

23 Příloha X: Bezpečnostní požadavky na peněženky EUDI a systémy eID, v rámci kterých jsou poskytovány

X.1 Účel a rozsah

Tato příloha X schématu EUDIW-CZ definuje bezpečnostní požadavky pro certifikaci řešení peněženek EUDI a systémů elektronické identifikace, v jejichž rámci jsou poskytovány.

Požadavky v této příloze pokrývají kybernetickou bezpečnost a jsou navrženy tak, aby řešily kybernetické bezpečnostní hrozby a rizika uvedená v registru rizik (příloha I CIR (EU) 2024/2981), a to až do požadované úrovně záruky „vysoká“, která vyžaduje odolnost proti útočníkům s vysokým potenciálem útoku v souladu s prováděcím nařízením (EU) 2015/1502.

Není-li stanoveno jinak, požadavky v kapitolách X.2 až X.5 platí pro všechny poskytovatele služeb EUDI zapojené do poskytování peněženky EUDI a systému eID, v jehož rámci je poskytována, včetně minimálně poskytovatele peněženky, poskytovatele PID a provozovatele ověřovací služby.

Přiřazení požadavků této přílohy komponentám architektury řešení peněženky a službám IKT v rozsahu certifikace je vedeno v příloze I schématu EUDIW-CZ. Cílovou komponentu jednotlivých požadavků uvádí rovněž matice trasovatelnosti v kapitole X.B.

Normy, technické specifikace a další referenční dokumenty, na které tato příloha odkazuje, se použijí ve vydání uvedeném v rejstříku referenčních dokumentů v příloze I schématu EUDIW-CZ. V textu této přílohy se proto vydání referenčních dokumentů zpravidla neuvádí.

X.1.1 Struktura bezpečnostních požadavků

Bezpečnostní požadavky jsou uspořádány do následujících kategorií:

- **Fun — Funkční bezpečnostní požadavky:** Doplnují funkční specifikace EUDIW o aspekty relevantní pro bezpečnost. Shodu lze obvykle hodnotit prostřednictvím testování.
- **Sec — Implementační bezpečnostní požadavky:** Požadavky na bezpečnou implementaci funkcí a ochranu citlivých aktiv. Shodu je třeba hodnotit prostřednictvím auditu nebo inspekce.
- **Cond — Podmíněné požadavky:** Požadavky, které se uplatní pouze za specifických architektonických podmínek (např. vzdálený WSCD, lokální externí WSCD).
- **Privacy — Požadavky na ochranu soukromí:** Požadavky na ochranu soukromí, které jsou zároveň bezpečnostními vlastnostmi, jsou integrovány v kategorii [Sec] a jsou povinné. Kategorie [Privacy] označuje výhradně doplňkové požadavky nad rámec kybernetické bezpečnosti, které lze zahrnout jako volitelné rozšíření rozsahu dle přílohy XIV kap. XIV.3.3.

Identifikátory požadavků používají prefix podle funkční oblasti (např. RMF-, POL-, ORG-, ACC-, CRY-, WUG-, PIDR-, VER- atd.) následovaný pořadovým číslem. Požadavky, které představují rozšíření nad rámec baseline ENISA (tj. jsou přidány specificky schématem EUDIW-CZ), jsou souhrnně uvedeny v kapitole X.1.4.

X.1.2 Metody hodnocení

Metody hodnocení používané v rámci schématu EUDIW-CZ jsou klasifikovány do čtyř kategorií:

- **A** = Audit (přezkum dokumentace a politik);
- **I** = Inspekce (ověření implementace);
- **T** = Testování (funkční a bezpečnostní testy);
- **C** = Certifikát (opětovné využití existujícího certifikátu s analýzou závislostí dle přílohy IX schématu).

Jejich definice a metodologický rámec jsou uvedeny v kapitole XI.1 přílohy XI schématu. U jednotlivých požadavků této přílohy je uváděn orientační odkaz na použitou metodu pomocí těchto zkratk. Podrobné určení metod a jejich kombinací pro konkrétní hodnocení je předmětem hodnotícího plánu připravovaného certifikačním orgánem.

X.1.3 Zjednodušující předpoklady a omezení rozsahu

Pro účely této přílohy se uvažují pouze řešení peněženky, jejichž jednotka peněženky (wallet unit) splňuje následující podmínky:

- a) každá jednotka peněženky obsahuje jednu WSCA a jeden WSCD pro zajištění vysoké úrovně záruky (elektronická potvrzení atributů mohou být uložena mimo toto WSCD v závislosti na rulebooku konkrétního EAA);
- b) každá jednotka peněženky obsahuje jednu instanci peněženky.

X.1.4 Rozšíření nad rámec baseline ENISA

Baseline bezpečnostních požadavků této přílohy X vychází z bezpečnostních požadavků na poskytovatele služeb souvisejících s peněženkou (požadavky ENISA, založeno na ETSI EN 319 401), doplněno o funkční požadavky EUDIW dle přílohy III CIR (EU) 2024/2981 a ARF. Schéma EUDIW-CZ doplňuje nad tuto baseline následující okruhy požadavků odvozené z architekturního profilu schématu (příloha I schématu EUDIW-CZ) a z rozšířeného registru rizik (kapitola X.A):

Oblast	Požadavky nad rámec ENISA baseline	Odůvodnění rozšíření
Rámec řízení rizik (X.2)	GEN-5-02, RMF-02, RMF-03, RMF-07	Explicitní zpracování rozšířeného registru rizik schématu do rámce řízení rizik poskytovatele
Politiky a postupy (X.3)	POL-07, POL-09, POL-10	Požadavky na český jazyk, na politiku pro architekturu se vzdáleným WSCD a na

Oblast	Požadavky nad rámec ENISA baseline	Odůvodnění rozšíření
		předpoklady o uživatelském zařízení
Správa a provoz (X.4)	ORG-05, HR-02, ACC-02, CRY-05, PHY-03, NET-02, NET-03, FRD-05, BCM-04, TRM-02, SUP-06, SUP-07	Specifika vyplývající z kumulace rolí ve schématu, z použití vzdáleného WSCD, z hrozby insiderů u poskytovatele peněženky, z fyzické bezpečnosti centrálního úložiště klíčů, ze síťové bezpečnosti rozhraní instance ↔ WSCD, z kontinuity činnosti centrální kryptografické infrastruktury a z řízení dodavatelského řetězce včetně úschovy zdrojového kódu
ISMS procesy (X.5)	DEV-04, DEV-05, VUL-05, INC-06, FRD-P03	Důkazy o procesech vývoje poskytovatele peněženky a jeho subdodavatelů, rozsah řízení zranitelností napříč komponentami, koordinace incidentů mezi rolími schématu, specifické scénáře podvodů pro architekturu
Požadavky na jednotku peněženky (X.6)	WUG-05, WUG-07, WUM-05, WUP-06, WSA-06, WSCD-02, WSCD-03	Specifika architektury se vzdáleným WSCD na rozhraní WSCA ↔ WSCD a WSCA ↔ instance peněženky
Služby poskytovatele peněženky (X.7)	WPS-05, WPS-07, WPS-09, WUS-01, WUS-02, WUS-03, UPD-01 až UPD-05	Obnova a nezávislá autentizace uživatele, autentizovaná komunikace se vzdáleným WSCD, služba jednotky peněženky a proces nahrávání a aktualizace, které baseline ENISA neupravuje
Služby poskytovatele PID (X.8)	ONB-02, ONB-03, ONB-04, PIDR-02, PIDR-09, PIDR-10, PIDR-11, PIDM-03, PIDR-R06	Integrace s prostředkem eID pro onboarding, spolupráce s QTSP pro pečeti PID, specifika revokace PID, validace vůči autoritativnímu zdroji a důkaz o ověření totožnosti
Ověřovací služba (X.9)	VER-03, VER-04, VER-06, VER-07, VER-09, VER-12	Požadavky vyplývající z kumulace rolí vlastníka schématu, orgánu dohledu a ověřovací služby
Předpoklady prostředí (X.10)	ENV-01 až ENV-04, ENV-UD-01 až ENV-UD-05, ENV-INF-01 až ENV-INF-05, ENV-WSCD-01 až ENV-WSCD-03	Předpoklady o infrastruktuře poskytovatele, o vzdáleném WSCD, o lokálním externím WSCD a o uživatelském zařízení
Ochrana údajů (X.7.7, X.6.3.5)	DPR-01–DPR-03, PRV-03	Explicitní provedení čl. 5a odst. 14 a čl. 5a odst. 5 písm. b) eIDAS. Do povinného rozsahu certifikace dle čl. 5c odst. 1 spadá z čl. 5a odst. 14 pouze logické oddělení osobních údajů (DPR-01). DPR-02 a DPR-03 jsou doplněním schématu a zůstávají povinné [Sec], protože jde o přímé

Oblast	Požadavky nad rámec ENISA baseline	Odůvodnění rozšíření
		zákonné povinnosti poskytovatele peněženky.

Tabulka uvádí požadavky, které matice trasovatelnosti v kapitole X.B váže na architekturně specifická rizika CZ-01 až CZ-10 nebo označuje jako specifické pro schéma EUDIW-CZ, a dále požadavky, které nemají v baseline ENISA protějšek.

Souhrn rozšíření nad rámec ENISA baseline na úrovni registru rizik (rizika architektonicky specifická pro schéma EUDIW-CZ) je uveden v kapitole X.A. Matice trasovatelnosti jednotlivých požadavků na rizika registru rizik je uvedena v kapitole X.B.

X.2 Rámec řízení rizik

Poskytovatel služby EUDI zavede, udržuje a provozuje rámec řízení rizik v souladu s čl. 8 odst. 3 písm. b) CIR (EU) 2024/2981 a s ETSI EN 319 401 kapitolou 5. Rámec řízení rizik tvoří metodický základ pro posuzování, ošetřování a monitorování rizik spojených s poskytováním služby EUDI a pro prokázání, že bezpečnostní opatření implementovaná poskytovatelem odpovídajícím způsobem pokrývají rizika uvedená v registru rizik (příloha I CIR (EU) 2024/2981), doplněná o architekturně specifická rizika dle kapitoly X.A této přílohy.

Rámec řízení rizik odpovídá **vrstvě 3** modelu definovaného v dokumentu *Guidance for the Development of EUDIW Certification Schemes*. Hodnocení probíhá v těchto úrovních:

- Vrstva 1: Rizika definovaná na úrovni Unie (příloha I CIR (EU) 2024/2981).
- Vrstva 2: Rizika specifická pro architekturu (kapitola X.A).
- Vrstva 3: Rizika konkrétní implementace u poskytovatele (předmět této kapitoly).

X.2.1 Obecné požadavky na rámec řízení rizik

GEN-5-01: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 5.

Poznámka: ETSI EN 319 401 kapitola 5 definuje ucelený rámec řízení rizik, který zohledňuje specifická rizika spojená s definicí a architekturou služby. Rámec tím pokrývá povinnost zahrnout rizika specifická pro architekturu řešení peněženky.

GEN-5-02: Posouzení rizik prováděné poskytovatelem služby EUDI musí jako vstup zohlednit registr rizik definovaný v příloze I CIR (EU) 2024/2981, jakož i rozšíření registru rizik podle kapitoly X.A této přílohy.

Poznámka: Mapování požadavků definovaných v této příloze na rizika a hrozby identifikované v registru rizik je uvedeno v kapitole X.B této přílohy.

X.2.2 Posouzení rizik

RMF-01: Poskytovatel služby EUDI provede posouzení rizik, které zpřesňuje rizika a hrozby identifikované v registru rizik (příloha I CIR (EU) 2024/2981) a doplňuje je o rizika specifická pro konkrétní implementaci služby.

RMF-02: Posouzení rizik musí jako povinná vstupní rizika zohlednit:

- a) všechny hrozby TR1 až TR133 z registru rizik dle přílohy I CIR (EU) 2024/2981;
- b) architekturně specifická rizika schématu EUDIW-CZ dle kapitoly X.A této přílohy.

Pro každé vstupní riziko poskytovatel služby EUDI v posouzení rizik uvede:

- a) posouzení aplikovatelnosti rizika na konkrétní implementaci služby, včetně odůvodnění v případě, že riziko není aplikovatelné;
- b) posouzení významu (dopadu) a pravděpodobnosti rizika;
- c) výslednou úroveň rizika dle metodiky posouzení rizik poskytovatele.

RMF-03: Posouzení rizik musí být úplné vůči rozhraním služby EUDI. Pro každé rozhraní mezi komponentami služby a pro každé rozhraní mezi službou a externími entitami (uživatelské zařízení, externí poskytovatel služeb vytvářejících důvěru, prostředek elektronické identifikace, spoléhající se strana, registrátor spoléhajících se stran) musí posouzení rizik obsahovat relevantní rizika a jejich posouzení.

X.2.3 Ošetření rizik

RMF-04: Pro každé aplikovatelné riziko identifikované v posouzení rizik poskytovatel služby EUDI určí bezpečnostní opatření, která riziko ošetřují, a identifikuje zbytková rizika.

RMF-05: Poskytovatel služby EUDI stanoví a dokumentuje postupy a kritéria pro:

- a) výběr bezpečnostních opatření pro ošetření rizik;
- b) ověřování účinnosti každého bezpečnostního opatření (např. prostřednictvím certifikace komponenty, auditu služby/procesu, inspekce, testování);
- c) určení zbytkových rizik a způsobu jejich monitorování.

RMF-06: Poskytovatel služby EUDI definuje a dokumentuje kritéria přijatelnosti zbytkových rizik (risk appetite) a zajistí, aby zbytková rizika byla v souladu s těmito kritérii. V opačném případě poskytovatel zavede dodatečná bezpečnostní opatření nebo zbytková rizika vyhodnotí jako nepřijatelná.

RMF-07: Pro architekturně specifická rizika dle kapitoly X.A této přílohy poskytovatel služby EUDI prokáže, že zavedená bezpečnostní opatření adekvátně pokrývají tato rizika, a to v kontextu konkrétní implementace služby a jejího provozního prostředí.

X.2.4 Přezkum a schválení posouzení rizik

RMF-08: Posouzení rizik musí být přezkoumáváno a aktualizováno:

- a) nejméně jednou ročně;
- b) při významné změně architektury, rozsahu nebo provozního prostředí služby EUDI;
- c) při identifikaci nové hrozby nebo významné změně ve vývoji prostředí hrozeb, které mají dopad na službu EUDI;
- d) při významné změně registru rizik dle přílohy I CIR (EU) 2024/2981 nebo rozšíření registru rizik dle kapitoly X.A této přílohy;
- e) při významném bezpečnostním incidentu nebo závažné zranitelnosti identifikované ve službě EUDI.

Poznámka: Pojem „významná změna“ a „závažná zranitelnost“ je definován v příloze II schématu EUDIW-CZ (Kontinuita záruky a životní cyklus certifikátu).

RMF-09: Posouzení rizik a jeho aktualizace musí být formálně schváleny vrcholovým vedením poskytovatele služby EUDI. Schválení musí být zdokumentováno a musí být k dispozici certifikačnímu orgánu.

X.2.5 Monitorování rizik

RMF-10: Poskytovatel služby EUDI zavede a udržuje proces průběžného monitorování rizik, který zahrnuje:

- a) monitorování vývoje prostředí hrozeb relevantního pro službu EUDI prostřednictvím zdrojů kybernetického bezpečnostního zpravodajství, informací od CSIRT, bezpečnostních hlášení výrobců a dalších relevantních zdrojů;
- b) monitorování účinnosti implementovaných bezpečnostních opatření prostřednictvím procesů definovaných v kapitole X.5 (ISMS procesy), zejména procesu řízení zranitelností (X.5.3) a procesu řízení incidentů (X.5.4);
- c) monitorování zbytkových rizik a jejich případné změny v průběhu provozu služby;
- d) monitorování změn v konfiguraci a stavu komponent služby, které mohou mít dopad na úroveň rizik.

Výsledky monitorování jsou vstupem pro přezkum posouzení rizik dle požadavku RMF-08.

X.2.6 Sdílení posouzení rizik a trasovatelnost

RMF-11: Posouzení rizik a veškeré jeho aktualizace musí být sdíleny s certifikačním orgánem pro účely hodnocení, jakož i s orgánem dohledu na jeho vyžádání.

RMF-12: Posouzení rizik musí obsahovat trasovatelnou matici mapující bezpečnostní opatření na rizika, která tato opatření ošetřují, a obráceně. Matice musí pro každé aplikovatelné riziko prokázat:

- a) bezpečnostní opatření, která riziko ošetřují;

- b) úplnost pokrytí rizika těmito opatřeními;
- c) odůvodnění dostatečnosti opatření vůči danému riziku;
- d) identifikaci zbytkového rizika.

Poznámka: Matice trasovatelnosti bezpečnostních požadavků této přílohy X vůči registru rizik a rozšíření registru rizik dle kapitoly X.A je uvedena v kapitole X.B. Tato matice slouží jako referenční vstup pro tvorbu matice trasovatelnosti poskytovatele služby EUDI, která ji dále zpřesňuje o implementačně specifická rizika a bezpečnostní opatření konkrétní implementace služby.

X.3 Politiky a postupy

Poskytovatel služby EUDI zavede, zdokumentuje a udržuje politiky a postupy, které řídí poskytování a provoz služby EUDI. Tyto dokumenty musí být k dispozici certifikačnímu orgánu pro účely hodnocení shody a zveřejněny příslušným stranám (uživatelům, spoléhajícím se stranám, orgánu dohledu, partnerským entitám ekosystému) v souladu s požadavky uvedenými v této kapitole.

Požadavky této kapitoly se uplatňují na poskytovatele peněženky, poskytovatele PID a provozovatele ověřovací služby. Konkrétní rozsah dokumentu politik a postupů se odvíjí od certifikační oblasti, v níž žadatel žádá o certifikaci dle přílohy I schématu.

X.3.1 Prohlášení o postupech služby peněženky

POL-01: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 6.1.

Poskytovatel služby EUDI definuje a zveřejní Prohlášení o postupech služby peněženky (Wallet Service Practice Statement), které popisuje postupy používané při poskytování a provozu služby EUDI.

Prohlášení musí pokrývat:

- a) identifikaci poskytovatele služby EUDI, jeho právní status a kontaktní údaje;
- b) popis poskytované služby EUDI a jejích komponent v souladu s přílohou I schématu EUDI-W-CZ;
- c) politiku a postupy řízení rizik dle kapitoly X.2;
- d) politiky a postupy provozu služby dle kapitol X.4, X.5 a X.7 až X.9;
- e) závazky a odpovědnosti poskytovatele, uživatelů a spoléhajících se stran;
- f) postupy podávání stížností a sporné řízení.

X.3.2 Podmínky poskytování služby

POL-02: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 6.2.

Poskytovatel služby EUDI zpřístupní všem uživatelům a spoléhajícím se stranám podmínky poskytování služby.

POL-03: Zveřejněné podmínky musí obsahovat zásady ochrany osobních údajů.

POL-04: Poskytovatel služby EUDI definuje a zavede politiky a postupy pro zajištění toho, aby uživatelé služby byli včas a spolehlivě informováni o jakýchkoli změnách v definici služby a ve všech použitelných podmínkách poskytování služby a politice ochrany osobních údajů pro danou službu.

POL-05: Poskytovatel služby EUDI definuje a zavede politiky a postupy, které zajišťují úplné a správné odpovědi na žádosti o informace.

POL-06: Podmínky poskytování služby musí obsahovat seznam služeb poskytovaných bezplatně, který musí zahrnovat alespoň vydávání, používání a odvolávání peněženek EUDI fyzickým osobám a možnost fyzických osob podepisovat kvalifikovanými elektronickými podpisy pro neprofesní účely.

POL-07: Podmínky poskytování služby a související dokumenty uvedené v této kapitole musí být zveřejněny v českém jazyce. Poskytovatel služby EUDI může zveřejnit i jazykové mutace, přičemž závaznou verzí v případě sporu je česká jazyková verze.

X.3.3 Politika bezpečnosti informací a sítí

POL-08: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 6.3, s výjimkou požadavku REQ-6.3-04.

Poskytovatel služby EUDI definuje, zavede a udržuje Politiku bezpečnosti informací a sítí (Information and Network Security Policy), která řeší ochranu všech aktiv souvisejících s poskytováním služby EUDI.

Poznámka: Požadavek REQ-6.3-04 normy ETSI EN 319 401 byl vypuštěn, protože se týká oznamování změn dozorovému orgánu. V případě certifikované služby EUDI oznamovací povinnosti existují, ale jsou definovány v certifikačním schématu jako pravidlo schématu (nikoli jako požadavek), s oznámením certifikačnímu orgánu, který za specifických okolností informuje orgán dohledu. Podrobnosti oznamovacích povinností jsou uvedeny v hlavním dokumentu schématu a v příloze II schématu.

