarové komponenty, může přispět k mnoha rizikům.

TT2. Chyby a chybné konfigurace

2.1 *Chyby při správě IT systému*

Chyby při správě IT systému jsou definovány jako únik informací, sdílení informací nebo poškození způsobené nesprávným používáním IT aktiv uživateli (nedostatečné povědomí o funkcích aplikace) nebo nesprávnou konfigurací či správou IT aktiv.

2.2 *Chyby na úrovni aplikace nebo chyby při používání*

Chyby na úrovni aplikace nebo chyby při používání jsou definovány jako nefunkčnost aplikace způsobené chybou v samotné aplikaci nebo chybou některého z uživatelů (uživatelů peněženky a spoléhajících se stran).

2.3 *Chyby při vývoji a chybné konfigurace systému*

Chyby při vývoji a chybné konfigurace systému jsou definovány jako dysfunkce nebo zranitelnosti způsobené nesprávně vyvinutými nebo nakonfigurovanými IT aktivy nebo obchodními procesy (nedostatečné specifikace IT produktů, nedostatečná použitelnost, nezabezpečená rozhraní, nesprávné zásady a postupy, chyby v návrhu).

TT3. Používání nespolehlivých zdrojů

Používání nespolehlivých zdrojů je definováno jako činnost vedoucí k neúmyslným škodám způsobeným nejasně definovanými vztahy důvěry, jako je důvěra v poskytovatele z řad třetích stran bez dostatečné záruky.

3.1 *Chybné použití nebo konfigurace komponentů peněženky*

Chybné použití nebo konfigurace komponentů peněženky je definováno jako neúmyslné poškození komponentů peněženky v důsledku chybného použití nebo chybné konfigurace ze strany uživatelů peněženky nebo nedostatečně vyškolených vývojářů nebo v důsledku nedostatečného přizpůsobení změnám v prostředí hrozeb, typicky použití zranitelných komponentů nebo běhových platforem třetích stran.

TT4. Poruchy a výpadky

4.1 *Porucha nebo nefunkčnost vybavení, zařízení nebo systémů*

Porucha nebo nefunkčnost vybavení je definována jako neúmyslné poškození IT aktiv v důsledku poruchy nebo nefunkčnosti vybavení, včetně infrastruktury poskytovatele a uživatelských zařízení.

4.2 *Ztráta zdrojů*

Ztráta zdrojů je definována jako výpadek nebo nefunkčnost v důsledku nedostupnosti těchto zdrojů, např. dílů pro údržbu.

4.3 *Ztráta podpůrných služeb*

Ztráta podpůrných služeb je definována jako výpadek nebo nefunkčnost v důsledku nedostupnosti podpůrných služeb potřebných pro řádné fungování systému, včetně síťového připojení infrastruktury poskytovatele a uživatelského zařízení.

TT5. Zlovolné jednání

5.1 *Zachycení informací*

Zachycení informací je definováno jako zachycení nesprávně zabezpečených informací při přenosu, včetně útoků „man-in-the-middle“.

5.2 *Phishing a spoofing*

Phishing je definován jako získání informací poskytnutých uživatelem po podvodné interakci, často spojené s podvržením (spoofing) legitimních komunikačních prostředků a internetových stránek. Tyto hrozby se zaměřují na uživatele a obvykle přispívají ke krádeži identity (R4) a neoprávněným transakcím (R9), často prostřednictvím krádeže údajů (R5) nebo zpřístupnění údajů (R6).

5.3 *Přehrání zpráv*

Přehrání zpráv je definováno jako opětovné použití dříve zachycených zpráv k provedení neautorizovaných transakcí, často na úrovni protokolu. Tato technická hrozba přispívá především k neautorizovaným transakcím, které pak mohou vést k dalším rizikům v závislosti na transakci.

5.4 *Útok hrubou silou*

Útok hrubou silou je definován jako narušení bezpečnosti, často důvěrnosti, provedením velkého počtu interakcí, dokud odpovědi neposkytnou cenné informace.

5.5 *Zranitelnosti softwaru*

Hrozba související se softwarovými zranitelnostmi představuje narušení bezpečnosti zneužitím zranitelnosti softwaru v komponentech peněženky nebo v softwarových a hardwarových komponentech použitých při zavedení peněženky, včetně zveřejněných zranitelností a nezveřejněných zranitelností (nultého dne).

5.6 *Útoky na dodavatelský řetězec*

Útok na dodavatelský řetězec je definován jako narušení bezpečnosti prostřednictvím útoků spáchaných na dodavatele poskytovatele peněženky nebo její uživatele, které umožňují další útoky na samotnou peněženku.

5.7 *Malware*

Malware je definován jako narušení bezpečnosti prostřednictvím škodlivých aplikací, které v peněžence provádějí nechtěné a neoprávněné činnosti.

5.8 *Predikce náhodných čísel*

Predikce náhodných čísel je definována jako umožnění útoků hrubou silou prostřednictvím částečné nebo úplné predikce generovaných náhodných čísel.

ODDÍL IV

Hrozby pro peněženky

V poslední části je uveden výběr typických scénářů hrozeb specifických pro peněženky, které jsou přiřazeny ke klíčovým souvisejícím rizikům na vysoké úrovni, jak jsou uvedena výše. Tento seznam uvádí hrozby, které je třeba pokrýt, ale nepředstavuje vyčerpávající seznam hrozeb, jenž do značné míry závisí na architektuře vybraného řešení peněženky a na vývoji prostředí hrozeb. Kromě toho může být poskytovatel peněženky v posouzení rizik a navrhovaných opatřeních odpovědný pouze za komponenty v rozsahu certifikace (*).

ID *Identifikátor*	Popis hrozby *Popis identifikované hrozby* (*)	Název rizika *Související rizika*
TR1	Útočník může zneplatnit pseudonymy bez oprávněného důvodu.	Vytvoření nebo použití falešné elektronické identity (R2)
TR2	Útočník může vydávat neexistující smyšlené elektronické identity.	Vytvoření nebo použití falešné elektronické identity (R2)
TR3	Útočník může začít vydávat neautorizované osobní identifikační údaje.	Vytvoření nebo použití falešné elektronické identity (R2)
TR4	Útočník může přimět správce, aby do seznamu důvěryhodných poskytovatelů osobních identifikačních údajů zadal nesprávného poskytovatele osobních identifikačních údajů.	Vytvoření nebo použití falešné elektronické identity (R2)
TR5	Útočník může obejít službu vzdáleného prokázání totožnosti.	Vytvoření nebo použití existující elektronické identity (R1) / vytvoření nebo použití falešné elektronické identity (R2)
TR6	Útočník může obejít službu fyzického prokázání totožnosti.	Vytvoření nebo použití existující elektronické identity (R1) / vytvoření nebo použití falešné elektronické identity (R2)
TR7	Útočník může obejít služby prokázání totožnosti spojené s použitím vzdáleného (kvalifikovaného) certifikátu.	Vytvoření nebo použití existující elektronické identity (R1) / vytvoření nebo použití falešné elektronické identity (R2)
TR8	Útočník může získat přístup k peněžence, která není vázána na osobu.	Vytvoření nebo použití existující elektronické identity (R1) / vytvoření nebo použití falešné elektronické identity (R2)
TR9	Útočník může překonat technické a procedurální kontroly a vytvořit nesprávné osobní identifikační údaje.	Vytvoření nebo použití existující elektronické identity (R1) / vytvoření nebo použití falešné elektronické identity (R2)
TR10	Útočník může aktivovat novou peněženku na neplatném bezpečném kryptografickém prostředku peněženky.	Vytvoření nebo použití existující elektronické identity (R1) / vytvoření nebo použití falešné elektronické identity (R2)
TR11	Útočník může obejít službu prokazování totožnosti spojenou s použitím stávajících prostředků pro elektronickou identifikaci.	Vytvoření nebo použití existující elektronické identity (R1) / krádež identity (R4) / neoprávněná transakce (R9)
TR12	Útočník může obejít ověření poskytovatelem osobních identifikačních údajů, že peněženku ovládá uživatel, a nechat si vydat osobní identifikační údaje do napadené peněženky pod útočníkovou kontrolou.	Vytvoření nebo použití existující elektronické identity (R1) / krádež identity (R4) / neoprávněná transakce (R9)