POL-09: Politika bezpečnosti informací a sítí musí výslovně adresovat předpoklady o provozním prostředí definované v kapitole X.10 této přílohy, a to:

a) pro prostředí, která poskytuje poskytovatel služby EUDI (včetně prostředí poskytovaných třetí stranou smluvně najatou poskytovatelem), musí politika definovat bezpečnostní opatření a požadavky na důkazy, že prostředí splňuje předpoklady;

b) pro prostředí, která poskytuje uživatel peněženky, musí politika definovat ověřovací mechanismy a bezpečnostní opatření k ověření předpokladů o uživatelském zařízení a reakci na situace, kdy předpoklady nejsou splněny.

POL-10: Politika bezpečnosti informací a sítí musí pokrývat bezpečnost komunikačních kanálů mezi komponentami jednotky peněženky provozovanými na různých systémech nebo zařízeních, zejména komunikační kanál mezi instancí peněženky a WSCD v architekturách, kde WSCD není provozován na stejném zařízení jako instance peněženky.

Poznámka: Požadavek POL-10 se vztahuje zejména na architekturu se vzdáleným WSCD a na architekturu s lokálním externím WSCD. Konkrétní bezpečnostní opatření vyplývající z této politiky jsou definována v kapitolách X.4.5 (kryptografická opatření), X.4.8 (síťová bezpečnost) a X.6.5 (požadavky na WSCA).

X.4 Správa a provoz poskytovatele

Tato kapitola definuje požadavky na správu a provoz služeb EUDI, založené na ETSI EN 319 401 kapitola 7 a doplněné o požadavky specifické pro ekosystém EUDIW vyplývající z CIR (EU) 2024/2981 a z architekturního profilu schématu EUDIW-CZ. Není-li stanoveno jinak, požadavky v této kapitole se vztahují na všechny poskytovatele služeb EUDI zapojené do poskytování řešení peněženky a systému eID, v jehož rámci je poskytována — minimálně na poskytovatele peněženky, poskytovatele PID a provozovatele ověřovací služby.

X.4.1 Vnitřní organizace

X.4.1.1 Obecné požadavky

ORG-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.1.1, zahrnující požadavky REQ-7.1.1-01 až REQ-7.1.1-07, pokrývající organizační spolehlivost, nediskriminační přístup, finanční stabilitu, vyřizování stížností a uspořádání subdodavatelských vztahů.

ORG-02 [Sec]: Poskytovatel služby EUDI musí efektivně provozovat systém řízení bezpečnosti informací (ISMS) založený na ověřených standardech nebo principech pro řízení a kontrolu rizik bezpečnosti informací.

X.4.1.2 Spolehlivost organizace

ORG-03 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.1.2.

X.4.1.3 Oddělení povinností

ORG-04 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.1.3.

ORG-05 [Sec, Cond]: V případě, že stejný subjekt zastává v ekosystému EUDIW více rolí (např. role poskytovatele peněženky a poskytovatele PID, role poskytovatele peněženky a provozovatele ověřovací služby, nebo role vlastníka schématu, orgánu dohledu a registrátora spoléhajících se stran současně), musí subjekt zavést a dokumentovat organizační opatření pro:

- a) jednoznačné vymezení odpovědností jednotlivých rolí a jejich oddělení v organizační struktuře;
- b) oddělení personálu vykonávajícího činnosti jednotlivých rolí, zejména v pozicích s privilegovaným přístupem k citlivým aktivům;

c) oddělení informačních systémů a technické infrastruktury podporujících jednotlivé role, pokud je to přiměřené rizikům plynoucím z kumulace rolí;

d) mechanismy předcházení střetu zájmů mezi jednotlivými rolemi a transparentního rozhodování;

e) nezávislé monitorování a kontrolní mechanismy, pokud totéž organizační pracoviště zastává současně roli regulovanou a roli dohledovou.

Organizační opatření podle tohoto požadavku musí být předmětem auditu ze strany certifikačního orgánu a musí být aktualizována při každé změně v rozsahu rolí zastávaných subjektem.

Poznámka: Požadavek ORG-05 pokrývá situaci kumulace dohledových a regulovaných rolí u jednoho subjektu, která je architekturně specifickou charakteristikou schématu EUDIW-CZ (kapitola X.A, riziko CZ-10).

X.4.2 Lidské zdroje

HR-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.2, v plném rozsahu, pokrývající důvěryhodnost personálu, kompetence, školení, svěřené role (trusted roles), prověření (background checks) a formální jmenování.

HR-02 [Sec]: Personál poskytovatele služby EUDI s privilegovaným přístupem ke zdrojovému kódu instance peněženky, ke konfiguraci WSCA, k administrativním rozhraním WSCD nebo k citlivým kryptografickým materiálům musí podléhat rozšířeným prověrkám a bezpečnostním požadavkům odpovídajícím kritičnosti aktiv, k nimž má daná role přístup.

Prověrky musí zahrnovat:

- a) ověření odborné způsobilosti a zkušeností relevantních pro vykonávanou roli;
- b) ověření bezúhonnosti prostřednictvím výpisu z rejstříku trestů a dalších kontrol odpovídajících citlivosti role (zejména u rolí s privilegovaným přístupem k WSCA, WSCD, podpisovým klíčům pro distribuci softwaru a administrativním rozhraním kritických komponent);
- c) bezpečnostní školení před nástupem do role a pravidelná opakovací školení, včetně školení k ochraně osobních údajů a ke specifickým hrozbám insidera.

Poznámka: Požadavek HR-02 je architekturně specifickým rozšířením reagujícím na hrozbu zneužití privilegovaného přístupu personálu poskytovatele peněženky k citlivým komponentám (kapitola X.A, riziko CZ-05).

X.4.3 Správa aktiv

X.4.3.1 Obecné požadavky

AST-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.3.1.

X.4.3.2 Klasifikace aktiv

AST-02 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.3.2.

Poznámka: Norma nedefinuje konkrétní požadavky pro jednotlivé kategorie aktiv, ale klasifikace aktiv typu osobní údaje, kryptografická data nebo autentizační data musí být prováděna s velkou obezřetností, bez ohledu na úroveň jejich kritičnosti.

AST-03 [Sec]: Poskytovatel služby EUDI musí definovat v klasifikačním schématu nejméně jednu úroveň klasifikace, která odpovídá kritickým aktivům chráněným v rámci WSCA/WSCD.

Poznámka: Kromě jednotky peněženky, pokud jsou některá z těchto kritických aktiv identifikována na infrastruktuře backendu poskytovatele peněženky, musí být rovněž adekvátně chráněna. Další požadavky vztahující se na kritická aktiva jsou definovány v této příloze, zejména v kapitolách X.4.5 (kryptografická opatření) a X.6 (požadavky na jednotku peněženky).

AST-04 [Sec]: Poskytovatel služby EUDI by měl definovat úroveň klasifikace odpovídající aktivům zpracovávaným na uživatelském zařízení, která jsou vystavena specifickým rizikům.

Poznámka: Požadavek AST-04 je doporučením. Klasifikace aktiv pro peněženky EUDI je zpravidla složitější než pro klasického poskytovatele služeb vytvářejících důvěru, protože část aktiv je zpracovávána v prostředí mimo přímou kontrolu poskytovatele. Předpoklady o uživatelském zařízení a související ověřovací mechanismy jsou definovány v kapitole X.10.

AST-05 [Sec]: Poskytovatel služby EUDI musí definovat jednu nebo více úrovní ochrany vhodných pro aktiva související s vazbou atestací na zařízení, včetně alespoň jedné, která umožňuje vazbu na WSCA/WSCD.

Poznámka: Vzhledem k předpokladu této přílohy, že se používá jedna WSCA, by povinná úroveň ochrany (tj. nejvyšší úroveň) měla být implementována ve WSCA.

X.4.3.3 Úložná média a nakládání s aktivy

AST-06 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.3.3.

X.4.4 Řízení přístupu

ACC-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.4, konkrétně podkapitoly 7.4.1 (obecné), 7.4.2 (privilegované a systémové administrátorské účty), 7.4.3 (administrativní systémy), 7.4.4 (identifikace), 7.4.5 (autentizace) a 7.4.6 (vícefaktorová autentizace).

Poznámka: ETSI EN 319 401 kapitoly 7.4.1 až 7.4.6 uceleně pokrývají řízení přístupu na infrastruktuře poskytovatele služby. Dodatečné požadavky na autentizaci uživatelů peněženky jsou definovány v kapitole X.6.3.1 (Autentizace uživatele).

ACC-02 [Sec]: Přístup k infrastruktuře provozující WSCD (zejména vzdálený WSCD provozovaný ve formě HSM) a k administrativním rozhraním WSCD musí podléhat rozšířeným opatřením řízení přístupu, zahrnujícím:

- a) síťovou segmentaci izolující administrativní rozhraní WSCD od ostatních sítí;
- b) vícefaktorovou autentizaci pro veškerý administrativní přístup k WSCD;

- c) řízení privilegovaného přístupu (Privileged Access Management, PAM) se záznamem administrativních relací;
- d) princip dvojité kontroly (dual control) pro kritické operace s konfigurací WSCD a s kryptografickými materiály;
- e) kontinuální monitorování a automatizované upozorňování na anomální přístupové vzory;
- f) úplnou a nepopíratelnou auditní stopu všech administrativních operací na WSCD.

Poznámka: Požadavek ACC-02 je architekturně specifickým rozšířením reagujícím na skutečnost, že WSCD je centrální komponentou, jejíž kompromitace má potenciálně systémový dopad na celý ekosystém služby EUDI. Požadavek se v plné šíři uplatní zejména u architektury se vzdáleným WSCD (kapitola X.A, rizika CZ-01 a CZ-06). Pro architekturu s lokálním externím WSCD se požadavek uplatní v rozsahu odpovídajícím povaze WSCD a jeho provozního prostředí.

X.4.5 Kryptografická opatření

CRY-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.5.

CRY-02 [Sec]: Kryptografie používaná při implementaci řešení peněženky musí implementovat doporučené mechanismy uvedené v dokumentu ECCG Agreed Cryptographic Mechanisms, s ohledem na relevantní pokyny k implementaci.

CRY-03 [Sec]: Kritická kryptografická aktiva zpracovávaná na systémech poskytovatele služby EUDI, mimo jednotku peněženky a WSCA/WSCD, musí být chráněna úrovní odolnosti proti útokům srovnatelnou s úrovní WSCA a WSCD. K ochraně těchto aktiv musí být použit hardwarový bezpečnostní modul (HSM). Způsob jeho ovládání a přístupu k němu musí být zabezpečen proti zneužití stejně přísně jako u provozovatele WSCD, s ohledem na konkrétní provozní podmínky.

Poznámka: Požadavek na použití HSM vyplývá z nutnosti dosáhnout u kritických kryptografických aktiv zpracovávaných mimo jednotku peněženky odolnosti srovnatelné s WSCA a WSCD.

CRY-04 [Sec]: WSCD, na němž jsou hostovány kryptografické funkce pro kritická aktiva peněženky, musí být certifikován minimálně na úrovni EAL4 s posouzením zranitelnosti AVA_VAN.5 v rámci EUCC nebo schématu Common Criteria, nebo musí poskytovat ekvivalentní úroveň záruky v souladu s přílohou IX schématu EUDIW-CZ.

CRY-05 [Sec]: Kryptografické kanály mezi instancí peněženky a WSCD, pokud WSCD není provozován na témže zařízení jako instance peněženky, musí zajistit:

- a) integritu, autenticitu a důvěrnost komunikace mezi těmito komponentami;
- b) ochranu proti opakování, přehrání a injektování zpráv (anti-replay);
- c) vazbu relace na konkrétní jednotku peněženky (session binding);

d) zamezení toho, aby zprostředkující infrastrukturní komponenty měly přístup k obsahu kryptografických operací (end-to-end ochrana).

Konkrétní technické požadavky na síťovou bezpečnost tohoto kanálu jsou definovány v kapitole X.4.8.

Poznámka: Požadavek CRY-05 se uplatní zejména v architektuře se vzdáleným WSCD.

X.4.6 Fyzická a environmentální bezpečnost

PHY-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.6.

Poznámka: ETSI EN 319 401 kapitola 7.6 zahrnuje požadavky REQ-7.6-01 až REQ-7.6-05, pokrývající řízení fyzického přístupu, prevenci ztráty, bezpečnostní perimetry a umístění kritických komponent.

PHY-02 [Sec]: Pro komponenty kritické pro bezpečný provoz služby EUDI, zejména ty, které byly certifikovány samostatně (WSCD, WSCA, HSM pro zpracování kritických kryptografických aktiv mimo WSCD), musí ochrana jejich fyzického prostředí splňovat požadavky bezpečnostních pokynů těchto komponent na očekávané úrovni záruky.

Poznámka: Požadavek PHY-02 doplňuje obecná ustanovení ETSI EN 319 401 kapitoly 7.6 o komponenty, jejichž bezpečnost je kritická. Pokrývá minimálně WSCD a WSCA v případech, kdy jsou provozovány v zařízeních poskytovatele služby EUDI, a zejména WSCA v případech, kdy je provozována mimo WSCD.

PHY-03 [Sec, Cond]: Datová centra hostující WSCD provozovaný ve formě vzdáleného HSM a další infrastrukturu kritickou pro provoz služby EUDI musí splňovat fyzické bezpečnostní požadavky odpovídající ochraně kritických aktiv na úrovni záruky „vysoká“ dle CIR (EU) 2015/1502, zahrnující minimálně:

- a) řízení fyzického přístupu do prostor s WSCD a souvisejícími komponentami na principu dvojité kontroly (dual control), se zaznamenáváním všech přístupů;
- b) environmentální kontroly zajišťující ochranu před požárem, zaplavením, výpadkem napájení, přepětím a poruchou klimatizace;
- c) opatření proti neoprávněné fyzické manipulaci (tamper-evident a tamper-responsive mechanismy) na hardware WSCD;
- d) kontinuální monitorování fyzického prostředí a detekci neoprávněných pokusů o vstup;
- e) oddělení zón s různou úrovní citlivosti a definované postupy přechodu mezi zónami.

Poznámka: Požadavek PHY-03 je architekturně specifickým rozšířením reagujícím na skutečnost, že v profilu EUDI-W-CZ představuje WSCD centrální komponentu chránící kryptografická aktiva všech uživatelů služby. Existující certifikace fyzické bezpečnosti datového centra (např. dle EN ISO/IEC 27001 s rozšířením o fyzickou bezpečnost, nebo certifikace TIER) mohou být použity jako vstup analýzy závislostí dle přílohy IX schématu.

X.4.7 Provozní bezpečnost

OPS-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.7.

Poznámka: ETSI EN 319 401 kapitola 7.7 zahrnuje požadavky na dokumentované provozní postupy, řízení změn, plánování kapacity, oddělení vývojového, testovacího a produkčního prostředí, ochranu proti škodlivému kódu a aplikaci bezpečnostních oprav (patching).

OPS-02 [Sec]: Poskytovatel služby EUDI zavede a implementuje opatření zajišťující, aby v provozu byla použita výhradně aktuálně certifikovaná verze řešení peněženky, včetně:

- a) procesu ověření, že verze komponent nasazených do produkčního prostředí odpovídá verzím pokrytým platným certifikátem;
- b) kontrolních mechanismů zabraňujících nasazení necertifikovaných verzí komponent do produkčního prostředí;
- c) auditní stopy všech verzí nasazených v produkčním prostředí, umožňující zpětné ověření souladu s certifikátem;
- d) postupu oznámení certifikačnímu orgánu v případech, kdy je nezbytně nutné nasadit verzi, která ještě nebyla pokryta certifikátem (např. nasazení kritické bezpečnostní opravy před dokončením dozorového hodnocení).

X.4.8 Síťová bezpečnost

NET-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.8.

Poznámka: ETSI EN 319 401 kapitola 7.8 zahrnuje požadavky REQ-7.8-01 až REQ-7.8-09, pokrývající síťovou segmentaci, zónové řízení přístupu, oddělení administrativní sítě a ochranu proti útokům.

NET-02 [Sec, Cond]: Komunikační kanál mezi instancí peněženky a WSCA, pokud WSCA není provozována na témže zařízení jako instance peněženky, musí být chráněn následujícími síťovými opatřeními:

- a) šifrováním pomocí protokolu TLS 1.3 nebo ekvivalentního protokolu poskytujícího srovnatelnou úroveň ochrany, s použitím kryptografických mechanismů dle dokumentu ECCG Agreed Cryptographic Mechanisms;
- b) vzájemnou autentizací koncových bodů s použitím důvěryhodných kotev definovaných poskytovatelem služby EUDI;
- c) vazbou relace (session binding) na konkrétní jednotku peněženky a mechanismy proti opakovanému přehrání zpráv (anti-replay);
- d) síťovou segmentací zajišťující, že zprostředkující infrastrukturní komponenty (včetně síťových zařízení a zařízení pro koncové síťové služby) nemohou přistupovat k obsahu kryptografických operací ani je modifikovat.

Poznámka: Požadavek NET-02 je architekturně specifickým rozšířením pro architektury, v nichž je WSCA provozována mimo zařízení uživatele, zejména pro architekturu se vzdáleným WSCD (kde WSCA typicky běží na serveru sousedícím s WSCD). Pro architekturu s lokálním externím WSCD, kde je WSCA integrována s

WSCD jako součást externího zařízení (typicky čipové karty), se opatření tohoto požadavku přiměřeně aplikují na lokální rozhraní (NFC, BLE, USB) mezi instancí peněženky a externím zařízením.

Poznámka 2: Bezpečnost rozhraní mezi WSCA a WSCD je samostatným předmětem hodnocení v rámci certifikace WSCA dle EUCC; v architektuře se vzdáleným WSCD je toto rozhraní typicky interní serverové rozhraní, jehož bezpečnostní vlastnosti jsou pokryty certifikací WSCA a posouzením předpokladů jejího provozního prostředí (ENV-INF-04).

NET-03 [Sec, Cond]: Administrativní přístup k infrastruktuře provozující kritické komponenty služby EUDI (zejména WSCD, HSM, servery hostující PID provisioning) musí být oddělen od produkčního síťového provozu vlastní síťovou zónou, chráněn přes samostatný bastion/jump server s vícefaktorovou autentizací a zaznamenáván na principu nezávislého logování.

Poznámka: Požadavek NET-03 doplňuje NET-01 (ETSI EN 319 401 kap. 7.8) o specifické požadavky na oddělení administrativní sítě pro kritické komponenty architektury. Společně s požadavkem ACC-02 (X.4.4) tvoří vrstvenou ochranu administrativních rozhraní.

X.4.9 Řízení zranitelností a incidentů

VIM-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.9, konkrétně podkapitoly 7.9.1 (monitorování a logování), 7.9.2 (reakce na incidenty), 7.9.3 (hlášení), 7.9.4 (hodnocení a klasifikace událostí) a 7.9.5 (přezkum po incidentu).

Poznámka: ETSI EN 319 401 kapitola 7.9 pokrývá řízení incidentů a zranitelností na úrovni infrastruktury poskytovatele. Specifické řízení zranitelností pro peněženku EUDI je dále detailně definováno v kapitole X.5.3 této přílohy a v kláncích 21 až 28 hlavního textu schématu.

X.4.9.1 Řízení podvodů

FRD-01 [Sec]: Poskytovatel služby EUDI musí být průběžně informován o podvodech a pokusech o podvody týkajících se služeb, které poskytuje.

Poznámka 1: Pojem „podvod“ se v tomto kontextu rozumí jako pokus škodlivého subjektu přimět uživatele peněženky EUDI k provedení operace jménem škodlivého subjektu, což umožňuje zneužití identity nebo atributů uživatele, aniž by bylo využito konkrétní zranitelnosti služby.

Poznámka 2: Hlavní charakteristikou podvodu je, že se neopírá o zranitelnost certifikované služby IKT, ale buď o zneužití uživatele (sociální inženýrství), nebo o využití zranitelnosti či problému na uživatelském zařízení.

FRD-02 [Sec]: Poskytovatel služby EUDI analyzuje podvod nebo pokus o podvod a identifikuje, pokud je to možné, příležitost zneužitou škodlivým subjektem a kořenovou příčinu v implementaci své služby.

Poznámka: Cílem je identifikovat, zda konkrétní prvek peněženky EUDI (typicky v uživatelském rozhraní) poskytl škodlivému subjektu příležitost přesvědčit oběť k provedení operace jeho jménem. Taková příčina

nemusí být vždy přítomna — škodlivý subjekt může využít i jiné prostředky (donucení, obecnou dezorientaci uživatele).

FRD-03 [Sec, Cond]: Pokud byla identifikována kořenová příčina, která vytváří příležitost pro podvod, musí být následně řízena jako zranitelnost v souladu s kapitolou X.5.3 této přílohy a články 21 až 28 hlavního textu schématu.

Poznámka: Cílem je omezit příležitost pro škodlivé subjekty tím, že konkrétní prvek, který jim pomáhá podvod spáchat, je řízen jako zranitelnost vyžadující zmírnění. Dalším cílem je umožnit, aby informace o podvodu byla v souladu s povinnostmi řízení zranitelností a zveřejňování distribuována národním orgánům pro certifikaci kybernetické bezpečnosti (NÚKIB).

FRD-04 [Sec, Cond]: Pokud je podvod nebo pokus o podvod řízen jako zranitelnost, poskytovatel služby EUDI sdílí výslednou zprávu o posouzení dopadu a navrhovaná zmírňující opatření s certifikačním orgánem, bez ohledu na významnost dopadu.

FRD-05 [Sec]: Proces řízení podvodů musí zahrnovat mechanismy pro detekci anomálních vzorů v ekosystému služby EUDI, včetně minimálně:

- a) neobvyklých rychlostí aktivace jednotek peněženky, zejména prostřednictvím onboardingu přes prostředek elektronické identifikace;
- b) vzorů neúspěšných pokusů o autentizaci vůči WSCD a dalším kritickým komponentám;
- c) anomálních objemů transakcí vycházejících z konkrétních jednotek peněženky nebo směřujících na konkrétní spoléhající se strany;
- d) koordinovaných pokusů o podvody cílících na registr spoléhajících se stran nebo na službu pečetení PID.

Výsledky detekce jsou vstupem pro analýzu dle požadavku FRD-02 a pro monitorování rizik dle požadavku RMF-10.

Poznámka: Požadavek FRD-05 je architekturně specifickým rozšířením reagujícím na centralizovanou povahu komponent v ekosystému EUDIW-CZ. Centralizace (jeden WSCD, jeden onboarding flow, jeden registr spoléhajících se stran) umožňuje účinnější detekci anomálií, ale zároveň vytváří přitažlivý cíl pro koordinované útoky.

X.4.10 Shromažďování důkazů

EVD-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.10 relevantní pro konkrétní role.

Poznámka: Tyto požadavky pokrývají požadavky na vedení záznamů.

EVD-02 [Sec]: Záznamy shromažďované v rámci požadavku EVD-01 musí pokrývat minimálně:

- a) všechny operace s kritickými aktivy peněženky (operace vydávání, použití, revokace a ukončení platnosti PID a atestací);

- b) všechny administrativní operace na WSCD, WSCA a souvisejících komponentách;
- c) všechny bezpečnostní události identifikované v rámci monitorování dle požadavku VIM-01;
- d) všechny incidenty a pokusy o podvody identifikované v rámci procesů dle kapitol X.4.9 a X.4.9.1.

Záznamy musí být chráněny proti modifikaci a smazání, uchovávány po dobu stanovenou právními předpisy České republiky (minimálně však po dobu platnosti certifikátu a dva následující roky) a v relevantních případech k dispozici orgánu dohledu, certifikačnímu orgánu a orgánům činným v trestním řízení.

Poznámka: Požadavek EVD-02 zpřesňuje obecné záznamové povinnosti ETSI EN 319 401 kapitoly 7.10 specifickými kategoriemi záznamů relevantními pro ekosystém EUDIW. Požadavky na uchovávání záznamů vycházejí z obecných povinností dle eIDAS a nařízení (EU) 2016/679 (GDPR); konkrétní doby uchovávání pro jednotlivé kategorie záznamů jsou stanoveny v právních předpisech České republiky a v podmínkách poskytování služby dle kapitoly X.3.2.

X.4.11 Řízení kontinuity činnosti

X.4.11.1 Obecné požadavky

BCM-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.11.1.

X.4.11.2 Zálohování

BCM-02 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.11.2.

X.4.11.3 Krizové řízení

BCM-03 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.11.3.

X.4.11.4 Specifická ustanovení pro kontinuitu kritických komponent

BCM-04 [Sec, Cond]: Plán kontinuity činnosti poskytovatele služby EUDI musí výslovně adresovat dostupnost WSCD a dalších kritických komponent služby a zahrnovat minimálně:

- a) mechanismy přepnutí (failover) pro infrastrukturu WSCD, zajišťující nepřetržitou dostupnost kryptografických operací pro aktivní jednotky peněženky;
- b) cílové doby obnovy (Recovery Time Objective, RTO) a cílové body obnovy (Recovery Point Objective, RPO) pro kryptografický klíčový materiál a pro další kritická aktiva, přičemž tyto hodnoty musí být přiměřené kritičnosti služby a odůvodněné v posouzení rizik dle kapitoly X.2;
- c) postupy pro obnovu jednotky peněženky v případě ztráty nebo poškození uživatelského zařízení, zajišťující, že proces obnovy nenaruší bezpečnost identity uživatele ani integritu vydaných PID a atestací;
- d) geografickou nebo logickou redundanci kritických komponent, pokud to povaha komponenty a posouzení rizik vyžaduje;
- e) pravidelné testování plánu kontinuity činnosti včetně scénářů výpadku WSCD, výpadku konektivity mezi instancí peněženky a WSCD, a kompromitace kryptografického klíčového materiálu.

Poznámka: Požadavek BCM-04 je architekturně specifickým rozšířením reagujícím na centralizovaný charakter WSCD v profilu schématu EUDIW-CZ. Centralizovaný WSCD je jediným bodem selhání pro kryptografické operace všech aktivních jednotek peněženky. Jeho nedostupnost znamená plošný výpadek služby. Specifické požadavky na obnovu jednotky peněženky dle písm. c) jsou dále rozpracovány v kapitole X.7.5.

X.4.12 Ukončení činnosti poskytovatele

TRM-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.12.

Poznámka: V případě ukončení činnosti poskytovatele služby EUDI musí být zajištěna řádná migrace jednotek peněženky na následného poskytovatele, nebo jejich řízená revokace a deaktivace, s minimálním dopadem na uživatele.

TRM-02 [Sec, Cond]: Plán ukončení činnosti poskytovatele služby EUDI musí zahrnovat minimálně:

- a) ustanovení pro migraci nebo bezpečný přenos všech záznamů o jednotkách peněženky a souvisejícího kryptografického klíčového materiálu na následného poskytovatele schváleného vlastníkem schématu nebo orgánem dohledu, nebo předat orgánu dohledu pro evidenční účely, přičemž v architekturách využívajících vzdálený WSCD musí plán zahrnovat postup předání správy nebo fyzického převodu WSCD infrastruktury;
- b) alternativně postup pro řádnou revokaci a deaktivaci všech jednotek peněženky a znehodnocení kryptografického klíčového materiálu;
- c) postup informování uživatelů služby v dostatečném předstihu před plánovaným ukončením činnosti alespoň 3 měsíce předem, s uvedením možností přechodu k jinému poskytovateli služby EUDI a dopadů na platnost vydaných PID a atestací;
- d) postup předání záznamů dle požadavku EVD-02 následnému poskytovateli nebo orgánu dohledu v souladu s právními předpisy České republiky o uchování záznamů;
- e) finanční a smluvní zajištění realizace plánu ukončení, například formou depositního účtu, pojištění nebo bankovní záruky, v rozsahu přiměřeném kritičnosti služby.

Plán ukončení činnosti musí být předem projednán s orgánem dohledu a aktualizován nejméně jednou ročně, nebo při každé významné změně v rozsahu poskytované služby nebo ve smluvním postavení poskytovatele.

Poznámka: Požadavek TRM-02 je architekturně specifickým rozšířením reagujícím na skutečnost, že role poskytovatele může být časově omezena nebo ukončena z provozních, smluvních či regulatorních důvodů.

X.4.13 Shoda s předpisy

CMP-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.13.

Poznámka: Tyto požadavky pokrývají ustanovení oddílu 2.4.7 přílohy k CIR (EU) 2015/1502, zejména proto, že certifikace služby EUDI dle tohoto schématu vyžaduje pravidelné hodnocení třetí stranou (certifikačním orgánem) s dozorovými činnostmi dle přílohy II schématu.

CMP-02 [Sec]: Poskytovatel služby EUDI zajistí a dokumentuje shodu služby s relevantními právními předpisy EU a České republiky, v platném znění, zejména s:

- a) právními předpisy o ochraně osobních údajů, zejména nařízením (EU) 2016/679 (GDPR) a zákonem č. 110/2019 Sb., o zpracování osobních údajů;
- b) právními předpisy o kybernetické bezpečnosti, zejména zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, který transponuje směrnici (EU) 2022/2555 (NIS2), a jeho prováděcími předpisy;
- c) právními předpisy o elektronické identifikaci a službách vytvářejících důvěru, zejména nařízením (EU) č. 910/2014 ve znění nařízení (EU) 2024/1183 a souvisejícími prováděcími právními předpisy, zákonem č. 250/2017 Sb., o elektronické identifikaci, a zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce;
- d) právními předpisy o informačních systémech veřejné správy, pokud se vztahují na provoz služby EUDI;
- e) právními předpisy o archivnictví a spisové službě, pokud se vztahují na záznamy shromažďované v rámci služby EUDI dle požadavku EVD-01.

Poznámka: Požadavek CMP-02 zpřesňuje obecné ustanovení ETSI EN 319 401 kapitoly 7.13 o konkrétní právní předpisy České republiky relevantní pro provoz služby EUDI. Poskytovatel služby EUDI musí průběžně sledovat změny těchto předpisů a promítat je do svých politik a postupů dle kapitoly X.3. Specifické certifikované požadavky na ochranu údajů dle čl. 5c odst. 1 eIDAS stanoví kap. X.7.7 a X.6.3.5. CMP-02 pokrývá shodu s GDPR jako celkem.

X.4.14 Dodavatelský řetězec

X.4.14.1 Politika dodavatelského řetězce

SUP-01 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.14.1.

X.4.14.2 Postupy a procesy dodavatelského řetězce

SUP-02 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.14.2.

X.4.14.3 Odpovědnost, dohody s třetími stranami a SLA

SUP-03 [Sec]: Použijí se požadavky stanovené v ETSI EN 319 401 kapitola 7.14.3.

SUP-04 [Sec, Cond]: Pokud poskytovatel služby EUDI využívá služby třetích stran, musí všechny relevantní požadavky této přílohy splnit i tyto třetí strany.

Poznámka: Činnosti vykonávané třetími stranami spadají plně do rozsahu certifikace a je třeba poskytnout důkazy o tom, že třetí strana tyto požadavky splňuje. Například při využití cloudových služeb musí být k

dispozici odpovídající dokumentace o záruce pro danou cloudovou službu (zejména certifikáty, auditní zprávy, atestace), která se posuzuje v rámci analýzy závislostí dle přílohy IX schématu.

X.4.14.4 Softwarová skladba komponent

SUP-05 [Sec]: Poskytovatel služby EUDI musí udržovat softwarovou skladbu komponent (Software Bill of Materials, SBOM) pro všechny komponenty řešení peněženky, v běžně používaném a strojově čitelném formátu. SBOM musí pokrývat:

- a) přímé (top-level) závislosti každé komponenty;
- b) tranzitivní závislosti do hloubky automatizovaně zjistitelné z package managerů, build systémů a analýzy sestavených artefaktů. Cílem je úplný strom závislostí, nikoli pouze jeho první úroveň;
- c) pro každou položku minimálně název, dodavatele/původ, verzi a jednoznačný identifikátor (např. PURL nebo CPE) umožňující automatizované párování se zdroji informací o zranitelnostech.

Poznámka: SBOM je vstupem pro proces řízení zranitelností dle kapitoly X.5.3 a pro článek 22 hlavního textu schématu (postupy řízení zranitelností). Strojově čitelnými formáty se rozumí zejména SPDX (ISO/IEC 5962) a CycloneDX.

X.4.14.5 Posouzení dodavatelů kritických komponent

SUP-06 [Sec]: Poskytovatel služby EUDI musí provést a pravidelně aktualizovat posouzení bezpečnosti klíčových dodavatelů služby EUDI, kteří poskytují komponenty nebo služby s kritickým dopadem na bezpečnost služby EUDI.

Posouzení musí zahrnovat minimálně:

- a) dodavatele poskytujícího infrastrukturu pro hostování kritických komponent (zejména WSCD a jeho okolí);
- b) dodavatele poskytujícího službu pečetění PID;
- c) dodavatele zajišťujícího onboarding uživatele prostřednictvím prostředku elektronické identifikace;
- d) dodavatele hardwaru WSCD (výrobce HSM nebo čipové karty);
- e) dodavatele systému poskytovatele PID (pokud je vyvíjen externím dodavatelem);
- f) klíčové subdodavatele dodavatelů uvedených v písm. a) až e).

Posouzení musí ověřovat, že bezpečnostní opatření každého dodavatele odpovídají kritičnosti aktiv nebo služeb, které tento dodavatel poskytuje, a to minimálně formou ověření existujících certifikací a auditních zpráv dodavatele dle přílohy IX schématu. V případě absence vhodných důkazů o záruce musí posouzení zahrnovat samostatné auditní činnosti.

Poznámka: Požadavek SUP-06 je architekturně specifickým rozšířením reagujícím na fakt, že v profilu schématu EUDIW-CZ je služba EUDI rozdělena mezi vícero subjektů s vysokou kritickou závislostí. Bezpečnost (security posture) každého z klíčových dodavatelů přímo ovlivňuje bezpečnost celé služby.

SUP-07 [Sec, Cond]: Pro kritické komponenty řešení peněženky vyvíjené externími dodavateli musí poskytovatel služby EUDI zavést smluvní mechanismus úschovy zdrojového kódu (code escrow) u nezávislé třetí strany usazené v Evropské unii. Mechanismus musí splňovat následující podmínky:

- a) rozsah artefaktů — úschova zahrnuje úplný zdrojový kód, dokumentaci sestavení (build instructions), seznam použitých knihoven třetích stran s jejich verzemi (SBOM dle požadavku SUP-05) a dokumentaci nezbytnou pro pokračování vývoje a údržby komponenty třetí stranou;
- b) komponenty v rozsahu úschovy — minimálně instance peněženky, WSCA a systém poskytovatele PID; úplný seznam je dokumentován v rámci požadavku TRM-02 v kapitole X.4.12;
- c) podmínky uvolnění (release conditions) — úpadek nebo likvidace dodavatele, ukončení činnosti bez zajištění nástupce, závažné a opakované porušení smluvních povinností v oblasti údržby a bezpečnostních aktualizací, nebo rozhodnutí orgánu dohledu, soudu nebo orgánu činného v trestním řízení;
- d) příjemce uvolnění (release beneficiary) — primárně vlastník schématu EUDIW-CZ, oprávněný artefakty využít nebo postoupit jejich využití třetí straně určené k pokračování provozu komponenty;
- e) aktualizace — uložené artefakty musí být aktualizovány nejméně při každé větší verzi (major release) komponenty a při každé bezpečnostně významné aktualizaci dle požadavku UPD-01 v kapitole X.7.6;
- f) periodické ověřování — funkčnost úschovního mechanismu musí být nezávisle ověřována nejméně jednou ročně, včetně testu sestavitelnosti komponenty z uložených artefaktů.

Poznámka: Úschova kódu je kompenzačním opatřením k riziku ztráty dostupnosti kritické komponenty v důsledku selhání dodavatelského řetězce, doplňujícím požadavky BCM-04 (X.4.11) a TRM-02 (X.4.12). Hodnotitel ověří existenci úschovní smlouvy, soulad jejího obsahu s tímto požadavkem a výsledky posledního ročního ověření.

X.5 ISMS procesy

Tato kapitola definuje požadavky na pět povinných procesů ISMS, které musí každá certifikovaná služba IKT zahrnovat jako komponenty v souladu s přílohou I schématu (Rozsah certifikace).

Kapitola X.4 definuje požadavky na provozní úrovni převzaté z ETSI EN 319 401 kapitoly 7 (včetně 7.9 o řízení zranitelnosti a incidentů na úrovni infrastruktury). Tato kapitola X.5 definuje požadavky na úrovni procesu, které se vztahují na každý proces jako na samostatně certifikovatelnou komponentu. Požadavky kapitol X.4 a X.5 se vzájemně doplňují, nejsou duplicitní — kapitola X.4 stanoví, **která** bezpečnostní opatření musí existovat, zatímco kapitola X.5 stanoví, **jak** musí být procesy řídicí tato opatření strukturovány, dokumentovány a hodnoceny.

X.5.1 Proces vývoje

DEV-01 [Sec]: Poskytovatel služby EUDI zavede, zdokumentuje, udržuje a provozuje bezpečný životní cyklus vývoje softwaru (Secure Software Development Lifecycle, SSDLC) pro všechny komponenty řešení peněženky a systému eID, v jehož rámci je peněženka poskytována.

Poznámka: ETSI EN 319 401 kapitola 7.7 o provozní bezpečnosti zahrnuje aspekty vývoje, EN ISO/IEC 27001:2022 oddíly A.8.25 až A.8.31 specificky pokrývají bezpečný vývoj. Pro hodnocení vyspělosti SSDLC lze použít rámec OWASP SAMM. Úroveň přísnosti SSDLC musí odpovídat kritičnosti komponenty: vývoj WSCA vyžaduje nejvyšší úroveň přísnosti odpovídající vývojovým třídám záruky Common Criteria, vývoj instance peněženky používá metodologii EN 17640 (FitCEM).

DEV-02 [Sec]: Proces vývoje musí zahrnovat minimálně:

- a) modelování hrozeb (threat modelling) ve fázi návrhu komponenty;
- b) pokyny pro bezpečné programování a pravidelné školení vývojářů v bezpečnostních praktikách;
- c) statické testování bezpečnosti aplikací (SAST) integrované do vývojové a integrační pipeline (CI/CD);
- d) dynamické testování bezpečnosti aplikací (DAST) provedené před vydáním verze do produkčního prostředí;
- e) revizi zdrojového kódu prováděnou recenzentem nezávislým na autorovi kódu;
- f) skenování závislostí (dependency scanning) pro identifikaci známých zranitelností v komponentách třetích stran, navázané na softwarovou skladbu komponent (SBOM) dle požadavku SUP-05.

DEV-03 [Sec]: Vývojové, testovací, předprodukční a produkční prostředí musí být striktně oddělena. Poskytovatel služby EUDI musí dokumentovat opatření zabraňující neoprávněnému přenosu zdrojového kódu, konfigurace nebo dat mezi prostředími a zajistit, že produkční prostředí neobsahuje žádné prvky vývojového prostředí (včetně vývojových účtů, vývojových klíčů, ladících rozhraní apod.).

DEV-04 [Sec]: Poskytovatel služby EUDI musí prokázat soulad s postupy bezpečného vývoje prostřednictvím dokumentovaných důkazů, zahrnujících minimálně:

- a) politiku a postupy SSDLC;
- b) záznamy o aktivitách modelování hrozeb pro klíčové komponenty;
- c) výsledky skenování SAST a DAST a záznamy o nápravě nálezů;
- d) záznamy o revizích kódu (peer review records);
- e) doklady o školení personálu vývojového procesu v bezpečném programování;
- f) záznamy o správě konfigurace a verzování zdrojového kódu (zahrnující auditovatelnou historii změn).

Tyto důkazy musí být k dispozici certifikačnímu orgánu pro počáteční certifikaci a musí být průběžně aktualizovány pro účely dozorových hodnocení dle přílohy II schématu.

DEV-05 [Sec, Cond]: Pokud je vývoj komponent služby EUDI nebo její části zadán subdodavateli, poskytovatel služby EUDI zajistí, že proces vývoje subdodavatele splňuje stejné požadavky DEV-01 až DEV-04 v rozsahu odpovídajícím dodávané komponentě, a zahrne ověření souladu subdodavatele do svých postupů řízení dodavatelského řetězce dle kapitoly X.4.14 (zejména požadavku SUP-06).

Poznámka: Požadavek DEV-05 reaguje na rizika spojená s nedostatečným oddělením prostředí u subdodavatelů a se zneužitím privilegovaného přístupu personálu subdodavatele (CZ-07). Subdodavatelské vztahy musí být dokumentovány smluvně a musí zahrnovat ustanovení o auditních právech poskytovatele služby EUDI a certifikačního orgánu.

X.5.2 Proces řízení změn

CHG-01 [Sec]: Poskytovatel služby EUDI zavede, zdokumentuje, udržuje a provozuje formální proces řízení změn pro všechny změny certifikovaného řešení peněženky a systému eID, v jehož rámci je peněženka poskytována.