ID *Identifikátor*	Popis hrozby *Popis identifikované hrozby (*)*	Název rizika *Související rizika*
TR13	Útočník může získat platné osobní identifikační údaje do neplatné jednotky peněženky.	Vytvoření nebo použití existující elektronické identity (R1) / krádež identity (R4) / neoprávněná transakce (R9)
TR14	Poskytovatel osobních identifikačních údajů může vydávat smyšlené identity, pokud je identita spojena s existující osobou.	Vytvoření nebo použití existující elektronické identity (R1) / krádež identity (R4) / neoprávněná transakce (R9)
TR15	Útočník může spojit osobní identifikační údaje s nesprávnou peněženkou, protože poskytovatel osobních identifikačních údajů není schopen spojit osobní identifikační údaje se správnou peněženkou.	Vytvoření nebo použití existující elektronické identity (R1) / krádež identity (R4) / neoprávněná transakce (R9)
TR16	Útočník může zajistit, aby uživatel schvalující aktivaci nové jednotky/instance peněženky byl pod jeho kontrolou – s následnou kontrolou i nad potvrzeními.	Vytvoření nebo použití existující elektronické identity (R1) / vytvoření nebo použití falešné elektronické identity (R2) / krádež identity (R4) / neoprávněná transakce (R9)
TR17	Útočník může vydat osobní identifikační údaje jiného státu a získat tak přístup k údajům / digitálním aktivům cílených občanů.	Vytvoření nebo použití existující elektronické identity (R1) / krádež identity (R4) / neoprávněná transakce (R9)
TR18	Útočník může překonat technické a procedurální kontroly a vytvořit falešná (kvalifikovaná) elektronická potvrzení atributů.	Vytvoření nebo použití falešných atributů (R3)
TR19	Útočník může předložit (kvalifikovaná) elektronická potvrzení atributů, která mu nebyla platně vydána.	Vytvoření nebo použití falešných atributů (R3)
TR20	Útočník může napadnout mechanismus kryptografického propojení peněženky mezi osobními identifikačními údaji a (kvalifikovaným) elektronickým potvrzením atributů, které by mu nemělo být vydáno.	Vytvoření nebo použití falešných atributů (R3)
TR21	Útočník může použít (kvalifikované) elektronické potvrzení atributů v peněžence, přestože platnost fyzického protějšku (kvalifikovaného) elektronického potvrzení atributů vypršela nebo je tento protějšek neplatný.	Vytvoření nebo použití falešných atributů (R3)
TR22	Útočník může obejít ověření poskytovatelem (kvalifikovaného) elektronického potvrzení atributů, že peněženka je pod kontrolou uživatele, a nechat vydat (kvalifikované) elektronické potvrzení atributů do napadené peněženky pod kontrolou útočníka.	Vytvoření nebo použití falešných atributů (R3)
TR23	Útočník může zfalšovat elektronická potvrzení atributů.	Vytvoření nebo použití falešných atributů (R3)
TR24	Útočník může do peněženky vložit padělaná elektronická potvrzení atributů.	Vytvoření nebo použití falešných atributů (R3)
TR25	Peněženka může spoléhající se straně předložit atributy bez souhlasu uživatele.	Zpřístupnění údajů (R6)
TR26	Osobní identifikační údaje, (kvalifikované) elektronické potvrzení atributů nebo pseudonymy mohou být předloženy nesprávné spoléhající se straně.	Zpřístupnění údajů (R6)
TR27	Útočník může iniciovat zlovolné obnovení elektronického potvrzení atributů.	Zpřístupnění údajů (R6)
TR28	Útočník může uživatele přimět k neoprávněnému schválení žádosti o elektronická potvrzení atributů (phishing nebo jiné).	Zpřístupnění údajů (R6)

ID *Identifikátor*	Popis hrozby *Popis identifikované hrozby (*)*	Název rizika *Související rizika*
TR29	Útočník může z peněženky vypustit atributy a identifikovat uživatele peněženky tam, kde identifikace není vyžadována/ povolena.	Zpřístupnění údajů (R6)
TR30	Útočník může překonat technické a procesní kontroly a získat údaje.	Zpřístupnění údajů (R6)
TR31	Požadavek může být prozrazen útočníkovi.	Zpřístupnění údajů (R6)
TR32	Útočník může získat znalosti o vložených zásadách zpřístupňování atributů a předložit atributy obsažené v aktuálním požadavku ze strany jednotek peněženky.	Zpřístupnění údajů (R6)
TR33	Útočník může získat protokoly nebo jejich části.	Zpřístupnění údajů (R6)
TR34	Útočník může zjistit, zda je peněženka nainstalována na stejném zařízení, které používá, nebo na jiném, a získat o ní informace.	Zpřístupnění údajů (R6)
TR35	Útočník může získat znalostní faktor používaný pro autentizaci uživatelů v rámci bezpečné kryptografické aplikace peněženky.	Zpřístupnění údajů (R6)
TR36	Elektronické potvrzení atributů o osobě, které je předloženo ve více transakcích s jednou spoléhající se stranou nebo s více různými spoléhajícími se stranami, neúmyslně umožňuje propojit více transakcí s příslušnou osobou.	Zpřístupnění údajů (R6)
TR37	Veřejný seznam zneplatněných potvrzení / spoléhajících se stran může obsahovat informace o tom, jak uživatel své potvrzení používá (např. umístění, IP adresa…).	Zpřístupnění údajů (R6)
TR38	Pokud spoléhající se strany nejsou schopny prokázat souhlas uživatele se sdílenými atributy, může to ovlivnit integritu protokolů.	Zpřístupnění údajů (R6)
TR39	Útočník může neoprávněně sledovat uživatele peněženky pomocí jedinečných/sledovatelných identifikátorů.	Zpřístupnění údajů (R6) / dozor (R14)
TR40	Spoléhající se strana, která se skládá z více jednotek/subjektů, z nichž každý má jiný rozsah toho, co má povoleno požadovat/zpracovávat, může požadovat a zpracovávat údaje, pro které nemá oprávněné důvody.	Zpřístupnění údajů (R6) / neoprávněná transakce (R9)
TR41	Útočník může narušit kontrolu integrity a pravosti pomocí peněženky osobních identifikačních údajů tak, aby byla vždy úspěšná.	Manipulace s údaji (R7)
TR42	Útočník může obejít nebo narušit výkon kontrol peněženkou, které ověřují integritu a pravost požadovaných atributů, aby byly vždy úspěšné.	Manipulace s údaji (R7)
TR43	Útočník může obejít nebo narušit výkon kontrol peněženkou, které ověřují všechny požadované atributy patřící stejnému uživateli, aby byly vždy úspěšné.	Manipulace s údaji (R7)
TR44	Útočník může obejít nebo narušit výkon kontrol peněženkou, které ověřují, zda jsou osobní identifikační údaje platné a vydané důvěryhodným poskytovatelem osobních identifikačních údajů, aby byly kontroly vždy úspěšné.	Manipulace s údaji (R7)