CHG-02 [Sec]: Každá změna certifikovaného řešení peněženky musí být před nasazením posouzena z hlediska potenciálního dopadu na bezpečnost certifikované služby IKT a na platnost certifikátu EUDIW-CZ. Posouzení musí určit významnost (materialitu) změny v souladu s kritérii definovanými v příloze II schématu.

Poznámka: Změna se považuje za významnou, pokud může vést k významné neshodě s certifikačními požadavky. Za významné se zpravidla považují: funkční změny s dopadem na bezpečnost, změny organizace nebo architektury služby a změny kritických komponent (zejména WSCD, WSCA, instance peněženky a komponent zpracovávajících PID).

CHG-03 [Sec]: Proces řízení změn musí definovat:

- a) role a odpovědnosti pro posouzení, schválení a implementaci změn;
- b) kritéria pro určení významnosti změn;
- c) požadavky na oznamování významných změn certifikačnímu orgánu;
- d) postupy pro nouzové (emergency) změny a pro retroaktivní schválení takových změn;
- e) postupy pro přezkum po implementaci (post-implementation review);
- f) vazbu mezi procesem řízení změn a procesem řízení verzí dle požadavku OPS-02 v kapitole X.4.7.

CHG-04 [Sec]: Významné změny musí být oznámeny certifikačnímu orgánu.

Oznámení musí zahrnovat minimálně:

- a) popis plánované nebo provedené změny;

- b) posouzení dopadu změny na bezpečnost služby a na platnost certifikátu;
- c) navržená nápravná opatření, pokud jsou relevantní;
- d) plánovaný nebo skutečný termín nasazení změny do produkčního prostředí.

Po obdržení oznámení certifikační orgán rozhodne, zda je nezbytné provést zvláštní hodnocení.

CHG-05 [Sec]: Provozní účinnost procesu řízení změn musí být hodnocena nejméně jednou ročně v rámci dozorových hodnocení, v rámci souboru opatření souvisejících s vývojem a řízením změn.

X.5.3 Proces řízení zranitelností

Články 21 až 28 hlavního EUDIW-CZ schématu definují procedurální povinnosti držitele certifikátu vůči certifikačnímu orgánu a vlastníkovi schématu (oznamování, hlášení, zveřejňování). Tato kapitola přílohy X definuje požadavky na úrovni procesu pro to, jak poskytovatel služby EUDI řídí zranitelnosti interně, doplňující pravidla na úrovni schématu.

VUL-01 [Sec]: Poskytovatel služby EUDI zavede, udržuje a provozuje proces řízení zranitelností v souladu s normou EN ISO/IEC 30111, doplněnou o požadavky definované v článcích 21 až 25 hlavního textu schématu EUDIW-CZ a o pravidla stanovená v této kapitole.

VUL-02 [Sec]: Proces řízení zranitelností musí pro všechny relevantní komponenty služby IKT zahrnovat:

- a) použití softwarové skladby komponent (SBOM) v běžně používaném a strojově čitelném formátu, pokrývající minimálně závislosti na nejvyšší úrovni každé komponenty (požadavek SUP-05);
- b) použití bezpečnostních aktualizací k nápravě zranitelností a, pokud je to technicky proveditelné, oddělení bezpečnostních aktualizací od funkčních aktualizací;
- c) mechanismus pro bezpečnou distribuci aktualizací, včetně mechanismu zajišťujícího bezodkladnou nápravu zranitelností;
- d) v relevantních případech automatizovanou distribuci bezpečnostních aktualizací;
- e) v relevantních případech mechanismus pro pozastavení činnosti jednotky peněženky do doby, než budou aplikovány požadované bezpečnostní aktualizace;
- f) distribuci informačních zpráv poskytujících uživatelům relevantní informace, včetně informací o doporučených opatřeních.

Poznámka: Požadavek VUL-02 odráží procesní stránku povinností definovaných v článku 22 odst. 2 EUDIW-CZ schématu.

VUL-03 [Sec]: Poskytovatel služby EUDI musí udržovat a zveřejňovat vhodné metody pro příjem informací o zranitelnostech souvisejících s řešením peněženky z externích zdrojů, včetně uživatelů, certifikačních orgánů, bezpečnostních výzkumníků a národních CSIRT.

Poznámka: Požadavek VUL-03 implementuje stranu „příjmu“ v rámci koordinovaného zveřejňování zranitelností (Coordinated Vulnerability Disclosure, CVD) v souladu s článkem 22 odst. 3 a článkem 26 hlavního EUDIW-CZ schématu.

VUL-04 [Sec]: Proces řízení zranitelností musí definovat kritéria pro určení významnosti dopadu zranitelností na certifikovanou službu IKT. Určení významnosti musí být zdokumentováno v politice řízení zranitelností a posouzeno certifikačním orgánem v rámci hodnocení.

Poznámka: Klíčový princip určení významnosti je založen na dopadu, nikoli na zranitelnosti samotné. Kritická zranitelnost s včas aplikovanou opravou a bez prokazatelného zneužití může mít nevýznamný dopad. Tento přístup se promítá do analýzy dopadu zranitelností dle článků 23 a 24 EUDIW-CZ schématu. Kritéria významnosti dopadu zranitelností jsou definována v příloze II schématu (kapitola Významnost dopadu zranitelností).

VUL-05 [Sec]: Proces řízení zranitelností musí pokrývat zranitelnosti v celém rozsahu certifikace, zahrnující minimálně:

- a) software instance peněženky;
- b) WSCA;
- c) WSCD, včetně koordinace s dodavatelem WSCD pro zranitelnosti specifické pro hardwarovou komponentu;
- d) backendové služby (zejména službu poskytování a správy peněženek a službu poskytování a správy PID);
- e) knihovny a závislosti třetích stran (prostřednictvím SBOM dle požadavku VUL-02);
- f) infrastrukturní komponenty, prostřednictvím koordinace s poskytovatelem infrastruktury;
- g) komponenty integrované od externích poskytovatelů služeb (zejména pro onboarding uživatelů a pro pečetění PID).

Poskytovatel služby EUDI musí mít dokumentované koordinační postupy pro zveřejňování a nápravu zranitelností pro každého klíčového dodavatele identifikovaného v rámci požadavku SUP-06.

Poznámka: V architekturním profilu schématu EUDIW-CZ řízení zranitelností pokrývá více subjektů (poskytovatel peněženky, dodavatel infrastruktury, dodavatel WSCD, poskytovatel pečetící služby, poskytovatel prostředku elektronické identifikace, dodavatel systému poskytovatele PID). Účinnost procesu závisí na koordinaci mezi těmito subjekty.

VUL-06 [Sec]: Provozní účinnost procesu řízení zranitelností musí být hodnocena nejméně jednou ročně v rámci dozorových hodnocení v souladu s přílohou II schématu, v rámci souboru opatření souvisejících s řízením incidentů, zranitelností a podvodů.

X.5.4 Proces řízení incidentů

INC-01 [Sec]: Poskytovatel služby EUDI zavede, zdokumentuje, udržuje a provozuje proces řízení incidentů pro detekci, reakci, eskalaci a obnovu po kybernetických bezpečnostních incidentech ovlivňujících službu EUDI.

INC-02 [Sec]: Proces řízení incidentů musí definovat:

- a) klasifikační kritéria závažnosti incidentů (zpravidla úrovně: kritický, závažný, méně závažný, informační);
- b) postupy eskalace a časové limity pro reakci na jednotlivé úrovně závažnosti;
- c) role a odpovědnosti v týmu pro reakci na incidenty (Incident Response Team);
- d) komunikační postupy, včetně požadavků na interní a externí oznamování;
- e) postupy pro uchovávání důkazů s respektováním požadavků na forenzní integritu (chain of custody);
- f) postupy pro koordinaci s externími subjekty (orgán dohledu, certifikační orgán, NÚKIB, národní CSIRT, orgány činné v trestním řízení), pokud je to relevantní pro daný typ incidentu.

INC-03 [Sec]: Poskytovatel služby EUDI oznámí certifikačnímu orgánu bez zbytečného odkladu jakékoli narušení nebo ohrožení řešení peněženky nebo systému eID, v jehož rámci je peněženka poskytována, které má pravděpodobný dopad na soulad s požadavky schématu EUDIW-CZ.

Poznámka: Požadavek INC-03 představuje primární oznamovací povinnost vůči certifikačnímu orgánu.

Konkrétní procedurální požadavky na obsah, formu a lhůty oznamování jsou definovány v článku 16 odst. 3 EUDIW-CZ schématu.

INC-04 [Sec]: Proces řízení incidentů musí zahrnovat oznamovací povinnosti vůči orgánu dohledu, vedle oznamovací povinnosti vůči certifikačnímu orgánu definované v požadavku INC-03. V relevantních případech musí proces zahrnovat i oznamovací povinnosti dle směrnice (EU) 2022/2555 (NIS2) a souvisejících prováděcích předpisů.

Poznámka: Čl. 5a odst. 10 eIDAS ukládá poskytovatelům peněženek zajistit, aby uživatelé mohli snadno hlásit technické problémy a jiné incidenty. Postup při narušení bezpečnosti peněženek upravuje čl. 5e eIDAS.

Souběh oznamovacích povinností (orgán dohledu, certifikační orgán, NÚKIB dle NIS2, ÚOOÚ dle GDPR) musí být v procesu řízení incidentů řešen tak, aby každá oznamovací povinnost byla splněna ve stanovené lhůtě a v požadovaném rozsahu.

INC-05 [Sec]: Poskytovatel služby EUDI provede přezkum po každém incidentu klasifikovaném jako závažný nebo kritický a získané poznatky promítne do:

- a) posouzení rizik dle kapitoly X.2 (přezkum dle požadavku RMF-08);
- b) zlepšení bezpečnostních opatření v relevantních kapitolách této přílohy;

- c) aktualizace procesů ISMS dle této kapitoly X.5;
- d) bezpečnostních školení personálu dle požadavku HR-01.

INC-06 [Sec, Cond]: Proces řízení incidentů musí zahrnovat koordinační postupy s klíčovými subjekty v ekosystému služby EUDI pro situace, kdy incident zasahuje vícero subjektů. Koordinace musí pokrývat minimálně:

- a) infrastrukturní incidenty ovlivňující dostupnost WSCD nebo souvisejících kritických komponent;
- b) incidenty ovlivňující službu pečetění PID;
- c) incidenty ovlivňující službu poskytovatele PID, včetně incidentů spojených s vydáváním nebo správou PID;
- d) incidenty vyžadující širší národní koordinaci, zejména prostřednictvím národního CSIRT a NÚKIB.

Koordinační postupy musí být zdokumentovány smluvně mezi relevantními subjekty a musí zahrnovat jednoznačné určení odpovědností, kontaktních bodů a komunikačních kanálů pro každý typ incidentu.

Poznámka: Distribuovaný charakter ekosystému služby EUDI znamená, že jediný incident může postihnout více subjektů současně. Jasně koordinační postupy jsou nezbytné pro zajištění včasné reakce a minimalizaci dopadu na uživatele služby.

INC-07 [Sec]: Provozní účinnost procesu řízení incidentů musí být hodnocena nejméně jednou ročně v rámci dozorových hodnocení v souladu s přílohou II schématu, v rámci souboru opatření souvisejících s řízením incidentů, zranitelností a podvodů.

X.5.5 Proces řízení podvodů

Tato kapitola definuje procesní stránku řízení podvodů jako certifikovatelné komponenty ISMS, zatímco kapitola X.4.9.1 definuje provozní stránku řízení podvodů (provozní povinnosti poskytovatele). Požadavky FRD-01 až FRD-05 v kapitole X.4.9.1 stanoví, co musí poskytovatel dělat (být informován, analyzovat, řídit podvod jako zranitelnost, hlásit). Tato kapitola stanoví, **jak** musí být tento proces strukturován.

FRD-P01 [Sec]: Poskytovatel služby EUDI zavede, zdokumentuje, udržuje a provozuje proces řízení podvodů pro detekci, prevenci a reakci na podvodné aktivity související se službou EUDI.

FRD-P02 [Sec]: Proces řízení podvodů musí definovat:

- a) mechanismy detekce podvodů a zdroje dat pro detekci (zejména dle požadavku FRD-05 v kapitole X.4.9.1);
- b) klasifikační kritéria podvodů (pokus o podvod, úspěšný podvod, úroveň dopadu);
- c) postupy eskalace, včetně vazby na proces řízení zranitelností v případech identifikace kořenové příčiny ve službě (požadavek FRD-03 v kapitole X.4.9.1);

d) postupy hlášení certifikačnímu orgánu bez ohledu na významnost dopadu (požadavek FRD-04 v kapitole X.4.9.1);

e) role a odpovědnosti pro vyšetřování podvodů a pro správu evidence případů;

f) koordinační postupy s orgány činnými v trestním řízení v relevantních případech;

g) koordinační postupy s ostatními držiteli certifikátu v ekosystému EUDIW pro sdílení informací o vzorcích podvodů (prostřednictvím certifikačního orgánu).

FRD-P03 [Sec, Cond]: Proces řízení podvodů musí pokrývat minimálně následující kategorie scénářů podvodu relevantní pro architekturní profil schématu EUDIW-CZ:

a) podvod s identitou během onboarding, zejména spoofing nebo zneužití procesu ověření identity prostřednictvím prostředku elektronické identifikace;

b) neoprávněné použití jednotky peněženky, včetně útoků typu session hijacking na komunikaci instance peněženky se vzdáleným WSCD;

c) podvodné vydání PID, včetně zneužití privilegovaného přístupu personálu poskytovatele PID nebo jeho subdodavatelů;

d) útoky sociálního inženýrství cílící na uživatele peněženky za účelem zveřejnění atributů nebo autorizace transakcí ve prospěch útočníka;

e) koluze (spolupráce) mezi spoléhajícími se stranami pro sledování uživatelů nad rámec oprávněného rozsahu zpracování;

f) zneužití slabín v procesu obnovy jednotky peněženky pro převzetí cizí identity.

Poznámka: Tyto kategorie scénářů jsou odvozeny z analýzy hrozeb v registru rizik (zejména hrozby TR5, TR6, TR7, TR9, TR11, TR14, TR28, TR40, TR51, TR84, TR87, TR98, TR99, TR100) a z architekturně specifických rizik schématu EUDIW-CZ (zejména CZ-03, CZ-05, CZ-09).

FRD-P04 [Sec]: Poskytovatel služby EUDI provádí periodickou analýzu trendů podvodů, nejméně jednou ročně, zahrnující data z:

a) vlastních mechanismů detekce podvodů;

b) informací sdílených certifikačním orgánem od jiných držitelů certifikátu (prostřednictvím článku 27 hlavního textu schématu);

c) veřejně dostupných zpravodajských informací o hrozbách relevantních pro ekosystémy digitální identity (Cyber Threat Intelligence);

d) informací sdílených národním CSIRT a NÚKIB.

Výsledky analýzy trendů podvodů jsou vstupem pro přezkum posouzení rizik dle požadavku RMF-08 a pro úpravy procesu řízení podvodů a souvisejících bezpečnostních opatření.

FRD-P05 [Sec]: Provozní účinnost procesu řízení podvodů musí být hodnocena nejméně jednou ročně v rámci dozorových hodnocení v souladu s přílohou II schématu, v rámci souboru opatření souvisejících s řízením incidentů, zranitelností a podvodů.

X.6 Požadavky na jednotku peněženky

Tato kapitola definuje bezpečnostní požadavky na komponenty jednotky peněženky (wallet unit). Požadavky jsou klasifikovány jako funkční (Fun) nebo implementační bezpečnostní (Sec) v souladu s klasifikací uvedenou v kapitole X.1.1.

Požadavky jsou primárně formulovány na úrovni jednotky peněženky jako celku, protože rozdělení funkcí mezi jednotlivé komponenty (instance peněženky, WSCA, WSCD, keystore) závisí na architektuře zvolené poskytovatelem. Pouze vybrané požadavky jsou přiřazeny konkrétním komponentám (zejména kryptografické operace prováděné ve WSCA a WSCD, uživatelské rozhraní implementované v instanci peněženky). Pro architekturní profil schématu EUDIW-CZ musí certifikační orgán ověřit, že alokace požadavků na jednotlivé komponenty je v souladu s architekturním profilem definovaným v příloze I schématu.

X.6.1 Obecné požadavky a životní cyklus

WUG-01 [Fun]: Jednotka peněženky musí být aktivována vydáním alespoň jedné atestace jednotky peněženky (Wallet Unit Attestation, WUA) vázané na WSCA/WSCD předtím, než ji uživatel může použít pro vyžádání vydání PID.

Poznámka k hodnocení: Testování zahrnující negativní případy, kdy se uživatel pokusí o žádost o vydání PID před aktivací jednotky peněženky.

WUG-02 [Fun]: Jednotka peněženky by měla obsahovat aktivní PID před tím, než ji uživatel může použít pro vyžádání vydání atestace atributu (EAA).

Poznámka k hodnocení: Pokud lze atestaci vydat před PID, hodnotitel ověří, že situace nemůže být zneužita k vydání atestace bez dostatečné identifikační záruky.

WUG-03 [Sec]: Atestace jednotky peněženky (WUA) musí obsahovat jeden nebo více veřejných klíčů a odpovídající soukromé klíče musí být vygenerovány v rámci WSCA/WSCD nebo keystore popsáno v WUA.

Poznámka k hodnocení: Inspekce ověřující, že soukromé klíče jsou vygenerovány v prostředí WSCA nebo keystore a že nejsou nikdy exportovány mimo toto prostředí.

WUG-04 [Sec]: Pokud WSCA/WSCD obsahuje kryptografické klíče související s více jednotkami peněženky, jednotka peněženky musí mít přístup výhradně ke klíčům a dalším aktivům, která se vztahují k dané

jednotce peněženky. Mechanismus izolace musí zajistit, že kompromitace jedné jednotky peněženky nevede k neoprávněnému přístupu k aktivům jiných jednotek peněženky hostovaných ve stejném WSCA/WSCD.

Poznámka k hodnocení: Tento požadavek je zásadní pro architektury, v nichž jeden WSCA/WSCD obsluhuje vícero jednotek peněženky (zejména u vzdáleného WSCD). Inspekce ověří, že WSCA autentizuje uživatele před přístupem ke klíčům, a že instance peněženky se autentizuje před přístupem k WSCA. Testování musí zahrnovat pokusy o neoprávněný přístup napříč jednotkami peněženky.

WUG-05 [Sec]: Poskytovatel peněženky musí definovat a implementovat přísná opatření omezující přístup poskytovatele peněženky k obsahu jednotky peněženky. Opatření musí zabraňovat poskytovateli peněženky v získání informací zejména o:

- a) atestacích přítomných v jednotce peněženky;
- b) stavu atestací;
- c) hodnotách atributů;
- d) obsahu logu jednotky peněženky.

Poznámka k hodnocení: Pro architektury se vzdáleným WSCD tento požadavek vyžaduje přísné oddělení mezi infrastrukturou služby jednotky peněženky a administrativní infrastrukturou poskytovatele peněženky. Uživatelská data spravovaná na straně serveru musí být šifrována a přístup k nim řízen. Hodnotitel ověří oddělení infrastruktur, šifrování a řízení přístupu k uživatelským datům a potvrdí, že případné výjimečné přístupy (například pro forenzní účely) jsou zaznamenávány a řízeny dokumentovaným procesem.

WUG-06 [Sec, Cond]: V architekturách, kde WSCD obsluhuje více jednotek peněženky současně, musí mít každá jednotka peněženky jedinečné kryptografické svázání se specifickou logickou instancí WSCD v rámci fyzického WSCD, s ověřitelným důkazem tohoto svázání. Mechanismus svázání musí zabránit:

- a) neoprávněné migraci stavu jednotky peněženky mezi logickými instancemi WSCD;
- b) duplikaci jednotky peněženky na základě zkopírování kryptografických klíčů;
- c) záměně jednotek peněženky v důsledku chyby v izolaci logických instancí WSCD.

Poznámka k hodnocení: Tento požadavek je zásadní architektonickou charakteristikou, bez níž nelze zaručit izolaci mezi uživateli ve sdíleném WSCD. Hodnotitel formou inspekce ověří mechanismus svázání na úrovni implementace WSCA a jeho vazbu na WSCD. Testování zahrnuje pokusy o migraci stavu jednotky peněženky a pokusy o duplikaci.

WUG-07 [Sec]: Životní cyklus jednotky peněženky musí být řízen definovanými stavy a přechody mezi stavy, zahrnujícími minimálně:

- aktivace,
- běžný provoz,

- pozastavení,
- revokace a
- ukončení.

Přechody mezi stavy provádí poskytovatel peněženky, který je dle požadavku REV-01 jedinou entitou oprávněnou provést revokaci jednotky peněženky. O přechod může požádat uživatel (REV-02) nebo poskytovatel PID (REV-03), případně k němu dochází na základě rozhodnutí orgánu dohledu, soudu nebo orgánu činného v trestním řízení a dalších spouštěcích událostí dle požadavku REV-04. Přechody musí být zaznamenávány s nepopíratelnou auditní stopou.

Poznámka k hodnocení: Hodnotitel ověří diagram stavů životního cyklu, postupy přechodů mezi stavy, oprávnění pro jednotlivé subjekty a integritu záznamů o přechodech.

X.6.2 Správa PID a atestací atributů

X.6.2.1 Vydávání PID a atestací

WUI-01 [Sec]: Jednotka peněženky musí podporovat proces aktivace PID v souladu s požadavky úrovně záruky „vysoká“ dle CIR (EU) 2015/1502. Prezentace PID, který nebyl aktivován, nesmí být jednotkou peněženky umožněna.

Poznámka k hodnocení: Kombinace auditu specifikace aktivačního procesu, inspekce implementace a testování s negativními případy (pokus o prezentaci neaktivovaného PID).

WUI-02 [Sec]: Před vydáním PID nebo atestace vázané na zařízení musí jednotka peněženky:

a) požádat WSCA/WSCD o vygenerování nového páru klíčů; b) poskytnout poskytovateli PID nebo poskytovateli atestace platnou WUA popisující WSCA/WSCD; c) poskytnout důkaz držení soukromého klíče (proof of possession); d) poskytnout kryptografický důkaz, že WSCA/WSCD popsaná v WUA skutečně provedla operaci generování klíče.

Poznámka k hodnocení: Inspekce ověřující, že všechny soukromé klíče jsou generovány a uloženy výhradně ve WSCD; testování toku generování klíčů a toků důkazu držení.

WUI-03 [Sec]: Jednotka peněženky musí autentizovat a validovat přístupový certifikát poskytovatele PID před zasláním žádosti o vydání PID. Validace musí zahrnovat ověření:

a) autenticity a platnosti přístupového certifikátu; b) toho, že vydavatel certifikátu je uveden v seznamu důvěryhodných entit pro certifikační autority přístupu (Access Certificate Authority List of Trusted Entities); c) autenticity metadat poskytovatele PID pomocí veřejného klíče obsaženého v přístupovém certifikátu; d) toho, že poskytovatel PID je registrovaným poskytovatelem PID v národním ekosystému EUDIW.

Poznámka k hodnocení: Testování s negativními testovacími případy (neplatná metadata, revokované certifikáty, neregistrovaný poskytovatel PID) a inspekce implementace validačních kroků.

WUI-04 [Sec]: Před vyžádáním počátečního vydání PID musí jednotka peněženky požádat uživatele o nastavení autentizačních faktorů pro pokročilou autentizaci vázanou na kritická aktiva.

Poznámka k hodnocení: Inspekce ověřující nemožnost vyžádat vydání PID před dokončením nastavení pokročilé autentizace. Konkrétní požadavky na pokročilou autentizaci uživatele jsou definovány v kapitole X.6.3.1.

WUI-05 [Fun]: Jednotka peněženky musí požádat uživatele o souhlas před uložením PID nebo atestace. Před žádostí o souhlas musí jednotka peněženky zobrazit uživateli:

a) obsah PID nebo atestace, která má být uložena; b) identitu poskytovatele PID nebo poskytovatele atestace, a to s použitím informací o subjektu obsažených v přístupovém certifikátu poskytovatele; c) informace o rozsahu oprávnění poskytovatele a o platnosti jeho registrace v ekosystému EUDIW.

Poznámka k hodnocení: Interaktivní testování, které ověří, že veškeré požadované informace jsou uživateli prezentovány pravdivě a srozumitelně. Požadavky na interakci s uživatelem jsou dále rozpracovány v kapitole X.6.3.2.

X.6.2.2 Správa PID a atestací

WUM-01 [Fun, Privacy]: Jednotka peněženky musí podporovat Metodu A (jednorázové atestace, once-only attestations) a Metodu B (atestace s časově omezenou platností, limited-time attestations) pro omezení počtu opakovaných prezentací téhož PID nebo atestace. Podpora Metody C (rotující dávky, rotating-batch) a Metody D (per-RP) je volitelná.

WUM-02 [Sec]: Jednotka peněženky musí implementovat mechanismus prokazující, že znovu vydaný PID nebo atestace vázaná na zařízení byly vydány téže jednotce peněženky jako existující PID nebo atestace.

Poznámka k hodnocení: Audit bezpečnosti mechanismu a inspekce implementace. Pokud mechanismus používá znovu-vydávací tokeny na úrovni WSCA, musí být tyto tokeny zabezpečeny na úrovni WSCA (tj. uloženy a zpracovávány výhradně v rámci WSCA).

WUM-03 [Sec]: Pokud jednotka peněženky smaže PID nebo atestaci vázanou na zařízení na žádost uživatele, musí zajistit, že veškerý kryptografický klíčový materiál v rámci WSCA/WSCD nebo keystore související s tímto PID nebo atestací je bezpečně zničen (secure destruction).

Poznámka k hodnocení: Inspekce ověří, že smazání PID nebo atestace spouští zničení odpovídajícího klíčového materiálu ve WSCD. Pro architekturu se vzdáleným WSCD se kromě toho ověří mechanismus pro vzdálené zničení klíčového materiálu včetně potvrzení úspěšnosti operace.

WUM-04 [Sec]: Jednotka peněženky by měla pravidelně kontrolovat stav revokace svých PID, atestací a WUA a upozornit uživatele v případě, že některý z těchto prvků byl revokován. Frekvence kontrol musí být přiměřená kritičnosti prvku a musí být dokumentována v politice poskytovatele peněženky.

Poznámka k hodnocení: Inspekce ověří, že kontroly stavu revokace jsou prováděny s odpovídající frekvencí a že jednotka peněženky přijímá odpovídající opatření při detekci revokace (pozastavení použití revokovaného prvku, notifikace uživatele).

WUM-05 [Sec, Cond]: V architekturách, kde je správa PID a atestací závislá na dostupnosti vzdáleného WSCD, musí jednotka peněženky definovat chování v situaci, kdy vzdálený WSCD není dostupný. Chování musí zahrnovat:

a) zachování integrity lokálně uložených dat jednotky peněženky; b) omezení operací na ty, které nevyžadují přístup ke vzdálenému WSCD; c) informování uživatele o dočasné nedostupnosti služby; d) automatické obnovení plné funkcionality po obnově dostupnosti vzdáleného WSCD bez nutnosti opakované aktivace jednotky peněženky.

Poznámka k hodnocení: Testování scénářů nedostupnosti vzdáleného WSCD (výpadek sítě, výpadek WSCD infrastruktury), ověření integrity dat po obnově dostupnosti.

X.6.2.3 Presentace PID a atestací

WUP-01 [Fun]: Jednotka peněženky musí provést autentizaci spoléhající se strany ve všech transakcích prezentace PID nebo atestace, ať už ve scénáři proximity (fyzická blízkost), nebo ve scénáři remote (vzdálená prezentace). Autentizace musí používat přístupový certifikát spoléhající se strany ověřený vůči důvěryhodným kotvám v seznamu důvěryhodných entit všech certifikačních autorit přístupu notifikovaných členskými státy (List of Trusted Entities of All Access Certificate Authorities).

Poznámka k hodnocení: Rozsáhlé testování pokrývající oba scénáře prezentace, včetně negativních případů s neplatnými, revokovanými nebo neznámými certifikáty spoléhající se strany.

WUP-02 [Fun]: Po ověření žádosti o prezentaci musí jednotka peněženky zobrazit uživateli:

a) identitu spoléhající se strany dle informací obsažených v přístupovém certifikátu; b) stav registrace spoléhající se strany v národním registru spoléhajících se stran a autorizovaný rozsah zpracování dle této registrace; c) seznam požadovaných atributů; d) účel zpracování atributů sdělený spoléhající se stranou; e) žádost o souhlas uživatele s prezentací těchto atributů.

Poznámka k hodnocení: Rozsáhlé testování, které ověří, že zobrazení probíhá pouze po plném ověření spoléhající se strany a že interakce s uživatelem odpovídá požadavkům kapitoly X.6.3.2.

WUP-03 [Fun]: Po obdržení souhlasu uživatele musí jednotka peněženky prezentovat spoléhající se straně výhradně ty atributy, které uživatel odsouhlasil. Jednotka peněženky musí podporovat selektivní zveřejnění (selective disclosure) tak, aby nebyly prezentovány atributy, které nebyly vyžádány nebo které uživatel neschválil.

Poznámka k hodnocení: Testování a inspekce integrity seznamu atributů od okamžiku vytvoření až po odpověď spoléhající se straně. Ověření, že mechanismus selektivního zveřejnění nezpřístupňuje atributy nad rámec souhlasu.

WUP-04 [Sec]: Jednotka peněženky musí zajistit, že hodnoty atributů PID a atestací sdělované spoléhající se straně jsou shodné s hodnotami, které byly jednotce peněženky vydány poskytovatelem PID nebo atestace.

Poznámka k hodnocení: Inspekce ověří ochranu integrity hodnot atributů v klidu (at rest) i při použití, kompatibilní s úrovní záruky „vysoká“.

WUP-05 [Sec]: Jednotka peněženky musí ověřit pověření spoléhající se strany vůči národnímu registru spoléhajících se stran a musí jednoznačně indikovat uživateli:

a) stav registrace spoléhající se strany v registru; b) kategorizaci spoléhající se strany (například soukromý subjekt, orgán veřejné moci, zdravotnické zařízení); c) autorizovaný rozsah zpracování osobních údajů dle registrace; d) případné bezpečnostní varování v případech, kdy spoléhající se strana není registrována nebo je její registrace pozastavena nebo zneplatněna.

Poznámka k hodnocení: Testování s různými stavy registrace spoléhajících se stran. Ověření, že informace o stavu registrace jsou uživateli zobrazeny před požadavkem na souhlas.

WUP-06 [Sec]: Jednotka peněženky musí odmítnout prezentaci PID nebo atestace v případech, kdy:

a) se nepodaří ověřit totožnost spoléhající se strany — zejména proto, že její přístupový certifikát je neplatný nebo revokovaný, nebo že vydavatele certifikátu nelze najít v seznamu důvěryhodných entit vedeném na úrovni EU; b) registrace spoléhající se strany byla zrušena nebo pozastavena v registru toho členského státu, kde je spoléhající se strana usazena, a jednotka peněženky si tuto skutečnost dokáže spolehlivě ověřit; c) uživatel neudělí souhlas dle požadavku WUP-02; d) jednotka peněženky je v pozastaveném, revokovaném nebo ukončeném stavu dle požadavku WUG-07.

Poznámka k hodnocení: Testování s negativními případy pokrývající kategorie (a) až (d) a situaci, kdy spoléhající se strana žádá více údajů, než smí - včetně případu spoléhající se strany registrované v jiném členském státě. Ověření, že odmítnutí prezentace je uživateli srozumitelně vysvětleno a zaznamenáno v logu jednotky peněženky, a že se varování zobrazí dříve, než uživatel udělí souhlas.

X.6.3 Průřezové požadavky

X.6.3.1 Autentizace uživatele

AUTH-01 [Sec]: Po počátečním nastavení autentizace na úrovni aplikace nesmí být umožněna žádná operace na jednotce peněženky před dokončením autentizace na úrovni aplikace. Autentizace vázaná na aktiva nesmí být umožněna před autentizací na úrovni aplikace.

Poznámka k hodnocení: Interaktivní testování, které ověří, že před dokončením autentizace na úrovni aplikace není dostupná žádná operace jednotky peněženky.

AUTH-02 [Sec]: Autentizace vázaná na aktiva musí být založena nejméně na dvou faktorech patřících do různých kategorií autentizačních faktorů (znalost, vlastnictví, biometrie).

Poznámka k hodnocení: Zpravidla kombinace faktoru znalosti (například PIN) a faktoru vlastnictví (například kryptografického klíče uloženého ve WSCD), přičemž oba jsou ověřovány na WSCD a propojeny s autorizací kritických kryptografických aktiv.

AUTH-03 [Sec]: Ověření autentizace vázané na aktiva by mělo být prováděno v rámci WSCD a jeho implementace musí odolat útokům útočníků s vysokým potenciálem útoku. Operace s PID a atestacemi vázanými na zařízení musí být umožněny pouze po úspěšné autentizaci vázané na aktiva na takovém zařízení.

Poznámka k hodnocení: Tento požadavek je zpravidla pokryt v rámci hodnocení WSCD a WSCA dle metodologie EUCC/Common Criteria. Hodnotitel ověří konzistenci tvrzení v certifikátu WSCD s požadavky tohoto požadavku.

AUTH-04 [Sec]: Autentizace vázaná na aktiva musí být platná pouze pro jednu uživatelem autorizovanou operaci. Po dokončení autorizované operace musí jednotka peněženky vyžadovat novou autentizaci vázanou na aktiva pro další operaci, s výjimkou operací prováděných v rámci dávkového zpracování s předem definovanou a uživatelem schválenou politikou.

Poznámka k hodnocení: Audit politiky pro dávkové operace (batch operations) a inspekce ověřující, že pouze předem svázané operace mohou být provedeny bez opakované autentizace.

AUTH-05 [Sec]: Autentizace vázaná na aktiva musí být kryptograficky svázána s jedinečným identifikátorem zamýšlené spoléhající se strany nebo poskytovatele, aby nebylo možné přenést autentizační kredenciály na jinou transakci (proti-phishingový požadavek).

Poznámka k hodnocení: Audit nebo inspekce mechanismu svázání mezi autentizací a identifikátorem cílové entity transakce.

X.6.3.2 Interakce s uživatelem

UI-01 [Sec]: Uživatelské rozhraní jednotky peněženky musí:

- a) bezpečně využívat mechanismy uživatelského rozhraní platformy (Android, iOS);
- b) zobrazovat informace konzistentně a jednoznačně, s ohledem na riziko pokusů o phishing a zmatení uživatele;
- c) jednoznačně informovat uživatele o rozhodnutí, které se chystá učinit, před žádostí o jeho potvrzení;
- d) při žádosti o pokročilou autentizaci (autentizaci vázanou na aktiva) připomenout uživateli rozhodnutí, které se potvrzuje, včetně identifikace cílové spoléhající se strany nebo poskytovatele.

Poznámka k hodnocení: Kombinace auditu a inspekce, která ověří proti-phishingová opatření a že obsah od externích subjektů (poskytovatelé, spoléhající se strany) je uživateli prezentován pravdivě.

X.6.3.3 Orchestrace

ORC-01 [Sec]: Jednotka peněženky musí v rámci orchestrace operací:

- a) validovat formát všech externích vstupů (žádostí od spoléhajících se stran, metadat poskytovatelů, potvrzovacích zpráv) před jejich použitím;
- b) odmítnout neplatné vstupy s minimálními chybovými zprávami, které neposkytují informace využitelné útočníkem;
- c) ověřit autenticitu všech externích vstupů před zobrazením uživateli;
- d) zobrazit relevantní charakteristiky operace (identita protistrany, požadované atributy, účel zpracování) před rozhodnutím uživatele;
- e) vyžadovat pokročilou autentizaci pro akce s kritickými aktivy;
- f) ověřit, že všechny požadované kroky byly provedeny, než je uskutečněna akce s kritickými aktivy.

Poznámka k hodnocení: Inspekce mechanismu validace vstupů; audit politiky pro výjimečné případy; inspekce mechanismu ověření kroků.

X.6.3.4 Ověření autenticity a kotvy důvěry

TRU-01 [Sec]: Pro veškerá ověření autenticity externích dat (PID, atestace, metadata poskytovatelů, přístupové certifikáty spoléhajících se stran) musí jednotka peněženky:

- a) zajistit, že příslušný seznam důvěryhodných entit je aktuální (nejvýše 24 hodin starý před použitím);
- b) ověřit, že vydavatel ověřovaného prvku je uveden v příslušném seznamu důvěryhodných entit;
- c) použít registrovanou kotvu důvěry (trust anchor) k ověření autenticity prvku;
- d) prvek syntakticky analyzovat a validovat, včetně kontroly expirace a dalších atributů platnosti;
- e) pokud je prvek revokovatelný, ověřit, že nebyl revokován, za pomoci aktuálního seznamu revokací nebo seznamu stavu;
- f) nepoužít prvek, dokud nebyly úspěšně dokončeny všechny výše uvedené kontroly.

Poznámka k hodnocení: Inspekce každého kroku kontroly; ověření správného pořadí kontrol (nejprve přítomnost v seznamu důvěryhodných entit, pak ověření podpisu, pak syntaktická analýza). Testování s neplatnými, revokovanými a falešnými prvky.

X.6.3.5 Soukromí a nesledovatelnost

PRV-01 [Sec, Privacy]: Jednotka peněženky musí podporovat použití různých pseudonymů pro různé spoléhající se strany za účelem prevence sledování napříč spoléhajícími se stranami. Návrh mechanismu pseudonymů musí zajistit, že poskytovatel peněženky, poskytovatel PID ani žádná jednotlivá spoléhající se strana nemohou korelovat transakce téhož uživatele napříč různými spoléhajícími se stranami.

Poznámka k hodnocení: Inspekce návrhu pseudonymů a audit vlastností nesledovatelnosti. Jedná se o zásadní požadavek v režimu privacy-by-design.

PRV-02 [Sec, Privacy]: Revokační mechanismy pro PID a atestace musí být navrženy tak, aby chránily soukromí uživatele. Veřejné revokační seznamy nesmí odhalovat vzorce používání jednotlivých uživatelů, zejména nesmí umožňovat propojení revokovaného prvku s konkrétním uživatelem nebo s konkrétní transakcí.

Poznámka k hodnocení: Architektonické rozhodnutí o mechanismu revokace (například použití akumulátorových mechanismů, kryptografických seznamů stavu nebo stromů Merkle) musí být auditováno s ohledem na vlastnosti ochrany soukromí.

PRV-03 [Sec]: Jednotka peněženky ani služby poskytovatele peněženky nesmí poskytovat poskytovatelům služeb vytvářejících důvěru, kteří vydali elektronická potvrzení atributů, žádné informace o používání těchto potvrzení (čl. 5a odst. 5 písm. b) eIDAS). Prezentace atestace spoléhající se straně zejména nesmí vyvolat žádnou komunikaci s vydavatelem atestace. Ověřování stavu atestace probíhá výhradně mechanismy dle PRV-02 a PIDR-R04, které vydavateli neodhalují jednotlivé transakce.

X.6.4 Požadavky na instanci peněženky

X.6.4.1 Ochrana aktiv

WIN-01 [Sec]: Instance peněženky musí:

- a) bezpečně ukládat a zpracovávat data podle jejich klasifikace citlivosti dle kapitoly X.4.3;
- b) využívat bezpečnostní mechanismy platformy (Android, iOS), jsou-li vhodné, nebo poskytovat ekvivalentní alternativy, nejsou-li mechanismy platformy vhodné;
- c) zabránit úniku citlivých dat mimo instanci peněženky (například prostřednictvím mezipaměti schránky, zálohování, ladících rozhraní, sdílení mezi aplikacemi);
- d) používat kryptograficky bezpečný generátor pseudonáhodných čísel pro veškeré kryptografické operace prováděné instancí peněženky;
- e) chránit soukromé klíče používané k autentizaci atestací instance peněženky;
- f) vzájemně autentizovat a šifrovat veškerou komunikaci mezi komponentami jednotky peněženky hostovanými na různých systémech nebo zařízeních (zejména komunikaci instance peněženky se vzdálenou WSCA a s backendovými službami poskytovatele peněženky).

Poznámka k hodnocení: Hodnocení se provádí dle rámce OWASP MAS a dle FitCEM Wallet Instance Protection Profile. Bod f) je zásadní pro architekturu se vzdáleným WSCD a je propojen s požadavky NET-02 a CRY-05 v kapitole X.4.

X.6.4.2 Mobilní aplikace

WIN-02 [Sec]: Všechny varianty instance peněženky ve formě mobilní aplikace (Android, iOS) musí:

- a) vyžadovat aktuální podporovanou verzi platformy operačního systému uživatelského zařízení;

- b) zahrnovat mechanismus vynucení aktualizací instance peněženky;
- c) používat pouze softwarové komponenty bez známých zranitelností s významným dopadem;
- d) validovat a sanitizovat všechny nedůvěryhodné vstupy;
- e) validovat integritu platformy uživatelského zařízení (kontrola stavu bootloaderu, detekce root/jailbreak, detekce hookovacích frameworků);
- f) implementovat mechanismy proti neoprávněné manipulaci s aplikací (anti-tampering);
- g) implementovat mechanismy proti statické analýze aplikace (anti-static analysis);
- h) implementovat techniky proti dynamické analýze aplikace (anti-dynamic analysis);
- i) zahájit proces aktivace ihned po instalaci;
- j) zajistit, že aktivace probíhá pouze s autentizovaným backendem poskytovatele peněženky;
- k) informovat uživatele, pokud podmínky pro aktivaci nejsou splněny, včetně uvedení důvodu;
- l) zajistit bezpečné zničení lokálně uloženého klíčového materiálu při odinstalaci aplikace.