ID *Identifikátor*	Popis hrozby *Popis identifikované hrozby (*)*	Název rizika *Související rizika*
TR45	Útočník může obejít nebo narušit výkon kontrol peněženkou, které ověřují, zda je kvalifikované elektronické potvrzení atributů platné a vydané kvalifikovaným poskytovatelem služeb vytvářejících důvěru, který je registrován k vydávání kvalifikovaného elektronického potvrzení atributů, aby byly kontroly vždy úspěšné.	Manipulace s údaji (R7)
TR46	Útočník může obejít nebo narušit výkon kontrol peněženkou, které ověřují, zda byly osobní identifikační údaje poskytovatelem osobních identifikačních údajů zneplatněny, aby byly kontroly vždy úspěšné.	Manipulace s údaji (R7)
TR47	Útočník může obejít nebo narušit výkon kontrol peněženkou, které ověřují, zda bylo (kvalifikované) elektronické potvrzení atributů poskytovatelem (kvalifikovaného) elektronického potvrzení atributů zneplatněno, aby byly kontroly vždy úspěšné.	Manipulace s údaji (R7)
TR48	Útočník může změnit obsah údajů pro zálohování a obnovení, která by měla být výhradně pod kontrolou uživatele.	Manipulace s údaji (R7) / ztráta údajů (R8)
TR49	Útočník může z protokolů aktivit upravit historii transakcí pro danou instanci peněženky.	Manipulace s údaji (R7) / ztráta údajů (R8)
TR50	Útočník může odposlouchávat během spojení mezi peněženkou a spoléhajícími se stranami.	Krádež údajů (R5) / zpřístupnění údajů (R6)
TR51	Útočník může přesvědčit uživatele, aby s ním nebo s třetí stranou sdílel osobní údaje (tj. osobní identifikační údaje, elektronické potvrzení atributů, pseudonymy, elektronické podpisy, protokoly a další údaje), což uživatel neměl v úmyslu.	Krádež údajů (R5) / zpřístupnění údajů (R6)
TR52	Útočník si může z protokolů aktivit přečíst historii transakcí pro danou instanci peněženky.	Krádež údajů (R5) / zpřístupnění údajů (R6)
TR53	Útočník může exportovat nebo extrahovat kryptografický klíčový materiál mimo bezpečný kryptografický prostředek peněženky.	Krádež údajů (R5) / zpřístupnění údajů (R6) / neoprávněná transakce (R9)
TR54	Útočník může číst obsah údajů pro zálohování a obnovení, která by měla být výhradně pod kontrolou uživatele.	Krádež údajů (R5) / zpřístupnění údajů (R6)
TR55	Útočník může obejít metodu autentizace uživatele a použít pseudonym vygenerovaný jednotkou peněženky.	Krádež identity (R4)
TR56	Útočník může uživatelům nabídnout aplikaci, která napodobuje konkrétní oprávněnou peněženku.	Krádež identity (R4)
TR57	Útočník může exportovat údaje peněženky včetně osobních identifikačních údajů, (kvalifikovaných) elektronických potvrzení atributů nebo protokolů.	Krádež identity (R4)
TR58	Útočník může exportovat materiál kryptografické vazby.	Krádež identity (R4)
TR59	Útočník může převzít identity prostřednictvím kryptografických klíčů peněženky.	Krádež identity (R4)
TR60	Útočník může duplikovat osobní jednotku peněženky jiného uživatele v jeho osobním zařízení a použít ji.	Krádež identity (R4) / vytvoření nebo použití existující elektronické identity (R1)

ID *Identifikátor*	Popis hrozby *Popis identifikované hrozby (*)*	Název rizika *Související rizika*
TR61	Orgány jiného státu mohou uživatele požádat, aby ukázal nebo sdílel všechny údaje peněženky, když se nachází v jeho blízkosti, například při překročení hranice tohoto státu.	Krádež identity (R4) / dozor (R14)
TR62	Uživatelé nemohou po selhání uživatelského zařízení přenést protokoly transakcí, což vede ke ztrátě sledovatelnosti předchozích transakcí v nové peněžence.	Popření (R11)
TR63	Uživatelé nemohou po selhání uživatelského zařízení obnovit své protokoly transakcí, což vede ke ztrátě sledovatelnosti v nové peněžence.	Popření (R11)
TR64	Spoléhající se strany mohou mít potíže s prokazováním souhlasu s elektronickými podpisy na dálku.	Popření (R11)
TR65	Útočník může zahltit připojení požadavky na spoléhající se strany během připojení.	Narušení služby (R13)
TR66	Útočník může službu zajišťování stavu zahltit připojeními ke spoléhajícím se stranám.	Narušení služby (R13)
TR67	Útočník může způsobit, že se předložení atributu zobrazí jako sporné/odmítnuté, přestože je v předložení atributu uvedena jeho platnost.	Narušení služby (R13)
TR68	Útočník může osobní identifikační údaje zneplatnit bez oprávněného důvodu.	Narušení služby (R13)
TR69	Útočník může osobní identifikační údaje zneplatnit bez souhlasu uživatele.	Narušení služby (R13)
TR70	Útočník může (kvalifikované) elektronické potvrzení atributů zneplatnit bez oprávněného důvodu.	Narušení služby (R13)
TR71	Útočník může (kvalifikované) elektronické potvrzení atributů zneplatnit bez souhlasu uživatele.	Narušení služby (R13)
TR72	Útočník může spustit více požadavků na identifikaci, aniž by byly rozpoznány jako záměrné osiřelé požadavky.	Narušení služby (R13)
TR73	Útočník může odeslat více požadavků bez následné transakce.	Narušení služby (R13)
TR74	Útočník může povolit spoléhající se straně vyžádat si identifikaci bez odpovídající identifikace (odpovědi) a plné kontroly.	Narušení služby (R13)
TR75	Útočník může odeslat odpověď na požadavek po uplynutí jeho časového limitu nebo v podobných situacích, které vedou k narušení služby.	Narušení služby (R13)
TR76	Spoléhající se strana může odeslat více neplatných požadavků.	Narušení služby (R13)
TR77	Útočník může poskytovateli peněženky odeslat více neplatných požadavků.	Narušení služby (R13)
TR78	Útočník může členskému státu znemožnit zneplatnit nedůvěryhodného poskytovatele osobních identifikačních údajů z důvěryhodného seznamu poskytovatelů osobních identifikačních údajů.	Narušení služby (R13)
TR79	Útočník může zabránit pozastavení platnosti nebo zneplatnění peněženky.	Narušení služby (R13)

ID *Identifikátor*	Popis hrozby *Popis identifikované hrozby (*)*	Název rizika *Související rizika*
TR80	Útočník může zablokovat transakce spoléhajících se stran, uživatelů nebo poskytovatele osobních identifikačních údajů.	Narušení služby (R13)
TR81	Útočník může deaktivovat nebo znepřístupnit bezpečný kryptografický prostředek peněženky.	Narušení služby (R13)
TR82	Útočník může znemožnit poskytovateli osobních identifikačních údajů zneplatnit osobní identifikační údaje nebo pozastavit jejich platnost.	Narušení služby (R13) / neoprávněná transakce (R9)
TR83	Spoléhající se strana může odvodit identifikační údaje uživatele nad rámec údajů, které s ní sdílí.	Dozor (R14)
TR84	Skupina spoléhajících se stran nebo poskytovatelů osobních identifikačních údajů, kteří jsou účastníky koluze, může odvodit identifikační údaje uživatele nad rámec jim známých údajů.	Dozor (R14)
TR85	Útočník může sledovat a vystopovat uživatele pomocí osobních identifikačních údajů uživatele v případech, kdy identifikace uživatele není vyžadována.	Dozor (R14)
TR86	Útočník může zkombinovat „podvržené“ předložení kombinací (kvalifikovaného) elektronického potvrzení atributů.	Manipulace s transakcemi (R10)
TR87	Útočník může aktivovat peněženku / převzít nad ní kontrolu na dálku (např. bankovní aplikace, jejíž součástí je požadavek na autentizaci nebo potvrzení) bez výslovného souhlasu nebo výhradní kontroly uživatele, a to v situacích, kdy uživatel o spoléhající se straně neví (např. spí) nebo ji nevidí.	Manipulace s transakcemi (R10)
TR88	Útočníci mohou provádět změny v metadatech požadavku (název služby, použití atd.).	Manipulace s transakcemi (R10)
TR89	Útočníci mohou provádět změny v informacích v odpovědi (stav služby, nonce atd.).	Manipulace s transakcemi (R10)
TR90	Útočníci mohou provádět změny v informacích o atributech požadavku (přes dotazování atd.).	Manipulace s transakcemi (R10)
TR91	Spoléhající se strana může přehrát prvky z předchozí relace v jiné relaci.	Manipulace s transakcemi (R10)
TR92	Útočník může nahradit nebo upravit osobní identifikační údaje během jejich přenosu od poskytovatele osobních identifikačních údajů do jednotky peněženky.	Manipulace s transakcemi (R10)
TR93	Útočník může nahradit nebo upravit osobní identifikační údaje během jejich přenosu z jednotky peněženky k online spoléhající se straně.	Manipulace s transakcemi (R10)
TR94	Útočník může nahradit nebo upravit osobní identifikační údaje během jejich přenosu z jednotky peněženky k offline spoléhající se straně.	Manipulace s transakcemi (R10)
TR95	Útočník může vydat osobní identifikační údaje bez souhlasu uživatele.	Neoprávněná transakce (R9)
TR96	Útočník může použít zneplatněné nebo neplatné vložené zásady zpřístupnění, případně bez vědomí spoléhajících se stran.	Neoprávněná transakce (R9)
TR97	Útočník může peněženku oklamat, aby ověřila nesprávné elektronické podpisy.	Neoprávněná transakce (R9)
TR98	Útočník může peněženku použít mimo kontrolu uživatele.	Neoprávněná transakce (R9)

ID *Identifikátor*	Popis hrozby *Popis identifikované hrozby (*)*	Název rizika *Související rizika*
TR99	Útočník může přesvědčit uživatele, aby autentizoval a schválil transakce s útočníkem nebo neoprávněnou třetí stranou.	Neoprávněná transakce (R9)
TR100	Útočník může uživatele přimět k elektronickému podpisu, aniž by mu byl předložen obsah, nebo po předložení nesprávného obsahu.	Neoprávněná transakce (R9)
TR101	Útočník může obejít kontrolu přístupu k účtu uživatele u poskytovatele peněženky.	Neoprávněná transakce (R9)
TR102	Útočník se může během připojení ke spoléhajícím se stranám vydávat za spoléhající se strany.	Neoprávněná transakce (R9) / zpřístupnění údajů (R6)
TR103	Uživatel za spojením spoléhající se strana – prohlížeč může být jiný než uživatel za spojením spoléhající se strana – peněženka.	Neoprávněná transakce (R9) / zpřístupnění údajů (R6) / krádež identity (R4)
TR104	Útočník může přesvědčit uživatele, aby bezdůvodně zneplatnil svou peněženku.	Neoprávněná transakce (R9) / narušení služby (R13)
TR105	Útočník může provádět útoky „man-in-the-middle“.	Neoprávněná transakce (R9) / zpřístupnění údajů (R6) / dozor (R14)
TR106	Útočník může předložit neplatné nebo zneplatněné atributy z peněženky, která se pravidelně nepřipojuje k síti.	Vliv na různá rizika
TR107	Útočník může uživateli ukrást informace podvržením peněženky.	Vliv na různá rizika
TR108	Útočník se může vydávat za uživatele přehráním/imitací požadavku na data (např. autentizace), který se bude jevit jako platný.	Vliv na různá rizika
TR109	Útočník může přehrát vložené zásady zpřístupnění směrem k uživateli a napodobit tak schválený požadavek.	Vliv na různá rizika
TR110	Útočník může využít nedostatku informací o uživatelích peněženky nebo zbytečných prodlev po narušení nebo ohrožení bezpečnosti.	Vliv na různá rizika
TR111	Útočník může upravit dříve nainstalovanou oprávněnou instanci peněženky a přidat do ní škodlivé funkce.	Vliv na různá rizika
TR112	Útočník může upravit oprávněnou instanci peněženky a nabídnout ji uživatelům jako oprávněnou.	Vliv na různá rizika
TR113	Útočník může překonat samotný mechanismus autentizace uživatele a obejít tak autentizaci uživatele peněženky.	Vliv na různá rizika
TR114	Útočník může do kódu peněženky při jejím zavádění do uživatelského zařízení zavést škodlivý kód nebo zadní vrátka.	Vliv na různá rizika
TR115	Útočník může do kódu peněženky během jejího vývoje zavést škodlivý kód nebo zadní vrátka.	Vliv na různá rizika
TR116	Útočník může manipulovat s generováním náhodných čísel a snížit jejich entropii natolik, aby umožnil útoky.	Vliv na různá rizika

ID *Identifikátor*	Popis hrozby *Popis identifikované hrozby (*)*	Název rizika *Související rizika*
TR117	Útočník může manipulovat s uživatelskými zařízeními v dodavatelském řetězci tak, že do nich vloží kód nebo konfigurace, které nesplňují podmínky použití peněženky.	Vliv na různá rizika
TR118	Útočník může aktivovat jednotku peněženky pomocí podvrženého bezpečného kryptografického prostředku peněženky ovládaného útočníky.	Vliv na různá rizika
TR119	Útočník může číst informace odeslané do bezpečné kryptografické aplikace peněženky nebo bezpečného kryptografického prostředku peněženky.	Vliv na různá rizika
TR120	Útočník může do bezpečné kryptografické aplikace peněženky odeslat libovolné informace.	Vliv na různá rizika
TR121	Útočník může ukrást informace zachycením výměn mezi bezpečnou kryptografickou aplikací peněženky a bezpečným kryptografickým prostředkem peněženky.	Vliv na různá rizika
TR122	Útočník může do bezpečného kryptografického prostředku peněženky odeslat libovolné informace.	Vliv na různá rizika
TR123	Útočník může odeslat informace do bezpečného kryptografického prostředku peněženky a obejít tak bezpečnou kryptografickou aplikaci peněženky.	Vliv na různá rizika
TR124	Útočník může pomocí phishingu dostat uživatele do falešné webové aplikace pro správu peněženky a osobních identifikačních údajů.	Vliv na různá rizika
TR125	Útočník může nahradit klíče peněženky jinými klíči a vytvořit tak zprávy, které budou použity při jiném útoku.	Vliv na různá rizika
TR126	Útočník může klíče peněženky upravit nebo zničit, čímž se některé funkce peněženky stanou nepoužitelnými.	Vliv na různá rizika
TR127	Útočník může ovládat malware, který mu umožní přístup k datům uloženým v peněžence.	Vliv na různá rizika
TR128	Útočník může získat přístup k důkazům generovaným v peněžence.	Vliv na různá rizika
TR129	Poskytovatelé peněženky mohou přistupovat k objektům v peněžence.	Vliv na různá rizika
TR130	Poskytovatelé peněženky mají přístup k důkazům generovaným v peněžence.	Vliv na různá rizika
TR131	Útočník může ukrást odemčené zařízení s peněženkou.	Vliv na různá rizika
TR132	Útočník může manipulovat se systémem tak, aby zabránil zaznamenávání určitých událostí.	Vliv na různá rizika
TR133	Útočník může zachytit komunikaci mezi instancí peněženky a bezpečnou kryptografickou aplikací peněženky nebo přehrát/napodobit uživatele (např. odcizením mechanismu autentizace (hijacking)).	Vliv na různá rizika

PŘÍLOHA II

KRITÉRIA PRO POSOUZENÍ PŘIJATELNOSTI INFORMACÍ O ZÁRUCE

Název	Předmět	Důležité informace
EUCC	Produkty IKT	O vydavateli: žádné (akreditované certifikační subjekty) O rozsahu: — kontrola profilu ochrany a bezpečnostního cíle — kontrola úrovně záruky hodnocení a rozšíření O záruce: — kontrola omezení v uživatelské dokumentaci — v případě složení může být vyžadován přístup k technické hodnotící zprávě
EUCS (je-li k dispozici)	Cloudové služby	O vydavateli: žádné (akreditované certifikační subjekty) O rozsahu: — kontrola popisu cloudové služby — kontrola úrovně hodnocení a profilů rozšíření O záruce: — kontrola informací o transparentnosti a případně informací o složení
Systémy založené na společných kritériích provozované v EU, včetně systémů výboru SOG-IS	Produkty IKT	O vydavateli: žádné (členské státy) O rozsahu: — kontrola profilu ochrany a bezpečnostního cíle — kontrola úrovně záruky hodnocení a rozšíření O záruce: — kontrola omezení v uživatelské dokumentaci — v případě složení může být vyžadován přístup k technické hodnotící zprávě
EN 17640:2018 (FITCEM, včetně CSPN, BSZ, LINCE, BSZA)	Produkty IKT	O vydavateli: — kontrola systému a požadavků na certifikační subjekty O rozsahu: — kontrola popisu produktu — kontrola tvrzení o bezpečnosti — kontrola úrovně záruky O záruce: — kontrola provedených činností a zjištění ve zprávě
Systémy certifikace kvalifikovaných prostředků pro vytváření podpisů podle článku 30 nařízení (EU) č. 910/2014	QSCD	O vydavateli: — kontrola systému a požadavků na certifikační subjekty O rozsahu: — kontrola popisu produktu — kontrola tvrzení o bezpečnosti — kontrola úrovně záruky O záruce: — kontrola provedených činností