Poznámka k hodnocení: Hodnocení dle metodologie FitCEM (EN 17640) na úrovni záruky nejméně AVA_VAN.3, s použitím FitCEM Wallet Instance Protection Profile. Body (f) až (h) jsou specifické pro hodnocení odolnosti mobilní aplikace a typicky jsou pokryty v rámci FitCEM MASVS-RESILIENCE kontrol.

WIN-03 [Sec]: Instance peněženky musí být certifikována dle metodologie EN 17640 (FitCEM) na základě FitCEM Wallet Instance Protection Profile, nejméně na úrovni posouzení zranitelnosti AVA_VAN.3. Jako alternativní metodologie jsou přijatelná národní schémata odvozená z FitCEM (CSPN, BSZ, LINCE, BSZA) za předpokladu, že pokrývají stejný rozsah kontrol na ekvivalentní úrovni záruky dle kapitoly IX.6.3 přílohy IX schématu. Jako prozatímní alternativa do nasazení FitCEM Wallet Instance PP je přijatelné hodnocení dle OWASP MAS s aplikací testovacích profilů MAS-L2 + MAS-R + MAS-P na základě katalogu slabín OWASP MASWE; toto hodnocení odpovídá úrovni CSA „značná“ a jeho přijatelnost se řídí scénářem (3) kritérií přiměřenosti dle kapitoly IX.5.2 přílohy IX schématu.

Poznámka k hodnocení: Přijatelnost existujícího certifikátu FitCEM nebo národního schématu se posuzuje formou analýzy závislosti dle přílohy IX schématu.

X.6.4.3 Webová aplikace

WIN-04 [Sec, Cond]: Pokud poskytovatel peněženky poskytuje webovou aplikaci uživatelského rozhraní peněženky, musí webová aplikace:

- a) implementovat všechna relevantní opatření OWASP ASVS na úrovni 3 (Advanced);
- b) používat pouze kryptografické algoritmy doporučené v dokumentu ECCG Agreed Cryptographic Mechanisms.

Poznámka k hodnocení: Hodnocení webové instance peněženky je formou auditu shody s OWASP ASVS úrovně 3 v rámci hodnocení služby poskytovatele peněženky dle kapitoly X.7.

X.6.5 Požadavky na WSCA

Požadavky uvedené v této kapitole jsou určeny k hodnocení metodologií Common Criteria (EUCC). Měly by být pokryty Profilem ochrany WSCA (WSCA Protection Profile) vyvíjeným v rámci CEN TC224 WG17, nebo ekvivalentním bezpečnostním cílem (Security Target). Jsou-li použity ekvivalentní metodologie, tyto požadavky musí být nadále pokryty.

WSA-01 [Sec]: WSCA musí autentizovat:

- a) poskytovatele peněženky před přijetím jakékoli žádosti poskytovatele;
- b) instanci peněženky před přijetím jakékoli žádosti instance;
- c) WSCD před odesláním jakékoli žádosti na WSCD.

Poznámka k hodnocení: V architekturách, kde WSCA běží uvnitř WSCD, může být autentizace WSCA→WSCD implicitní. V architekturách se vzdáleným WSCD, kde WSCA běží na serveru v blízkosti WSCD, musí být autentizace explicitní a chráněná kryptograficky dle požadavku CRY-05.

WSA-02 [Sec]: WSCA musí umožnit poskytovateli peněženky vytvořit jednoho uživatele a může umožnit vytvoření více uživatelů. Pokud je podporováno více uživatelů v rámci téže WSCA, musí WSCA zajistit, že data daného uživatele jsou přístupná pouze po úspěšné autentizaci tohoto uživatele v téže relaci.

Poznámka k hodnocení: V architektuře se vzdáleným WSCD zpravidla WSCA obsluhuje vícero uživatelů současně. Izolace uživatelů v rámci WSCA je kritickou vlastností a hodnotitel ji ověří formou inspekce implementace a testování napříč uživateli.

WSA-03 [Sec]: WSCA musí zahrnovat mechanismy pro autentizaci uživatele s nejméně dvěma autentizačními faktory různých kategorií, které splňují požadavky oddílů 2.2.1 a 2.3 přílohy k CIR (EU) 2015/1502 pro úroveň záruky „vysoká“.

WSA-04 [Sec]: WSCA musí:

- a) zahrnovat mechanismy pro správu a použití kryptografických klíčů jménem uživatele (vytváření klíčových párů, použití klíčů pro šifrování, podepisování a ověřování, export veřejných klíčů);
- b) umožnit použití kryptografických aktiv spravovaných WSCD pouze po úspěšné autentizaci uživatele dle požadavku WSA-03;
- c) zajistit, že po úspěšné autentizaci mohou být provedeny pouze ty operace, pro které byla autentizace poskytnuta (v souladu s požadavkem AUTH-04).

Poznámka k hodnocení: Audit pravidel pro operace prováděné po jediné autentizaci; inspekce implementace; penetrační testování pokusu o rozšíření autorizace na jiné operace.

WSA-05 [Sec]: WSCA by neměla být schopna exportovat soukromé klíče spravované uživatelem. Pokud WSCD umožňuje export klíčů, výsledná úroveň ochrany exportovaných klíčů musí být ekvivalentní úrovni ochrany v rámci WSCD.

Poznámka k hodnocení: Doporučený princip je zákaz exportu soukromých klíčů z WSCA. V případech, kdy je export technicky nezbytný (například pro specifické scénáře obnovy), musí být podrobně dokumentován a auditován.

WSA-06 [Sec]: WSCA musí být hodnocena dle metodologie Common Criteria (EUC). Pro architekturu, v níž WSCA operuje v těsné blízkosti WSCD (zejména pro architekturu se vzdáleným WSCD, kde WSCA běží na serveru sousedícím s WSCD), je minimální požadovanou úrovní posouzení zranitelností AVA_VAN.3, a to za předpokladu, že:

- a) existuje zdokumentované odůvodnění prokazující, že provozní prostředí eliminuje vektory fyzického útoku na WSCA;
- b) toto odůvodnění je konzistentní s požadavky přílohy IV oddílů 2 a 3 CIR (EU) 2024/2981 pro hodnocení zbytkových rizik a pokrytí předpokladů provozního prostředí;
- c) snížení úrovně posouzení zranitelností z AVA_VAN.5 na AVA_VAN.3 nemá negativní dopad na celkovou bezpečnost certifikované služby.

Úroveň AVA_VAN.5 zůstává preferovaným cílem, je-li její dosažení technicky a ekonomicky proveditelné. Certifikace WSCA je nezávislá na certifikaci řešení peněženky a může být prováděna samostatně v rámci schématu EUC.

X.6.6 Požadavky na WSCD a keystore

WSCD-01 [Sec]: WSCD musí být certifikován nejméně na úrovni EAL4 s posouzením zranitelností AVA_VAN.5 v rámci EUC nebo schématu Common Criteria, nebo poskytnout ekvivalentní úroveň záruky v souladu s přílohou IV CIR (EU) 2024/2981.

Poznámka k hodnocení: Přijatelnost existujícího certifikátu WSCD se posuzuje formou analýzy závislosti dle přílohy IX schématu. Požadavek je propojen s požadavkem CRY-04 v kapitole X.4.5.

WSCD-02 [Sec, Cond]: V architekturách, kde jeden WSCD (zejména WSCD provozovaný ve formě HSM) obsluhuje více uživatelů současně, musí WSCD ve spolupráci s WSCA implementovat logické oddělení jednotek peněženky různých uživatelů (multi-tenancy security), zajišťující, že:

- a) kryptografický klíčový materiál každého uživatele je přístupný pouze autentizovaným relacím tohoto uživatele a nelze k němu přistoupit z jiné relace;
- b) administrativní přístup k WSCD nemůže přistupovat ke klíčovému materiálu jednotlivých uživatelů bez explicitní autorizace prostřednictvím mechanismů dvojité kontroly dle požadavku ACC-02 v kapitole X.4.4;

c) selhání nebo kompromitace logické instance WSCD jednoho uživatele nesmí ovlivnit bezpečnost logických instancí WSCD jiných uživatelů.

Poznámka k hodnocení: Multi-tenancy izolace je jednou z nejkritičtějších vlastností architektury se vzdáleným WSCD. Hodnotitel ji ověří formou inspekce implementace a testování pokusem o přístup k aktivům jiného uživatele a pokusem o eskalaci privilegií z uživatelské relace na administrativní.

WSCD-03 [Sec, Cond]: V architekturách, kde WSCD představuje centralizovanou komponentu obsluhující více jednotek peněženky, musí WSCD implementovat redundanci a mechanismy obnovy po havárii zajišťující kontinuitu kryptografických služeb, s cílovými dobami obnovy (RTO) a cílovými body obnovy (RPO) definovanými v souladu s požadavky BCM-04 v kapitole X.4.11.

Poznámka k hodnocení: Požadavek je propojen s BCM-04 (Kontinuita činnosti) a s NET-02 (Síťová bezpečnost). Hodnotitel ověří existenci redundance, provedené testy obnovy a dokumentované RTO/RPO.

KST-01 [Sec]: Jednotka peněženky může zahrnovat jeden nebo více keystore (úložišť klíčů) pro uložení kryptografického materiálu s nižší úrovní kritičnosti než u kritických aktiv spravovaných WSCA/WSCD. Každému keystore musí být přiřazena úroveň záruky odpovídající citlivosti uloženého materiálu. Keystore jsou hodnoceny jako součást hodnocení instance peněženky nejméně na úrovni posouzení zranitelnosti AVA_VAN.3.

Poznámka k hodnocení: Keystore jsou architektonickým prvkem umožňujícím diferenciaci úrovně ochrany různých kategorií aktiv v jednotce peněženky. Kritická aktiva (zejména soukromé klíče vázané na PID) musí být vždy uložena ve WSCD, nikoli v keystore.

X.7 Požadavky na služby poskytovatele peněženky

Tato kapitola definuje bezpečnostní požadavky na služby provozované poskytovatelem peněženky. Pokrývá správu jednotky peněženky (aktivace, monitorování, správu WUA a WIA), službu jednotky peněženky a proces nahrávání a aktualizace.

Výchozí metoda hodnocení pro požadavky této kapitoly je kombinace auditu (přezkum politik a dokumentace) a inspekce (ověření implementace), doplněná o specifické testování pro aktivační tok, revokační tok a aktualizací tok. Specifické metody jsou uvedeny v poznámce k hodnocení u jednotlivých požadavků.

X.7.1 Aktivace a monitorování jednotky peněženky

WPS-01 [Fun]: Poskytovatel peněženky musí zajistit, že nerevokovaná jednotka peněženky ve stavu „provozní“ a „platná“ je schopna prezentovat časově platnou a nerevokovanou WUA poskytovateli PID nebo poskytovateli atestace v průběhu vydávání PID nebo atestace.

WPS-02 [Sec]: Po celou dobu životního cyklu jednotky peněženky musí poskytovatel peněženky pravidelně ověřovat, že její bezpečnost není narušena ani kompromitována. Pokud je narušení detekováno, poskytovatel peněženky:

- a) analyzuje příčiny a dopady narušení;
- b) je-li ovlivněna důvěryhodnost jednotky peněženky, administrativně revokuje dotčenou jednotku peněženky a okamžitě revokuje všechny její WUA;
- c) rozšíří analýzu na další potenciálně dotčené jednotky peněženky.

Poznámka k hodnocení: Revokace je vyžadována přinejmenším v situacích, kdy bezpečnost jednotky peněženky, mobilního zařízení nebo operačního systému, na němž je instance peněženky provozována, nebo WSCA/WSCD je kompromitována, je kompromitováno řešení peněženky jako celek, jsou kompromitovány společné autentizační mechanismy, nebo je kompromitován systém eID, v jehož rámci je peněženka poskytována.

WPS-03 [Sec]: Během aktivace nové jednotky peněženky musí poskytovatel peněženky ověřit, že nová instance peněženky je pravou instancí aplikace peněženky určené pro daný operační systém uživatelského zařízení.

Poznámka k hodnocení: Ověření zpravidla vyžaduje podporu platformy uživatelského zařízení (například Play Integrity API pro Android, App Attest pro iOS). Je-li použit mechanismus vlastního ověření poskytovatele peněženky, musí být tento mechanismus jednoznačně specifikován a jeho účinnost musí být prokázána v rámci hodnocení.

WPS-04 [Sec]: Během aktivace musí poskytovatel peněženky provést kontroly způsobilosti uživatelského zařízení dle definovaných kritérií způsobilosti (verze operačního systému, dostupné bezpečnostní funkce, integrity platformy). Pokud zařízení není způsobilé, poskytovatel peněženky o tom informuje uživatele a uvede důvod.

WPS-05 [Sec]: Během aktivace musí poskytovatel peněženky zajistit, že uživatel má uživatelský účet u poskytovatele peněženky, a to buď autentizací ke stávajícímu účtu, nebo zřízením nového účtu. Zřízení účtu musí:

- a) jasně vysvětlit účel účtu uživateli (zejména možnost revokace jednotky peněženky při ztrátě nebo krádeži uživatelského zařízení);
- b) zaregistrovat autentizační metody nezávislé na jednotce peněženky a na uživatelském zařízení;
- c) umožnit uživateli registraci pod aliasem, pokud uživatel nechce použít své skutečné jméno;
- d) nepoužívat registrovaná data pro jiné účely bez souhlasu uživatele.

Poznámka k hodnocení: Tento požadavek je zásadní pro scénář obnovy jednotky peněženky po ztrátě nebo krádeži uživatelského zařízení. Nezávislá autentizační metoda umožňuje obnovení jednotky peněženky bez nutnosti přístupu k původnímu zařízení. Konkrétní postup obnovy je definován v požadavku WPS-09.

WPS-06 [Sec]: Poskytovatel peněženky aktivuje novou jednotku peněženky pouze tehdy, pokud ověřil, že jednotka peněženky obsahuje WSCA/WSCD certifikovanou pro shodu s požadavky úrovně záruky „vysoká“.

Poznámka k hodnocení: Ověření certifikace WSCA/WSCD se provede formou kontroly platnosti certifikátu v rámci aktivačního toku. Certifikát musí splňovat požadavky CRY-04 v kapitole X.4.5 a WSCD-01 v kapitole X.6.6.

WPS-07 [Sec]: Veškerá komunikace mezi poskytovatelem peněženky a jednotkou peněženky musí být vzájemně autentizována a šifrována, jsou-li komponenty hostovány na různých systémech.

Poznámka k hodnocení: Tento požadavek je propojen s požadavky CRY-05 (kapitola X.4.5), NET-02 (kapitola X.4.8) a WIN-01 písm. f) (kapitola X.6.4.1).

WPS-08 [Sec]: Po celou dobu životního cyklu jednotky peněženky musí poskytovatel peněženky:

- a) aktualizovat jednotku peněženky podle potřeby pro zachování její bezpečnosti, v souladu s procesem řízení změn dle kapitoly X.5.2 a procesem řízení zranitelností dle kapitoly X.5.3;
- b) monitorovat instalovanou bázi jednotek peněženky pro účely údržby s dokumentovaným a transparentním sběrem dat;
- c) monitorovat bezpečnostní stav provozních instancí peněženky pro detekci kritických bezpečnostních rizik v provozním prostředí, včetně detekce neoprávněných úprav uživatelského zařízení (rooting, jailbreaking).

Poznámka k hodnocení: Rozsah sběru monitorovacích dat je omezen požadavkem DPR-02. Monitorovaná data zpravidla zahrnují chyby běhu, verzi a stav operačního systému, verzi instance peněženky, schopnosti WSCA/WSCD, identifikátory zařízení (např. IDfV, AndroidID), úroveň bezpečnostních záplat senzorů, podporu BLE/NFC. Detekce úprav uživatelského zařízení je povinná.

WPS-09 [Sec, Cond]: Poskytovatel peněženky musí implementovat proces obnovy jednotky peněženky po ztrátě nebo krádeži uživatelského zařízení, zajišťující, že ztracené nebo odcizené zařízení nepovede ke krádeži identity uživatele. Proces obnovy musí:

- a) vyžadovat autentizaci uživatele prostřednictvím nezávislé metody registrované během aktivace dle požadavku WPS-05;
- b) revokovat všechny WUA asociované se ztracenou jednotkou peněženky dle požadavků kapitoly X.7.3;
- c) bezpečně zničit kryptografický klíčový materiál ve WSCD asociovaný se ztracenou jednotkou peněženky;
- d) umožnit aktivaci nové jednotky peněženky na novém uživatelském zařízení s minimálním narušením pro uživatele, včetně pomoci uživateli s opakovaným vydáním PID a dalších atestací;
- e) zaznamenat celý proces obnovy v logu pro účely auditu a pro případné šetření orgánů činných v trestním řízení.

Poznámka k hodnocení: Architektura se vzdáleným WSCD má výhodu, že kryptografický klíčový materiál není uložen na ztraceném uživatelském zařízení, ale jeho zničení na straně WSCD musí být explicitně řízeno procesem definovaným tímto požadavkem. Hodnotitel ověří proces obnovy formou testování.

X.7.2 Vydávání a správa atestace jednotky peněženky (WUA)

WUA-01 [Sec]: Poskytovatel peněženky musí mít politiku řídící všechny aspekty vydávání a správy WUA. Pro WUA popisující WSCA/WSCD musí politika splňovat alespoň rozšířenou normalizovanou certifikační politiku (NCP+) dle ETSI EN 319 411-1. Pro WUA popisující keystore musí politika splňovat alespoň normalizovanou certifikační politiku (NCP).

WUA-02 [Sec, Privacy]: Poskytovatel peněženky nesmí zahrnovat žádné informace o uživateli jednotky peněženky do WUA.

Poznámka k hodnocení: Tento požadavek brání identifikaci uživatele prostřednictvím obsahu WUA. WUA popisuje pouze technické vlastnosti jednotky peněženky (zejména WSCA/WSCD a jejich možnosti), nikoli uživatele.

WUA-03 [Sec, Privacy]: Po vydání WUA poskytovatel peněženky odstraní hodnoty všech jedinečných prvků a časových razítek, jakmile již nejsou potřebné. Poskytovatel peněženky tyto hodnoty nesmí sdělovat žádné jiné straně.

Poznámka k hodnocení: Tento požadavek na ochranu soukromí brání sledování uživatele prostřednictvím metadat WUA.

WUA-04 [Sec]: WUA vydaná poskytovatelem peněženky musí mít minimální dobu platnosti 24 hodin a musí být kryptograficky podepsána s použitím algoritmů doporučených v dokumentu ECCG Agreed Cryptographic Mechanisms.

WUA-05 [Sec]: WUA musí obsahovat jedinečný identifikátor jednotky peněženky umožňující její identifikaci pro účely revokace, aniž by tento identifikátor umožnil identifikaci uživatele jednotky peněženky.

X.7.3 Revokace atestace jednotky peněženky

REV-01 [Sec]: Revokace WUA znamená revokaci celé jednotky peněženky. Poskytovatel peněženky je jedinou entitou oprávněnou provést revokaci jednotky peněženky. Revokace je nevratná — jakmile je jednotka peněženky revokována, nemůže být její stav vrácen do platného stavu, a uživatel musí pro pokračování v používání služby aktivovat novou jednotku peněženky.

REV-02 [Sec]: Poskytovatel peněženky musí revokovat jednotku peněženky na výslovnou žádost uživatele registrovaného během aktivace dle požadavku WPS-05 a musí poskytnout uživateli rozhraní pro takové žádosti dostupné prostřednictvím nezávislé autentizační metody. Revokace na žádost uživatele musí zahrnovat všechny platné WUA dané jednotku peněženky.

Poznámka k hodnocení: Tento požadavek je primárním ochranným mechanismem uživatele proti krádeži nebo ztrátě uživatelského zařízení.

REV-03 [Sec]: Poskytovatel peněženky musí revokovat jednotku peněženky na výslovnou žádost poskytovatele PID (zejména v případě úmrtí uživatele nebo ukončení činnosti právnické osoby), po ověření, že žádající poskytovatel PID je registrován v seznamu důvěryhodných entit poskytovatelů PID.