Název	Předmět	Důležité informace
EN ISO/IEC 27001:2022	ISMS	O vydavateli: žádné (akreditované certifikační subjekty) O rozsahu: — kontrola popisu systému řízení — kontrola prohlášení o aplikovatelnosti O záruce: — kontrola provedených činností
SOC2	Organizace	O vydavateli: — kontrola jeho statusu veřejného účetního O rozsahu: — kontrola prohlášení vedení a popisu kontrol — kontrola prohlášení o aplikovatelnosti O záruce: — kontrola zjištění ve zprávě — v případě potřeby kontrola překlenovacích listů (bridge letters)
MDSCert (GSMA) (je-li k dispozici)	Mobilní zařízení	O vydavateli: — kontrola požadavků na certifikační subjekty O rozsahu: — kontrola úrovně záruky bezpečnosti — kontrola požadavků na systém O záruce: — kontrola činností a zjištění ve zprávě
Jiné systémy	Jakýkoliv komponent	O systému: — kontrola relevantnosti a podmínek systému O vydavateli: — kontrola požadavků na certifikační subjekty O rozsahu: — kontrola požadavků na systém — kontrola bezpečnostního cíle nebo podobného dokumentu popisujícího funkční požadavky na bezpečnost a záruku — kontrola popisu produktu a vybraných funkčních požadavků na bezpečnost O záruce: — kontrola činností a zjištění ve zprávě

PŘÍLOHA III

FUNKČNÍ POŽADAVKY NA ŘEŠENÍ PENĚŽENKY

Podle čl. 5a odst. 4, 5, 8 a 14 nařízení (EU) č. 910/2014 zahrnují funkční kritéria, která musí splňovat certifikované řešení peněženky a systém elektronické identifikace, v jehož rámci je poskytováno, funkční požadavky na operace uvedené v těchto právních předpisech:

1) Prováděcí nařízení Komise (EU) 2024/2979 ([1]), kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o integritu a základní funkce;

2) prováděcí nařízení Komise (EU) 2024/2982 ([2]), kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o protokoly a rozhraní, které mají být podporovány evropským rámcem pro digitální identitu;

3) prováděcí nařízení Komise (EU) 2024/2977 ([3]), kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o osobní identifikační údaje a elektronická potvrzení atributů vydávané k evropským peněženkám digitální identity.

([1]) Prováděcí nařízení Komise (EU) 2024/2979 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o integritu a základní funkce (Úř. věst. L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Prováděcí nařízení Komise (EU) 2024/2982 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o protokoly a rozhraní, které mají být podporovány evropským rámcem pro digitální identitu (Úř. věst. L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Prováděcí nařízení Komise (EU) 2024/2977 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o osobní identifikační údaje a elektronická potvrzení atributů vydávané k evropským peněženkám digitální identity (Úř. věst. L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

PŘÍLOHA IV

METODY A POSTUPY PRO HODNOTICÍ ČINNOSTI

1. **Audit zavedení řešení peněženky**

Činnost posuzování shody se skládá z výběru konkrétních hodnoticích činností.

Vnitrostátní systémy certifikace stanoví hodnoticí činnost pro posouzení poskytnutých informací, která zahrnuje alespoň tyto prvky:

a) analýzu poskytnutých informací, která potvrdí, že jsou vhodné pro jednu z architektur uvedených ve vnitrostátních systémech certifikace;

b) analýzu pokrytí kybernetických bezpečnostních rizik a hrozeb identifikovaných v registru rizik v příloze I popsanými bezpečnostními kontrolami.

Analýza uvedená v písmenech a) až b) se opírá o důvody a odůvodnění poskytnuté poskytovatelem peněženky.

2. **Hodnoticí činnosti týkající se bezpečného kryptografického prostředku peněženky**

1) Kritické operace, včetně kryptografických výpočtů, nemusí být plně implementovány do bezpečného kryptografického prostředku peněženky. Část implementovaná do bezpečného kryptografického prostředku peněženky, pokud funguje jako součást řešení peněženky, však musí zaručit ochranu kritických operací, které provádí, před útoky útočníků s vysokým potenciálem útoku v souladu s prováděcím nařízením Komise (EU) 2015/1502 ([1]).

2) Bezpečný kryptografický prostředek nebo jeho část mohou být v rámci předmětu certifikace, pokud je poskytuje držitel certifikátu nebo žadatel o certifikaci, nebo mimo jeho rozsah, pokud jsou částí zařízení poskytovaného koncovým uživatelem. Vnitrostátní systémy certifikace dále určí hodnoticí činnosti pro ověření vhodnosti bezpečného kryptografického prostředku peněženky, a to v těchto dvou případech:

   a) pokud bezpečná kryptografická aplikace peněženky závisí na konkrétním bezpečném kryptografickém prostředku peněženky (tj. pokud je třeba ji hodnotit jako složený produkt založený na bezpečném kryptografickém prostředku peněženky), pak hodnocení bezpečné kryptografické aplikace peněženky vyžaduje přístup k dalším informacím souvisejícím s certifikací bezpečného kryptografického prostředku peněženky, včetně zejména jeho hodnotící technické zprávy;

   b) pokud architektura uvažovaná v systému využívá několik bezpečných kryptografických prostředků peněženky nebo pokud jsou některé operace s kritickými aktivy prováděny mimo bezpečný kryptografický prostředek peněženky, pak vnitrostátní systémy certifikace musí zahrnovat hodnoticí činnosti s cílem zajistit, že celkové řešení nabízí očekávanou úroveň bezpečnosti.

3) Předpokladem pro certifikaci v rámci vnitrostátních systémů certifikace je posouzení bezpečného kryptografického prostředku peněženky na základě požadavků vysokého stupně záruky, jak je stanoveno v prováděcím nařízení (EU) 2015/1502.

   Pokud jsou splněny podmínky uvedené v čl. 3 odst. 3 písm. b), musí hodnocení bezpečného kryptografického prostředku peněženky nebo jeho části zahrnovat posouzení zranitelnosti podle normy EN ISO/IEC 15408-3:2022 na úrovni AVA_VAN.5, jak je stanoveno v příloze I prováděcího nařízení Komise (EU) 2024/482 ([2]), ledaže je certifikačnímu subjektu řádně odůvodněno, že bezpečnostní charakteristiky bezpečné kryptografické aplikace peněženky umožňují použít nižší úroveň posouzení při zachování stejné celkové vysoké úrovně záruky, jak je stanoveno v prováděcím nařízení (EU) 2015/1502.

([1]) Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (Úř. věst. L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([2]) Prováděcí nařízení Komise (EU) 2024/482 ze dne 31. ledna 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC) (Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

4) Kromě toho musí vnitrostátní systémy certifikace v dokumentaci týkající se každé konkrétní architektury vymezit předpoklady pro toto hodnocení bezpečného kryptografického prostředku peněženky, za nichž lze zajistit odolnost proti útočníkům s vysokým potenciálem útoku v souladu s prováděcím nařízením (EU) 2015/1502, a určit hodnoticí činnosti, které potvrdí tyto předpoklady a po vydání certifikátu potvrdí, že předpoklady jsou stále ověřeny. Vnitrostátní systémy rovněž vyžadují, aby žadatelé o certifikaci tyto předpoklady upřesnili pro své konkrétní provádění a popsali zavedená opatření, jejichž účelem je zaručit, že předpoklady budou ověřeny po celý životní cyklus certifikace.

5) Ve všech případech musí vnitrostátní systémy certifikace zahrnovat hodnoticí činnost pro ověření, zda jsou informace o záruce dostupné pro bezpečný kryptografický prostředek peněženky vhodné pro účely daného řešení peněženky, a to prostřednictvím analýzy informací o záruce, jako je bezpečnostní cíl pro certifikáty EUCC, zahrnující tyto činnosti:

   a) ověření, zda je rozsah hodnocení vhodný, což například u certifikátů EUCC znamená ověření, zda je bezpečnostní cíl v souladu s jedním z profilů ochrany doporučených v EUCC;

   b) ověření, zda jsou předpoklady provozního prostředí kompatibilní s řešením peněženky, což například u certifikátů EUCC znamená, že tyto předpoklady lze nalézt v bezpečnostním cíli;

   c) ověření, zda jsou doporučení v pokynech nebo dokumentaci pro uživatele kompatibilní s podmínkami, za kterých má být bezpečný kryptografický prostředek peněženky v řešení peněženky používán;

   d) ověření, zda jsou předpoklady vnitrostátního systému certifikace týkající se bezpečného kryptografického prostředku peněženky ověřeny a zahrnuty v informacích o záruce.

6) V případech, kdy některá ověření nejsou zcela průkazná, vnitrostátní systémy certifikace vyžadují, aby certifikační subjekty určily kompenzační požadavky na bezpečnou kryptografickou aplikaci peněženky založenou na bezpečném kryptografickém prostředku peněženky, které budou zahrnuty do hodnocení bezpečné kryptografické aplikace peněženky. Pokud to není možné, považují vnitrostátní systémy certifikace bezpečný kryptografický prostředek peněženky za nevhodný, což znamená, že dotčenému řešení peněženky nebude vydán certifikát shody.

3. **Hodnoticí činnosti týkající se bezpečné kryptografické aplikace peněženky**

1) Vnitrostátní systémy certifikace vyžadují, aby bezpečná kryptografická aplikace peněženky jako součást řešení peněženky byla hodnocena podle požadavků alespoň na vysokou úroveň záruky, jak je stanoveno v prováděcím nařízení (EU) 2015/1502.

2) Toto hodnocení musí zahrnovat posouzení zranitelností podle normy EN ISO/IEC 15408-3:2022 na úrovni AVA_VAN.5, jak je stanoveno v příloze I prováděcího nařízení (EU) 2024/482, ledaže je certifikačnímu subjektu řádně odůvodněno, že bezpečnostní charakteristiky bezpečné kryptografické aplikace peněženky umožňují použít nižší úroveň posouzení při zachování stejné celkové vysoké úrovně záruky, jak je stanoveno v prováděcím nařízení (EU) 2015/1502.

3) Pokud poskytovatel peněženky bezpečnou kryptografickou aplikaci peněženky neposkytne, vnitrostátní systémy certifikace formulují předpoklady pro toto hodnocení bezpečné kryptografické aplikace peněženky, za nichž lze zajistit odolnost proti útočníkům s vysokým potenciálem útoku v souladu s prováděcím nařízením (EU) 2015/1502, a určit hodnoticí činnosti, které potvrdí tyto předpoklady a po vydání certifikátu potvrdí, že předpoklady jsou stále ověřeny. Vnitrostátní systémy rovněž vyžadují, aby žadatelé o certifikaci tyto předpoklady upřesnili pro své konkrétní provádění a popsali zavedená opatření, jejichž účelem je zaručit, že předpoklady budou ověřeny po celý životní cyklus certifikace.

4) Ve všech případech musí vnitrostátní systémy certifikace zahrnovat hodnoticí činnost pro ověření, zda jsou informace o záruce dostupné pro bezpečnou kryptografickou aplikaci peněženky vhodné pro účely daného řešení peněženky, a to prostřednictvím analýzy informací o záruce, jako je bezpečnostní cíl pro certifikáty EUCC, zahrnující tyto činnosti:

   a) ověření, zda je rozsah hodnocení vhodný, což například u certifikátů EUCC znamená ověření, zda je bezpečnostní cíl v souladu s jedním z profilů ochrany doporučených v EUCC;

   b) ověření, zda jsou předpoklady provozního prostředí kompatibilní s řešením peněženky, což například u certifikátů EUCC znamená, že tyto předpoklady lze nalézt v bezpečnostním cíli;

c) ověření, zda jsou doporučení v pokynech nebo dokumentaci pro uživatele kompatibilní s podmínkami, za kterých má být bezpečná kryptografická aplikace peněženky v řešení peněženky používána;

d) ověření, zda jsou předpoklady vnitrostátního systému certifikace týkající se bezpečné kryptografické aplikace peněženky ověřeny a zahrnuty v informacích o záruce.

5) Vnitrostátní systémy certifikace vyžadují, aby hodnocení bezpečné kryptografické aplikace peněženky zahrnovalo všechny bezpečnostní kontroly zavedené touto bezpečnou kryptografickou aplikací peněženky.

4. **Hodnoticí činnosti týkající se zařízení koncového uživatele**

Vzhledem k tomu, že registr rizik, jak je stanoven v příloze I tohoto nařízení, identifikuje rizika, která přímo souvisejí s bezpečností zařízení koncového uživatele, vnitrostátní systémy certifikace stanoví bezpečnostní požadavky na zařízení koncového uživatele. Protože však tato zařízení poskytuje koncový uživatel, a nikoli poskytovatel peněženky, musí být tyto požadavky pokryty předpoklady.

Pro každý předpoklad musí řešení peněženky obsahovat mechanismus, který má u každé jednotky peněženky ověřit, zda fyzické zařízení koncového uživatele splňuje daný předpoklad. Tyto mechanismy se považují za bezpečnostní kontroly a jsou předmětem hodnoticích činností, které mají prokázat jejich vhodnost a účinnost na příslušné úrovni záruky.

Níže jsou uvedeny dva příklady:

a) zařízení koncového uživatele může obsahovat certifikovaný bezpečný kryptografický prostředek peněženky (WSCD), což je třeba prokázat. Obvykle se to provádí pomocí kryptografického mechanismu, jehož účelem je v bezpečném kryptografickém prostředku peněženky ověřit přítomnost kryptografického tajemství, které je dostupné pouze v daném certifikovaném bezpečném kryptografickém prostředku peněženky. V tomto případě by toto kryptografické tajemství mělo být považováno za kritické aktivum a mělo by být pokryto certifikací bezpečného kryptografického prostředku peněženky nebo bezpečné kryptografické aplikace peněženky;

b) typickým požadavkem na zařízení koncových uživatelů je, že zařízení musí dostávat bezpečnostní aktualizace. Vzhledem k tomu, že tento požadavek se týká instance peněženky, je třeba mechanismus používaný k ověřování dostupnosti bezpečnostních aktualizací pokrýt pouze hodnoticími činnostmi na úrovni záruky vhodné pro instanci peněženky, zejména proto, že bude pravděpodobně integrován do instance peněženky.

5. **Hodnoticí činnosti týkající se instance peněženky**

1) Hodnocení instance peněženky zohlední tyto dvě hlavní výzvy:

a) instance peněženky bude pravděpodobně existovat v sadě variant téže základní aplikace, přičemž každá varianta bude specializovaná pro určitou kategorii zařízení koncových uživatelů;

b) různé varianty instance peněženky budou pravděpodobně potřebovat časté aktualizace, aby bylo možné sledovat vývoj základní bezpečnostní platformy, například při identifikování zranitelností, které vyžadují změny v aplikacích.

2) Hodnocení instance peněženky zohlední tyto specifické výzvy. Jedním z bezprostředních důsledků je, že rámec společných kritérií nemusí být vhodný ve všech případech. Proto se v případě potřeby zváží alternativní metodiky hodnocení. Vnitrostátní systémy certifikace zváží použití metodiky normy EN 17640:2018 v těchto formách:

a) jako součást samotného systému;

b) prostřednictvím vnitrostátních systémů založených na dané metodice;

c) prostřednictvím vnitrostátních systémů založených na podobných principech, ale vytvořených před vypracováním metodiky normy EN 17640:2018.

3) Vzhledem k tomu, že provádění úplného specializovaného hodnocení každé varianty může mít omezenou přidanou hodnotu, zváží vnitrostátní systémy certifikace stanovení kritérií umožňujících výběr vzorků s cílem zabránit opakování stejných hodnoticích činností a zaměřit se na činnosti, které jsou pro danou variantu specifické. Vnitrostátní systémy certifikace požadují, aby všechny certifikační subjekty odůvodnily použití výběru vzorků.