Poznámka k hodnocení: Komunikační kanál mezi poskytovatelem peněženky a poskytovatelem PID pro revokační žádosti musí být autentizovaný, šifrovaný a dokumentovaný v politice poskytovatele peněženky.

REV-04 [Sec]: Poskytovatel peněženky musí revokovat jednotku peněženky na základě dalších definovaných spouštěcích událostí, zejména:

- a) na základě výsledku monitorování dle požadavku WPS-08, pokud je detekována kompromitace bezpečnostního stavu jednotky peněženky;
- b) na základě výsledku procesu řízení podvodů dle kapitoly X.5.5, pokud je detekováno podvodné použití jednotky peněženky;
- c) na základě rozhodnutí orgánu dohledu, soudu nebo orgánu činného v trestním řízení v souladu s právními předpisy České republiky;
- d) na základě ukončení platnosti smluvního vztahu s uživatelem.

REV-05 [Sec]: Poskytovatel peněženky musí informovat uživatele bez zbytečného odkladu, nejpozději však do 24 hodin, o jakékoli revokaci jeho jednotky peněženky, a to prostřednictvím komunikačního kanálu nezávislého na jednotce peněženky. Notifikace musí zahrnovat:

- a) důvod nebo důvody revokace;
- b) technické údaje o případném bezpečnostním narušení, je-li to relevantní;
- c) postup pro aktivaci nové jednotky peněženky, pokud uživatel chce v používání služby pokračovat;
- d) informace o ochraně práv uživatele a o možnosti podání stížnosti.

REV-06 [Sec]: Poskytovatel peněženky musí zahrnout specifické ochrany proti útokům odepření služby (denial of service) pro mechanismy používané pro stahování seznamů stavu atestací. Mechanismy musí zahrnovat omezení rychlosti, geografickou distribuci a kapacitní rezervu odpovídající špičkovému zatížení.

X.7.4 Vydávání a správa atestace instance peněženky (WIA)

WIA-01 [Sec]: Poskytovatel peněženky musí:

- a) zajistit, že všechny WIA mají dobu platnosti kratší než 24 hodin (nevyžaduje se správa revokace);
- b) ověřit integritu instance peněženky před podpisem WIA, a to s použitím mechanismů verifikace platformy nebo ekvivalentních mechanismů poskytovatele peněženky.

WIA-02 [Fun]: Poskytovatel peněženky musí zajistit, že nerevokovaná jednotka peněženky je kdykoli schopna prezentovat časově platnou a nerevokovanou WIA poskytovateli PID nebo poskytovateli atestace v průběhu vydávání PID nebo atestace.

X.7.5 Služba jednotky peněženky

Služba jednotky peněženky je služba IKT poskytovaná poskytovatelem peněženky, který v rámci svých systémů IKT implementuje některé funkce jednotky peněženky. Jedná se o podmíněnou komponentu — uplatní se v případech, kdy zvolená architektura umísťuje část logiky jednotky peněženky na serverovou infrastrukturu poskytovatele peněženky. V architekturním profilu schématu EUDIW-CZ se vzdáleným WSCD je tato komponenta v rozsahu certifikace.

WUS-01 [Sec, Cond]: Služba jednotky peněženky musí implementovat striktní logické oddělení mezi serverovými daty jednotky peněženky a administrativní infrastrukturou poskytovatele peněženky, zajišťující, že personál poskytovatele peněženky nemůže přistupovat k obsahu jednotlivých jednotek peněženky.

Poznámka k hodnocení: Tento požadavek navazuje na požadavek WUG-05 v kapitole X.6.1. Hodnotitel formou inspekce ověří oddělení hostovací infrastruktury jednotky peněženky od administrativní infrastruktury poskytovatele a ověří šifrování a řízení přístupu k uživatelským datům spravovaným službou jednotky peněženky.

WUS-02 [Sec, Cond]: Služba jednotky peněženky provozovaná na vzdálené infrastruktuře musí zajistit:

- a) vzájemnou autentizaci a šifrování veškeré komunikace s instancí peněženky v souladu s požadavky NET-02 a CRY-05 v kapitole X.4;
- b) správu relací zabraňující neoprávněnému přístupu k datům jiných uživatelů;
- c) implementaci omezení rychlosti a detekci anomálních přístupových vzorů v souladu s požadavkem FRD-05 v kapitole X.4.9.1;
- d) zaznamenávání administrativního přístupu a uplatnění opatření řízení privilegovaného přístupu (PAM) dle požadavku ACC-02 v kapitole X.4.4.

WUS-03 [Sec, Cond]: Služba jednotky peněženky musí splňovat požadavky CIR (EU) 2015/1502 na úrovni záruky „vysoká“, zejména požadavky vztahující se na komponenty správy a autentizace prostředků elektronické identifikace.

X.7.6 Proces nahrávání a aktualizace

UPD-01 [Sec]: Poskytovatel služby EUDI musí zavést a provozovat bezpečný proces pro nahrávání a aktualizaci komponent instance peněženky a WSCA. Proces musí být integrován s procesem řízení změn dle kapitoly X.5.2 a s procesem řízení zranitelností dle kapitoly X.5.3.

UPD-02 [Sec]: Proces nahrávání a aktualizace musí implementovat podepisování kódu pro všechny distribuované komponenty. Klíč pro podepisování kódu musí být chráněn na úrovni odpovídající kritičnosti podepsané komponenty:

- a) klíč pro podepisování instance peněženky musí být chráněn na úrovni minimálně odpovídající úrovni záruky „vysoká“;

b) klíč pro podepisování WSCA musí být chráněn v HSM s certifikací odpovídající kritičnosti komponenty.

Poznámka k hodnocení: Kompromitace mechanismu aktualizace znamená kompromitaci celého řešení peněženky. Hodnotitel formou inspekce ověří uložení a použití podpisových klíčů.

UPD-03 [Sec]: Bezpečnostní aktualizace musí být distribuovány odděleně od funkčních aktualizací, je-li to technicky proveditelné, aby bylo umožněno rychlé nasazení nápravy zranitelnosti bez nutnosti úplného funkčního testování celé aktualizace.

UPD-04 [Sec]: Poskytovatel peněženky musí implementovat mechanismus pro bezpečnou distribuci aktualizací zahrnující v relevantních případech:

- a) automatizovanou distribuci bezpečnostních aktualizací;
- b) mechanismus pro pozastavení činnosti jednotky peněženky do doby, než budou aplikovány požadované bezpečnostní aktualizace;
- c) informační zprávy poskytující uživatelům relevantní informace o dostupných aktualizacích a doporučeních.

UPD-05 [Sec, Cond]: V architekturách, kde WSCA je provozována jako sdílená komponenta obsluhující více jednotek peněženky (zejména v architektuře se vzdáleným WSCD), musí proces aktualizace WSCA zajistit:

- a) aby aktualizace WSCA nepřerušila aktivní uživatelské relace;
- b) aby kompatibilita verze WSCA s verzí instance peněženky byla ověřena před aktivací aktualizované WSCA;
- c) aby byly definovány a otestovány postupy pro návrat k předchozí verzi v případě, že aktualizace zavede bezpečnostní problém;
- d) aby byli informováni uživatelé a klíčové entity ekosystému (zejména poskytovatel PID a provozovatel ověřovací služby) o plánovaných i skutečných změnách verze WSCA.

Poznámka k hodnocení: WSCA na vzdáleném WSCD je sdílenou infrastrukturou — aktualizace má dopad na všechny uživatele současně. Toto vytváří riziko odlišné od situace s lokálním WSCD, kdy má každé uživatelské zařízení vlastní instanci WSCA.

X.7.7 Ochrana údajů při poskytování peněženky

DPR-01 [Sec]: Poskytovatel peněženky musí uchovávat osobní údaje týkající se poskytování služby peněženky logicky odděleně od jakýchkoli jiných údajů, které má v držení. Oddělení musí být doloženo architektonickou dokumentací a datovými toky a přístup k těmto údajům musí být možný pouze prostřednictvím řízených rozhraní služby EUDI s řízením přístupu dle kap. X.4.4. Poskytuje-li peněženku soukromá strana, vztahuje se oddělení na údaje všech ostatních služeb, které poskytovatel nabízí (čl. 45h odst. 3 nařízení eIDAS se použije přiměřeně).

Poznámka k hodnocení: Požadavek provádí povinnost logického oddělení osobních údajů dle čl. 5a odst. 14 eIDAS, která jako jediná z povinností tohoto odstavce spadá do povinného rozsahu certifikace dle čl. 5c odst. 1. Požadavky DPR-02 a DPR-03 provádějí zbývající povinnosti čl. 5a odst. 14 (neshromažďovat informace o používání, nekombinovat údaje). Jde o přímé zákonné povinnosti poskytovatele peněženky, které schéma EUDIW-CZ ponechává jako povinné požadavky [Sec] a vede je jako doplnění schématu (kapitola X.1.4). Navazuje na WUG-05 (X.6.1) a WUS-01 (X.7.5), které řeší oddělení vůči administrativní infrastruktuře poskytovatele. DPR-01 rozšiřuje oddělení na veškerá ostatní data v držení poskytovatele. Hodnotitel ověří inspekci architektury, datových toků a řízení přístupu.

DPR-02 [Sec]: Poskytovatel peněženky nesmí shromažďovat informace o používání jednotky peněženky, které nejsou nezbytné pro poskytování služby peněženky. Sběr dat dle požadavků WPS-08 písm. b) a c) (monitorování) a EVD-01 (shromažďování důkazů) musí být omezen na tento nezbytný rozsah, dokumentován a nesmí zahrnovat informace o transakcích uživatele (zejména kdy, kde a vůči komu uživatel použil PID nebo atestaci), v souladu s WUG-05.

DPR-03 [Sec]: Poskytovatel peněženky nesmí kombinovat osobní identifikační údaje ani jiné osobní údaje uložené v jednotce peněženky nebo údaje o jejím používání s osobními údaji z jiných služeb, které nabízí, nebo ze služeb třetích stran, které nejsou nezbytné pro poskytování služby peněženky, ledaže o to uživatel výslovně požádal. Taková žádost uživatele musí být doložitelná auditním záznamem.

X.8 Požadavky na služby poskytovatele PID

Tato kapitola definuje bezpečnostní požadavky na služby provozované poskytovatelem PID za účelem poskytování systému eID, v jehož rámci jsou peněženky EUDI poskytovány. Požadavky vycházejí z rozsahu komponent definovaných v příloze I schématu EUDIW-CZ.

Komponenty služby poskytovatele PID, které spadají do rozsahu certifikace dle této kapitoly:

- a) systém IKT poskytovatele PID — pokrytý kapitolami X.4 a X.5;
- b) procesy ISMS poskytovatele PID — pokryté kapitolou X.5;
- c) registrace a správa uživatelů (onboarding) — pokrytá kapitolou X.8.4;
- d) poskytování a správa PID — pokrytá kapitolami X.8.1, X.8.2 a X.8.3.

Poskytovatel PID, který současně zastává jiné role v ekosystému EUDIW (zejména role vlastníka schématu, orgánu dohledu, registrátora spoléhajících se stran), musí dodržovat požadavky na oddělení povinností dle požadavku ORG-05 v kapitole X.4.1.

V případě subdodavatelského vývoje systému poskytovatele PID nebo subdodavatelského zajištění specifických komponent (zejména služby pečetení PID) se uplatní požadavky kapitoly X.4.14 na dodavatelský řetězec, zejména požadavky SUP-04 a SUP-06.

X.8.1 Vydávání PID

PIDR-01 [Sec]: Poskytovatel PID musí mít politiku upravující všechny aspekty vydávání a správy PID. Politika musí splňovat alespoň požadavky CIR (EU) 2024/2977, zohledňující PID Rulebook a případně rovněž specifikace ETSI TS 119 471 a ETSI TS 119 472-2.

Poznámka k hodnocení: Tato politika je základním dokumentem politik poskytovatele PID. Hodnotitel formou auditu ověří soulad politiky s požadavky CIR (EU) 2024/2977, s respektováním specifik vydávání PID oproti vydávání certifikátů veřejných klíčů.

PIDR-02 [Sec]: Před aktivací PID musí poskytovatel PID ověřit identitu subjektu PID v souladu s požadavky úrovně záruky „vysoká“.

Poznámka k hodnocení: Konkrétní postup ověření identity je dále specifikován v kapitole X.8.4 (požadavky ONB-01 a ONB-02).

PIDR-03 [Sec]: Během vydávání PID musí poskytovatel PID ověřit, že poskytovatel peněženky uvedený v WIA je přítomen v seznamu důvěryhodných entit poskytovatelů peněženky (Wallet Provider List of Trusted Entities), a poté autentizovat WIA pomocí důvěryhodných kotev registrovaných pro daného poskytovatele peněženky v tomto seznamu.

Poznámka k hodnocení: Testování zahrnující negativní testovací případy s neplatnými, revokovanými nebo neznámými WIA, a inspekce ověřující, že je použit aktuální seznam důvěryhodných entit poskytovatelů peněženky.

PIDR-04 [Sec]: Během vydávání PID musí poskytovatel PID ověřit obsah WIA, zejména:

- a) platnost a integritu WIA;
- b) odpovídající dobu platnosti WIA (kratší než 24 hodin dle požadavku WIA-01);
- c) konzistenci obsahu WIA s ostatními informacemi dostupnými o jednotce peněženky.

Poznámka k hodnocení: Ověření obsahu WIA je významné, protože kontrola pravosti instance peněženky je propojena s vydáváním WIA.

PIDR-05 [Sec]: Poskytovatel PID musí používat kryptograficky bezpečný generátor pseudonáhodných čísel (CSRNG) pro generování všech náhodných čísel používaných v PID (hashovací soli, identifikátory, nonce a podobně).

PIDR-06 [Sec, Privacy]: Při vydávání PID v dávce do téže jednotky peněženky musí poskytovatel PID zajistit, že časová razítka v těchto PID neumožní spoléhajícím se stranám usoudit, že PID jsou součástí stejné dávky (a tedy patří témuž uživateli).

Poznámka k hodnocení: Tento požadavek je zásadní pro zachování nesledovatelnosti uživatele. Hodnotitel ověří mechanismus generování časových razítek a způsob jeho začlenění do procesu dávkového vydávání.

PIDR-07 [Sec, Privacy]: Po vydání PID musí poskytovatel PID odstranit hodnoty všech jedinečných prvků a všechna časová razítka, jakmile již nejsou potřebné pro provoz služby. Poskytovatel PID nesmí tyto hodnoty sdělovat žádné další straně uvnitř ani vně ekosystému EUDIW.

Poznámka k hodnocení: Tyto jedinečné prvky by mohly být použity pro sledování uživatele nebo pro jeho zosobnění. Hodnotitel formou inspekce ověří proces odstraňování hodnot a jejich nesdělování.

PIDR-08 [Sec]: Poskytovatel PID musí:

- a) zahrnout do svých metadat OpenID4VCI Issuer seznam metod prezentace, které mají být použity, seřazený dle preference, zahrnující alespoň Metodu A nebo Metodu B dle požadavku WUM-01 v kapitole X.6.2.2;
- b) v maximální možné míře zajistit, aby uživatelé nezaznamenali, která metoda je používána pro správu jejich PID.

PIDR-09 [Sec]: Poskytovatel PID musí validovat identifikační údaje ve vydávaných PID vůči autoritativnímu zdroji identitních údajů před vydáním PID, a zajistit, že obsah PID odpovídá aktuálnímu stavu autoritativního zdroje.

Poznámka k hodnocení: Validace vůči autoritativnímu zdroji představuje sekundární kontrolu nad rámcem kontroly identity uživatele provedené během onboardingu (požadavek PIDR-02). Autoritativním zdrojem identitních údajů se rozumí registr veřejné správy stanovený právními předpisy České republiky pro účely identifikace fyzických osob (zejména registr obyvatel).

PIDR-10 [Sec, Cond]: Pokud je elektronické pečetění PID prováděno externím poskytovatelem služby pečetění (kvalifikovaným poskytovatelem služeb vytvářejících důvěru), pečetění musí být provedeno s použitím kvalifikované elektronické pečeti v souladu s požadavky eIDAS. Poskytovatel PID musí ověřit integritu pečeti před uvolněním PID do jednotky peněženky.

Poznámka k hodnocení: Existující certifikace QTSP poskytovatele služby pečetění může být použita jako vstup analýzy závislosti dle přílohy IX schématu (kapitola IX.6.7). Hodnotitel ověří, že rozsah QTSP certifikace pokrývá specifické použití pro pečetění PID v ekosystému EUDIW.

PIDR-11 [Sec]: Poskytovatel PID musí implementovat anti-podvodné monitorování během procesu vydávání PID, zahrnující minimálně:

- a) detekci anomálních vzorů vydávání (například hromadné žádosti o vydání z jednoho zdroje, žádosti v neobvyklých časových vzorech);
- b) křížové kontroly s transakčními záznamy poskytovatele prostředku elektronické identifikace pro detekci anomálií onboardingu;
- c) eskalační postupy do procesu řízení podvodů definovaného v kapitole X.5.5.

Poznámka k hodnocení: Tento požadavek je propojen s požadavkem FRD-P03 písm. a) a c) v kapitole X.5.5 a s požadavkem FRD-05 v kapitole X.4.9.1.

X.8.2 Správa PID

PIDM-01 [Sec]: Poskytovatel PID musí zajistit, že atributy potvrzené ve vydaném PID jsou platné pro identifikovaný subjekt PID v jakémkoli okamžiku platnosti PID.

Poznámka k hodnocení: Tento požadavek vyžaduje, aby poskytovatel PID měl mechanismus pro detekci změn v autoritativním zdroji identitních údajů (zejména změna jména, úmrtí subjektu) a pro zahájení opětovného vydání PID nebo jeho revokace v reakci na takové změny. Konkrétní mechanismus je specifikován v požadavku PIDM-03.

PIDM-02 [Sec]: Poskytovatel PID musí ověřit, že znovu vydaný PID je vydán téže jednotce peněženky jako stávající PID.

Poznámka k hodnocení: Mechanismus typicky vychází z obnovovacích tokenů. Pro aktiva na úrovni WSCA musí být obnovovací token chráněn na úrovni WSCA (tj. uložen a zpracováván v rámci WSCA).

PIDM-03 [Sec]: Poskytovatel PID musí implementovat mechanismus pro automatickou detekci změn v autoritativním zdroji identitních údajů, které ovlivňují subjekty vydaných PID, a musí zahájit revokaci PID ve stanoveném časovém rámci po detekci takové změny (opětovné vydání PID je iniciováno jednotkou peněženky).

Poznámka k hodnocení: Konkrétní časový rámec pro reakci na detekované změny musí být definován v politice vydávání PID dle požadavku PIDR-01 a ověřen během dozorových hodnocení. Mechanismus detekce změn musí být odolný vůči zpožděním v autoritativním zdroji a musí zahrnovat postup pro situace, kdy autoritativní zdroj není dočasně dostupný.

X.8.3 Revokace PID

PIDR-R01 [Sec]: Pokud je PID revokovatelné, poskytovatel PID musí:

- a) mít politiku specifikující podmínky, za nichž bude PID revokováno;
- b) revokovat PID, pokud byla narušena jeho bezpečnost.

PIDR-R02 [Sec]: Pokud je PID revokovatelné, poskytovatel PID musí PID revokovat:

- a) na výslovnou žádost uživatele, jemuž bylo PID vydáno;
- b) pokud je revokována jednotka peněženky, na níž se PID nachází;
- c) po úmrtí fyzické osoby, která je subjektem PID;
- d) pokud poskytovatel PID detekuje významné změny v autoritativním zdroji identitních údajů, které vedou k tomu, že PID již neodpovídá skutečnosti (dle požadavku PIDM-03).

Poznámka k hodnocení: Detekce úmrtí subjektu PID se provádí prostřednictvím mechanismu detekce změn v autoritativním zdroji dle požadavku PIDM-03. Detekce revokace jednotky peněženky se provádí prostřednictvím mechanismu křížové kontroly dle požadavku PIDR-R06.

PIDR-R03 [Sec]: Poskytovatel PID musí být jedinou stranou odpovědnou za provedení revokace PID, které vydal. Revokace nesmí být vratitelná.

Poznámka k hodnocení: Delegace operativního provedení revokace na třetí stranu (například technického dodavatele) je možná, ale poskytovatel PID zůstává odpovědný za rozhodnutí o revokaci a za jeho správnost.

PIDR-R04 [Sec, Privacy]: Při použití seznamu stavu atestace (Attestation Status List) pro revokaci musí poskytovatel PID náhodně přiřadit index pro každé PID, aby se zabránilo tomu, že se index stane korelátorem umožňujícím sledování uživatele.

Poznámka k hodnocení: Privacy-preserving revokace je zásadním principem návrhu. Hodnotitel ověří mechanismus přiřazování indexů a vlastnost nesledovatelnosti seznamu stavu.