4) Vnitrostátní systémy certifikace zahrnují aktualizace instance peněženky do celkového procesu řízení změn stanoveného pro dané řešení peněženky. Rovněž stanoví pravidla pro postupy, které musí poskytovatel peněženky provádět při každé aktualizaci (např. analýza dopadu změn na bezpečnostní kontroly), a pro hodnoticí činnosti, které musí certifikační subjekt provádět u aktualizací za stanovených podmínek (např. posouzení provozní účinnosti změněné bezpečnostní kontroly). Jedním z procesů, jejichž provozní účinnost je třeba každoročně kontrolovat v souladu s čl. 18 odst. 3., je proces řízení změn.

6. **Hodnoticí činnosti týkající se služeb a procesů používaných při poskytování a provozu řešení peněženky**

1) Pro hodnocení služeb a procesů, které hrají roli při poskytování a provozu řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno, shromažďuje hodnotící tým důkazy prováděním hodnoticích činností, které mohou zahrnovat audit, inspekci, ověřování a ověřování platnosti.

2) Certifikační subjekt potvrdí dostatečnost a vhodnost důkazů, jejichž cílem je poskytnout dostatečnou záruku, že služby a procesy splňují požadavky na certifikaci, a to potvrzením těchto skutečností:

   a) přesnosti informací uvedených v popisu procesů a služeb;

   b) vhodnosti návrhu a kontrol procesů a služeb pro splnění kritérií hodnocení;

   c) provozní účinnosti zavedení těchto kontrol během určitého období před hodnocením.

3) Přesnost popisu a provozní účinnost zavádění kontrol lze ve smyslu normy ISO/IEC 17000:2020 považovat za cíle ověření příslušných tvrzení poskytovatele peněženky (tj. potvrzení pravdivosti událostí, které již nastaly, nebo výsledků, kterých již bylo dosaženo), zatímco vhodnost návrhu a kontrol služeb a procesů pro splnění kritérií hodnocení lze považovat za cíl ověření platnosti odpovídajícího tvrzení poskytovatele peněženky ve smyslu normy ISO/IEC 17000:2020 (tj. potvrzení věrohodnosti ohledně zamýšleného budoucího použití nebo předpokládaného výsledku).

4) Vzhledem k tomu, že řešení peněženky není povoleno provozovat před certifikací, nelze provozní účinnost potvrdit na základě skutečného provozu řešení. Proto se to potvrdí pomocí důkazů získaných během testů nebo pilotních zkoušek.

5) Mohou již existovat vnitrostátní systémy certifikace pro konkrétní služby a procesy, například pro zapojení uživatelů. Použití těchto systémů případně zváží vnitrostátní systémy certifikace.

7. **Hodnoticí činnosti týkající se služeb IKT používaných při poskytování a provozu řešení peněženky**

1) Některé architektury peněženky se mohou spoléhat na vyhrazené služby IKT, včetně cloudových služeb pro poskytování a provoz řešení peněženky, a tyto služby mohou hostit citlivé údaje, jakož i citlivé operace. V takovém případě vnitrostátní systémy certifikace stanoví bezpečnostní požadavky na tyto služby IKT.

2) Pro služby IKT, cloudové služby a další zdroje informací o záruce již existuje mnoho systémů certifikace, včetně systémů uvedených v příloze II. Vnitrostátní systémy certifikace se opírají o tyto stávající mechanismy, pokud jsou k dispozici a použitelné, a to prostřednictvím jednoho z těchto mechanismů:

   a) povinné použití konkrétního systému nebo vybraných systémů stanovením podmínek, za nichž se IKT nebo cloudové služby mají posuzovat pomocí těchto systémů;

   b) ponechání volby posouzení na poskytovateli peněženky a využití analýzy závislostí k analýze vhodnosti informací o záruce získaných prostřednictvím těchto posouzení.

3) V obou případech vnitrostátní systémy certifikace stanoví další hodnoticí činnosti případně potřebné k analýze nebo doplnění informací získaných prostřednictvím těchto systémů.

PŘÍLOHA V

SEZNAM VEŘEJNĚ DOSTUPNÝCH INFORMACÍ O PENĚŽENKÁCH

1. Informace, které se zveřejňují podle čl. 8 odst. 5 obsahují alespoň tyto údaje:

   a) veškerá omezení pro používání řešení peněženky;

   b) pokyny a doporučení poskytovatele peněženky, jež koncovým uživatelům usnadní bezpečnou konfiguraci, instalaci, uvedení do provozu, provoz samotný a údržbu peněženek;

   c) období, během něhož bude koncovým uživatelům k dispozici bezpečnostní podpora, zejména pokud jde o dostupnost aktualizací souvisejících s kybernetickou bezpečností;

   d) kontaktní údaje výrobce či poskytovatele a akceptované metody pro příjem informací o zranitelnostech ze strany koncových uživatelů nebo výzkumných pracovníků v oblasti bezpečnosti;

   e) odkaz na internetová úložiště zveřejněných zranitelností souvisejících s peněženkami a na jakákoli relevantní upozornění v oblasti kybernetické bezpečnosti.

2. Informace uvedené v odstavci 1 musí být zpřístupněny jasným, srozumitelným a jednoduše dostupným způsobem ve veřejně dostupné prostoru, a to všem osobám, které chtějí používat řešení peněženky.

PŘÍLOHA VI

METODIKA PRO POSOUZENÍ PŘIJATELNOSTI INFORMACÍ O ZÁRUCE

1. **Posouzení dostupnosti dokumentace o záruce**

Hodnotitelé uvedou seznam dokumentace o záruce dostupné pro každý příslušný komponent řešení peněženky a systém elektronické identifikace, v jehož rámci je poskytováno. Poté hodnotitelé posoudí celkovou vhodnost každé části dokumentace o záruce pro přezkum závislostí.

Při analýze se zváží tyto aspekty:

1) co se týče samotné dokumentace o záruce:

   a) druh dokumentace o záruce se všemi požadovanými údaji,

      (příkladem takových dokumentů jsou certifikáty shody podle normy EN ISO/IEC 27001:2022 nebo zprávy ISAE typu 1 nebo 2);

   b) doba, na kterou se vztahuje, nebo doba platnosti,

      (toto období může být doplněno překlenovacím listem (dokumentem, který pokrývá období mezi datem ukončení vykazovaného období stávající zprávy ISAE a vydáním nové zprávy ISAE) nebo podobným prohlášením);

   c) platný rámec (např. stávající norma);

   d) zda dokumentace o záruce obsahuje přiřazení k požadavkům systému;

2) co se týče odborné způsobilosti a nestrannosti vydavatele zprávy o záruce:

   a) název certifikačního subjektu a jméno hlavního hodnotitele, je-li k dispozici;

   b) důkazy o způsobilosti certifikačního subjektu a hodnotitele (např. akreditace, osobní osvědčení atd.);

   c) důkazy o nestrannosti certifikačního subjektu a hodnotitele (např. akreditace atd.).

2. **Posouzení záruky týkající se jednotlivých požadavků**

Hodnotitelé ověří, zda dokumentace o záruce dostupná pro dané řešení peněženky a systém elektronické identifikace, v jehož rámci je poskytováno, je dostatečná k určení toho, zda řešení peněženky splňuje očekávání ve vztahu k jednotlivým požadavkům systému certifikace.

Toto posouzení se provede pro každý příslušný komponent řešení peněženky a systém elektronické identifikace, v jehož rámci je poskytováno, a to formulováním předpokladu o bezpečnostních kontrolách řešení peněženky.

U každého takového předpokladu hodnotící tým určí, zda je záruka uvedená v dostupné dokumentaci o záruce přiměřená či nikoliv.

Určení, že je záruka přiměřená, se zakládá na těchto skutečnostech:

1) požadované informace jsou v dokumentaci o záruce dostupné s očekávanou úrovní záruky;

2) informace dostupné v dokumentaci o záruce nepokrývají celý rozsah požadavku, ale dodatečné kontroly nebo kompenzační kontroly (tj. vnitřní kontroly, které snižují riziko existujících nebo potenciálních slabin kontroly) zavedené v řešení peněženky nebo v systému elektronické identifikace, v jehož rámci je poskytováno, umožňují hodnotitelům určit, že informace jsou dostatečné;

3) informace dostupné v dokumentaci o záruce neposkytují očekávanou úroveň záruky, ale kontroly zavedené k posouzení a monitorování poskytovatele peněženky umožňují hodnotitelům určit, že informace jsou dostatečné;

4) pokud jsou v dokumentaci o záruce uvedeny nesoulady týkající se návrhu nebo zavedení kontrol použitých ke splnění předpokladu, musí být nápravná opatření navržena a provedená poskytovatelem peněženky a přezkoumaná jejich hodnotiteli dostatečná, aby zaručila, že předpoklad je skutečně splněn.

PŘÍLOHA VII

OBSAH CERTIFIKÁTU SHODY

1. Jedinečný identifikátor přidělený certifikačním subjektem vydávajícím certifikát shody.

2. Informace týkající se certifikovaného řešení peněženky a systémů elektronické identifikace, v jejichž rámci je poskytováno, a držitele certifikátu shody, včetně:
   a) názvu řešení peněženky,
   b) názvu systémů elektronické identifikace, v jejichž rámci je řešení peněženky poskytováno,
   c) verze řešení peněženky, která byla hodnocena,
   d) jména, adresy a kontaktních údajů držitele certifikátu,
   e) odkazu na internetové stránky držitele certifikátu shody obsahující informace, které musí být zveřejněny.

3. Informace týkající se hodnocení a certifikace řešení peněženky a systémů elektronické identifikace, v jejichž rámci je poskytováno, včetně:
   a) názvu, adresy a kontaktních údajů certifikačního subjektu, který certifikát shody vydal;
   b) pokud se liší od certifikačního subjektu, názvu subjektu posuzování shody, který provedl hodnocení, spolu s informacemi o jeho akreditaci;
   c) názvu vlastníka systému;
   d) odkazů na nařízení (EU) č. 910/2014 a na toto nařízení;
   e) odkazu na zprávu o certifikaci spojenou s certifikátem shody;
   f) odkazu na zprávu o posouzení certifikace spojenou s certifikátem shody;
   g) odkazu na normy použité pro hodnocení, včetně jejich verzí;
   h) data vydání certifikátu shody;
   i) doby platnosti certifikátu shody.

PŘÍLOHA VIII

OBSAH VEŘEJNÉ ZPRÁVY O CERTIFIKACI A ZPRÁVY O POSOUZENÍ CERTIFIKACE

1. Veřejná zpráva o certifikaci musí obsahovat alespoň tyto aspekty:
   a) shrnutí;
   b) identifikace řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno;
   c) popis řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno;
   d) bezpečnostní informace, které mají být zveřejněny, jak je popsáno v příloze V, nebo odkaz na tyto informace;
   e) shrnutí předběžného plánu auditu a ověření platnosti;
   f) shrnutí přezkumu a rozhodnutí o certifikaci.

2. Zpráva o posouzení certifikace musí obsahovat alespoň:
   a) popis formy řešení peněženky, identifikačního systému a procesu zapojování spolu s posouzením rizik a konkrétním plánem ověření platnosti;
   b) popis toho, jak řešení peněženky splňuje požadavky na vysokou úroveň záruky a jak je to prokázáno výsledky posouzení certifikace řešení peněženky provedeného v souladu s tímto nařízením;
   c) popis výsledku posouzení shody řešení peněženky a systému elektronické identifikace, v jehož rámci jsou příslušné jednotky peněženky poskytovány, zejména shody:
      — s požadavky stanovenými v čl. 5a odst. 4, 5 a 8 nařízení (EU) č. 910/2014,
      — s požadavkem na logické oddělení stanoveným v čl. 5a odst. 14 nařízení (EU) č. 910/2014,
      — případně s normami a technickými specifikacemi uvedenými v čl. 5a odst. 24 nařízení (EU) č. 910/2014, přičemž popíše, jak tyto požadavky souvisejí s odpovídajícími normativními požadavky stanovenými vnitrostátními systémy certifikace;
   d) shrnutí výsledku plnění plánu ověření platnosti, včetně všech zjištěných neshod.

PŘÍLOHA IX

HARMONOGRAM POVINNÝCH HODNOCENÍ DOZORU

1. Článek 18 stanoví požadavky na životní cyklus certifikace, zejména na provádění pravidelných hodnoticích činností. Tyto činnosti zahrnují alespoň:

   a) úplné hodnocení předmětu posuzování shody při počátečním hodnocení a při každém hodnocení recertifikace, včetně funkce aktualizace jakéhokoli komponentu produktu;

   b) posouzení zranitelnosti při počátečním hodnocení a při každém hodnocení recertifikace a nejméně jednou za dva roky při hodnoceních dozoru, které zahrnuje alespoň změny v předmětu posuzování shody a změny v prostředí hrozeb od posledního posouzení zranitelnosti;

   c) další činnosti, jako je penetrační testování v případě zvýšené úrovně rizika nebo výskytu nových hrozeb;

   d) hodnocení provozní účinnosti procesů údržby alespoň jednou ročně v rámci hodnocení dozoru a recertifikace, zahrnující alespoň procesy řízení verzí, aktualizací a zranitelností;

   e) po úspěšném přezkumu a rozhodnutí o certifikaci vydání certifikátu shody po počátečním hodnocení a po každém hodnocení recertifikace.

2. Referenční harmonogram je uveden v tabulce 1 na základě čtyřletého cyklu, kde:

   a) rok 1 začíná v okamžiku prvního vydání certifikátu shody a

   b) všechny hodnoticí činnosti se provedou do 12 měsíců od hodnocení předchozího roku.

3. Harmonogram uvedený v tabulce 1 je doporučením, které má zajistit včasnou recertifikaci a zabránit přerušení poskytování řešení peněženky. Jiné harmonogramy jsou možné, pokud platnost certifikátu shody nepřesáhne pět let, jak je stanoveno v čl. 5c odst. 4 nařízení (EU) č. 910/2014.

4. Kromě pravidelných hodnocení může být na žádost certifikačního subjektu nebo držitele certifikátu shody v důsledku významné změny předmětu certifikace nebo prostředí hrozeb zahájeno zvláštní hodnocení.

5. Jakékoli hodnocení, včetně hodnocení dozoru a zvláštních hodnocení, může vést k vydání nového certifikátu shody, zejména v případě významných změn předmětu certifikace, avšak se stejným datem ukončení platnosti jako původní certifikát shody.

Tabulka 1

Celý čtyřletý cyklus hodnocení

Čas	Druh hodnocení	Činnosti
Rok 0	Počáteční	— Úplné hodnocení předmětu certifikace, včetně posouzení zranitelnosti — Včetně funkce pro provádění aktualizací u každého softwarového komponentu — Hodnocení procesů údržby, s výjimkou jejich provozní účinnosti — Vydání certifikátu shody a zahájení čtyřletého cyklu
Rok 1	Dozor	— Hodnocení provozní účinnosti procesů údržby — Minimálně kontrola verze, řízení aktualizací, zranitelností — Vyhodnocení změn ovlivňujících bezpečnost produktu

Čas	Druh hodnocení	Činnosti
Rok 2	Dozor	— Posouzení zranitelnosti celého řešení — Hodnocení provozní účinnosti procesů údržby — Minimálně kontrola verze, řízení aktualizací, zranitelností — Vyhodnocení změn ovlivňujících bezpečnost produktu
Rok 3	Dozor	— Hodnocení provozní účinnosti procesů údržby — Minimálně kontrola verze, řízení aktualizací, zranitelností — Vyhodnocení změn ovlivňujících bezpečnost produktu
Rok 4	Recertifikace	1) Úplné hodnocení předmětu certifikace, včetně posouzení zranitelnosti 2) Zjednodušené hodnocení funkcí/procesů, které se nezměnily 3) Včetně funkce pro provádění aktualizací u každého softwarového komponentu 4) Hodnocení procesů údržby, včetně jejich provozní účinnosti 5) Vydání nového certifikátu shody