PIDR-R05 [Sec]: Poskytovatel PID vydávající revokovatelné PID musí:

- a) pro každý platný PID pravidelně ověřovat, zda poskytovatel peněženky nerevokoval jednotku peněženky, na níž se PID nachází;
- b) jakmile poskytovatel PID zjistí, že jednotka peněženky byla revokována, okamžitě revokovat příslušné PID.

Poznámka k hodnocení: Poskytovatel PID může pro tento účel využít informace o revokaci obsažené ve WUA přijaté během vydávání PID. Konkrétní mechanismus křížové kontroly s poskytovatelem peněženky je specifikován v požadavku PIDR-R06.

PIDR-R06 [Sec]: Poskytovatel PID musí implementovat mechanismus pro křížovou kontrolu stavu revokace jednotky peněženky s poskytovatelem peněženky nejméně jednou za 24 hodin. Tento mechanismus musí:

- a) být odolný vůči selháním komunikace mezi poskytovatelem PID a poskytovatelem peněženky;
- b) zahrnovat postup pro situace, kdy poskytovatel peněženky není dočasně dostupný;
- c) být dokumentován ve smluvním vztahu mezi poskytovatelem PID a poskytovatelem peněženky;
- d) být chráněn vzájemnou autentizací a šifrováním komunikace mezi oběma poskytovateli.

Poznámka k hodnocení: Tento požadavek řeší vztah mezi poskytovatelem PID a poskytovatelem peněženky pro účely sdílení informací o stavu revokace. Požadavek je propojen s požadavkem REV-03 v kapitole X.7.3, který upravuje opačný směr (revokace jednotky peněženky na žádost poskytovatele PID).

X.8.4 Onboarding a správa uživatelů

Tato kapitola doplňuje požadavky na ověření identity definované v požadavku PIDR-02 v kapitole X.8.1 o specifické požadavky na onboarding.

ONB-01 [Sec]: Proces onboardingu dle ETSI TS 119 461 V2.1.1 (2025-02) musí ověřit identitu žadatele na úrovni záruky „vysoká“ s použitím alespoň jedné z následujících metod:

- a) fyzická přítomnost žadatele s ověřením předložených dokladů totožnosti;
- b) použití prostředku elektronické identifikace vydaného v rámci kvalifikovaného systému elektronické identifikace na úrovni záruky „vysoká“ dle zákona 250/2017 Sb.;
- c) povýšení úrovně záruky prostředku elektronické identifikace vydaného v rámci kvalifikovaného systému elektronické identifikace z úrovně „značná“ na úroveň „vysoká“ (level-up) prostřednictvím dodatečného ověření, splňujícího požadavky CIR (EU) 2026/798, které aplikuje ETSI TS 119 461 V2.1.1 (2025-02).
 - Při ověřování totožnosti prostřednictvím dokladu totožnosti v případě vzdáleného automatického ověření bez dohledu musí být systém pro pořizování snímku žadatele hodnocen vůči „*biometric injection attack*“ nejpozději do konce roku 2026 (viz ETSI 119 461 V2.1.1 požadavek BIN-8.4.2-04C) akreditovanou laboratoří podle TS 18099 (viz ETSI 119 461 V2.1.1 požadavek BIN-8.4.2-04D).
 - Není-li k uvedenému datu prokazatelně dostupná laboratoř akreditovaná podle TS 18099, poskytovatel PID tuto skutečnost doloží certifikačnímu orgánu, uplatní do provedení hodnocení zdokumentovaná přechodná kompenzační opatření a hodnocení akreditovanou laboratoří doloží nejpozději při prvním dozorovém hodnocení následujícím po zpřístupnění takové laboratoře. Certifikační orgán přechodný stav zaznamená v certifikační zprávě.

Poznámka k hodnocení: V architekturním profilu schématu EUDIW-CZ je primární metodou onboardingu možnost ověření totožnosti prostřednictvím dokladu totožnosti v případě vzdáleného automatického ověření bez dohledu, tj. v souladu s odstavcem 9.5.2 normy ETSI TS 119 461 V2.1.1 (2025-02). Tato metoda je způsobem provedení písm. c) (povýšení úrovně záruky dle kap. 9.5 téže normy), jak je vymezeno v příloze Ib.1 schématu.

ONB-02 [Sec]: Proces onboardingu musí implementovat doplňková opatření k řešení rizik specifických dle ETSI TS 119 461 V2.1.1 (2025-02) pro infrastrukturu poskytovatele prostředku elektronické identifikace použitého pro onboarding, zahrnující minimálně:

- a) vazbu relace mezi autentizací prostřednictvím prostředku a aktivací jednotky peněženky;
- b) mechanismy proti opakovanému přehrání, zabraňující opakovanému použití autentizačních tokenů;
- c) detekci živosti (kontrola reálného uživatele, ochrana proti biometrickým podvrhům) pro krok biometrického ověření;
- d) časové limity platnosti výsledku ověření identity, do nichž musí být dokončena aktivace jednotky peněženky;
- e) mechanismy ochrany proti útokům typu identity injection v procesu povýšení úrovně záruky.

Poznámka k hodnocení: Vzhledem k tomu, že prostředek elektronické identifikace je součástí sdílené národní infrastruktury využívané více službami, je nezbytné jasně definovat a aktivně řídit veškeré navazující bezpečnostní vazby.

ONB-03 [Sec]: Proces onboardingu musí podléhat monitorování řízení podvodů v souladu s kapitolou X.5.5 (požadavek FRD-P03 písm. a)), zahrnující detekci minimálně:

- a) hromadných pokusů o onboarding z podobných profilů uživatelských zařízení;
- b) opakovaných neúspěšných pokusů o ověření identity z téhož zdroje;
- c) anomálních geografických vzorů v žádostech o onboarding;
- d) anomálních časových vzorů v žádostech o onboarding (například žádosti mimo obvyklou dobu nebo v neobvyklých koncentracích).

Poznámka k hodnocení: Onboarding je jedním z prioritních scénářů řízení podvodů dle požadavku FRD-P03 v kapitole X.5.5.

ONB-04 [Fun]: Výsledkem ověření totožnosti musí být důkaz ve smyslu kapitoly 8.5 ETSI TS 119 461 V2.1.1 (2025-02). Důkaz musí mít podobu strukturovaného dokumentu (např. JSON) a musí obsahovat minimálně výsledek ověření a čas ověření. Poskytovatel PID musí tyto důkazy uchovávat a jejich evidenci opatřit kvalifikovaným elektronickým časovým razítkem (jedno kvalifikované elektronické časové razítko může pokrývat i více těchto záznamů).

X.9 Požadavky na ověřovací službu

Tato kapitola definuje bezpečnostní požadavky na ověřovací (validační) službu umožňující ověření platnosti peněženek EUDI a autenticity registrovaných spoléhajících se stran v souladu s článkem 5a odst. 8 nařízení (EU) č. 910/2014 ve znění pozdějších předpisů (eIDAS).

Ověřovací služba je v rámci schématu EUDIW-CZ součástí certifikační oblasti služby peněženky vymezené v příloze I schématu EUDIW-CZ, tedy je certifikována společně se službou poskytovatele peněženky. Toto rozhodnutí vychází z architekturního profilu schématu EUDIW-CZ a je dále specifikováno v příloze I schématu EUDIW-CZ.

Komponenty ověřovací služby spadající do rozsahu certifikace:

- a) systém IKT ověřovací služby — pokrytý kapitolami X.4 a X.5;
- b) procesy ISMS provozovatele ověřovací služby — pokryté kapitolou X.5;
- c) mechanismy ověření platnosti jednotky peněženky — pokryté kapitolou X.9.2;
- d) mechanismy ověření identity spoléhající se strany — pokryté kapitolou X.9.3;

e) společný mechanismus pro identifikaci a autentizaci spoléhajících se stran — pokrytý kapitolou X.9.4.

Rozsah povinností ověřovací služby zahrnuje pouze poskytování informací o registrovaných spoléhajících se stranách a o stavu platnosti peněženek. Samotná registrace spoléhajících se stran (proces zařazení spoléhající se strany do registru) je pokryta v rámci povinností registrátora spoléhajících se stran a není přímou součástí rozsahu certifikace ověřovací služby.

X.9.1 Rozsah a kontext

Členské státy musí poskytovat bezúplatně validační mechanismy pro dva účely:

- a) zajištění ověření autenticity a platnosti peněženek EUDI;
- b) umožnění uživatelům peněženky ověřit autenticitu a platnost identity spoléhajících se stran.

Provozovatel ověřovací služby je pro účely tohoto schématu označen jako poskytovatel služby EUDI v rozsahu komponent dle této kapitoly. Pokud je provozovatel ověřovací služby současně poskytovatelem PID nebo zastává jiné role v ekosystému EUDIW (zejména role vlastníka schématu, orgánu dohledu, registrátora spoléhajících se stran), uplatní se požadavky na oddělení povinností dle požadavku ORG-05 v kapitole X.4.1 a požadavku VER-12 v kapitole X.9.5.

X.9.2 Ověření platnosti jednotky peněženky

VER-01 [Sec]: Ověřovací služba musí poskytnout mechanismus pro spoléhající se strany a další účastníky ekosystému k ověření autenticity a platnosti jednotek peněženky EUDI, zahrnující minimálně:

- a) možnost ověřit, že WUA bylo vydáno registrovaným poskytovatelem peněženky;
- b) možnost zkontrolovat stav revokace WUA;
- c) dostupnost seznamu důvěryhodných entit poskytovatelů peněženky (Wallet Provider List of Trusted Entities) registrovaných v České republice a v ostatních členských státech.

Poznámka k hodnocení: Tento mechanismus je základem kontrol důvěryhodných kotev definovaných v kapitole X.6.3.4 (požadavek TRU-01). Důvěryhodný řetězec registrace poskytovatele peněženky a jeho WUA je závislý na této službě.

VER-02 [Sec]: Ověřovací služba pro ověření platnosti peněženky musí zajistit integritu a autenticitu informací, které poskytuje, s využitím kvalifikovaných elektronických pečeti nebo ekvivalentních kryptografických mechanismů s odpovídající úrovní záruky.

Poznámka k hodnocení: Konkrétní kryptografické mechanismy musí splňovat doporučení ECCG Agreed Cryptographic Mechanisms a musí být v souladu s technickými specifikacemi definovanými prováděcími akty Komise.

VER-03 [Sec]: Ověřovací služba pro ověření platnosti peněženky musí být dostupná s úrovní dostupnosti odpovídající kritičnosti ekosystému peněženky EUDI a musí zahrnovat ochranu proti útokům odepření služby (denial of service).

Poznámka k hodnocení: Pokud je ověřovací služba nedostupná, jednotky peněženky nemohou ověřit identitu spoléhající se strany a spoléhající se strany nemohou ověřit platnost jednotek peněženky. To představuje systémové riziko pro celý ekosystém EUDIW. Konkrétní úroveň dostupnosti musí být definována v dohodě o úrovni služby (SLA) a musí být konzistentní s plánem kontinuity činnosti dle požadavku BCM-04 v kapitole X.4.11.

X.9.3 Ověření identity spoléhající se strany

VER-04 [Sec]: Ověřovací služba musí umožnit jednotkám peněženky a jejich uživatelům ověřit autenticitu a platnost identity spoléhajících se stran, zahrnující minimálně:

- a) možnost ověřit, že spoléhající se strana je registrována v národním registru spoléhajících se stran;
- b) možnost ověřit rozsah registrace spoléhající se strany (jaké údaje je spoléhající se strana oprávněna požadovat);
- c) dostupnost registračního certifikátu spoléhající se strany nebo ekvivalentního pověřujícího údaje;
- d) možnost ověřit kategorii spoléhající se strany (zejména soukromý subjekt, orgán veřejné moci, zdravotnické zařízení).

Poznámka k hodnocení: Tento požadavek se přímo váže na požadavky WUP-02 a WUP-05 v kapitole X.6.2.3 (jednotka peněženky ověřuje pověření spoléhající se strany vůči registru spoléhajících se stran).

VER-05 [Sec]: Ověřovací služba pro identitu spoléhající se strany musí poskytnout informace nezbytné pro jednotku peněženky k vyhodnocení, zda žádost spoléhající se strany o údaje vyhovuje vložené politice zpřístupnění PID nebo atestace, o kterou je žádáno.

Poznámka k hodnocení: Uživatel musí před udělením souhlasu vidět důvěryhodné informace o spoléhající se straně. Tento požadavek je propojen s požadavky WUP-01 (autentizace spoléhající se strany) a WUP-02 (zobrazení identity spoléhající se strany a požadovaných atributů) v kapitole X.6.2.3.

VER-06 [Sec]: Ověřovací služba musí implementovat mechanismy zajišťující aktuálnost a integritu informací o registraci spoléhajících se stran, zahrnující minimálně:

- a) včasné zohlednění změn stavu registrace spoléhající se strany (pozastavení, zneplatnění registrace);
- b) včasné zohlednění změn oprávnění spoléhající se strany (rozsah údajů, které smí požadovat);
- c) elektronickou pečeť nebo podpis chránící integritu všech zveřejňovaných informací;
- d) dokumentovaný časový rámec pro propagaci změn v registru spoléhajících se stran do informací poskytovaných ověřovací službou.

Poznámka k hodnocení: Integrita registru spoléhajících se stran je základem důvěry uživatele. Pokud útočník dokáže modifikovat registrační údaje spoléhající se strany, může způsobit, že jednotky peněženky budou zveřejňovat údaje neoprávněným stranám.

VER-07 [Sec]: Registr spoléhajících se stran používaný ověřovací službou musí implementovat:

- a) řízení přístupu zajišťující, že pouze oprávněný personál může upravovat registrační údaje spoléhajících se stran, na principu dvojité kontroly (dual control) pro přidávání, změny a mazání záznamů; b) auditní záznamy všech změn registračních údajů spoléhajících se stran s nepopíratelnou auditní stopou;
- c) mechanismus zálohování a obnovy registračních údajů spoléhajících se stran v souladu s plánem kontinuity činnosti dle požadavku BCM-04 v kapitole X.4.11;
- d) požadavky na dostupnost konzistentní s dohodou o úrovni služby ekosystému peněženky; e) opatření řízení privilegovaného přístupu (PAM) v souladu s požadavkem ACC-02 v kapitole X.4.4.

Poznámka k hodnocení: Registr spoléhajících se stran je kritickou infrastrukturou — jeho kompromitace by ovlivnila všechny transakce mezi jednotkami peněženky a spoléhajícími se stranami v celé České republice.

X.9.4 Společný mechanismus pro autentizaci spoléhajících se stran

VER-08 [Sec]: Ověřovací služba musí podporovat společný mechanismus pro identifikaci a autentizaci spoléhajících se stran, umožňující jednotkám peněženky autentizovat spoléhající se strany pomocí přístupových certifikátů vydaných poskytovatelem přístupových certifikátů spoléhajících se stran určeným členským státem.

Poznámka k hodnocení: Důvěryhodný řetězec přístupových certifikátů spoléhajících se stran je propojen s registrem spoléhajících se stran. Konkrétní určení poskytovatele přístupových certifikátů spoléhajících se stran v České republice je předmětem rozhodnutí vlastníka schématu.

VER-09 [Sec]: Proces vydávání přístupových certifikátů spoléhajících se stran musí před vydáním přístupového certifikátu ověřit stav registrace spoléhající se strany v národním registru spoléhajících se stran. Přístupové certifikáty spoléhajících se stran nesmí být vydány subjektům, které nejsou platně registrovány.

Poznámka k hodnocení: Tento požadavek vytváří závazné propojení mezi registrem spoléhajících se stran a vydáváním přístupových certifikátů spoléhajících se stran. Bez tohoto propojení by mohly být vydány přístupové certifikáty subjektům bez platné registrace, což by narušilo důvěryhodnost celého mechanismu autentizace.

X.9.5 Bezpečnostní požadavky na úroveň služby

VER-10 [Sec]: Provozovatel ověřovací služby musí implementovat všechny aplikovatelné požadavky z kapitol X.2 až X.5 této přílohy (řízení rizik, politiky a postupy, správa a provoz poskytovatele, ISMS procesy), přizpůsobené pro rozsah ověřovací služby.

Poznámka k hodnocení: Ověřovací služba zahrnuje jako komponenty: systém IKT, proces vývoje, proces řízení změn, proces řízení zranitelností, proces řízení incidentů a proces řízení podvodů. Požadavky na tyto komponenty jsou definovány v kapitolách X.4 a X.5 této přílohy.

VER-11 [Sec]: Ověřovací služba musí být navržena tak, aby se předcházelo jednotlivým bodům selhání, s mechanismy redundance a přepnutí (failover) zajišťujícími pokračující dostupnost v případě selhání komponenty.

Poznámka k hodnocení: Ověřovací služba je sdílenou závislostí celého ekosystému. Pokud se seznamy důvěryhodných entit nebo registr spoléhajících se stran stanou nedostupnými, jsou ovlivněny všechny prezentační transakce v ekosystému.

VER-12 [Sec, Cond]: Pokud provozovatel ověřovací služby současně poskytuje službu poskytovatele PID nebo jinou službu v rámci schématu EUDIW-CZ, infrastruktura ověřovací služby musí být logicky a provozně oddělena od ostatních infrastruktur tak, aby kompromitace jedné služby přímo neovlivnila druhou.

Poznámka k hodnocení: Tento požadavek je opatřením obrany do hloubky (defense-in-depth) — pokud je infrastruktura jedné služby kompromitována, ověřovací služba zůstane provozuschopná a důvěryhodná. Hodnotitel ověří oddělení formou inspekce architektury a opatření řízení přístupu.

VER-13 [Sec]: Ověřovací služba musí zveřejňovat informace, které poskytuje, ve formátu podporujícím automatizované zpracování jednotkami peněženky a spoléhajícími se stranami, v souladu s technickými specifikacemi definovanými prováděcími akty Komise.

VER-14 [Sec, Privacy]: Ověřovací služba musí v technicky proveditelném rozsahu implementovat mechanismy chránící soukromí, které zabrání provozovateli služby zjistit, které konkrétní jednotky peněženky nebo spoléhající se strany jsou v daném okamžiku ověřovány.

Poznámka k hodnocení: Ověřovací služba se nesmí stát bodem dohledu nad ekosystémem. Možné přístupy zahrnují cachování seznamů důvěryhodných entit jednotkami peněženky, dávková stahování (batch downloads) a diferenciální aktualizace.

X.10 Předpoklady provozního prostředí

Tato kapitola definuje požadavky na předpoklady o provozním prostředí, které poskytovatel služby EUDI musí definovat, ověřovat a udržovat pro komponenty řešení peněženky závisující na prostředích mimo přímou kontrolu poskytovatele.

Dvouúrovňový přístup CIR (EU) 2024/2981. Čl. 3 odst. 3 písm. b) ve spojení s čl. 8 odst. 3 písm. e) a f) rozlišuje dvě kategorie prostředí, na něž se uplatňují odlišné režimy zacházení:

a) **Prostředí dodávaná poskytovatelem služby EUDI**, včetně prostředí dodávaných třetími stranami smluvně najatými poskytovatelem (například poskytovatelem cloudových služeb, dodavatelem infrastruktury

hostující WSCD, dodavatelem služby pečetení PID). Pro tato prostředí poskytovatel služby EUDI musí poskytnout důkazy, že prostředí splňuje všechny předpoklady definované pro něj.

b) **Prostředí dodávané uživatelem peněženky**, zejména uživatelské zařízení (mobilní telefon, počítač). Pro tato prostředí poskytovatel služby EUDI musí:

- (1) definovat vhodné kontroly pro ověření předpokladů o prostředí;
- (2) potvrdit dostatečnost těchto kontrol;
- (3) ověřit účinnost těchto kontrol.

Oba režimy jsou pokryty v této kapitole.

X.10.1 Obecné požadavky na předpoklady prostředí

ENV-01 [Sec]: Poskytovatel služby EUDI musí definovat předpoklady o provozním prostředí používaném komponentami služby IKT, které umožní těmto komponentám splnit požadavky vztahující se na ně.

Poznámka k hodnocení: Předpoklady musí být explicitní, dokumentované a trasovatelné na požadavky, které podporují. Hodnotitel ověří úplnost dokumentace předpokladů a jejich propojení s požadavky kapitol X.4 až X.9.

ENV-02 [Sec]: Pokud je provozní prostředí dodáváno poskytovatelem služby IKT (včetně prostředí dodávaných třetími stranami smluvně najatými poskytovatelem), poskytovatel musí poskytnout důkazy, že prostředí splňuje všechny předpoklady definované pro něj.

Poznámka k hodnocení: Pojem „prostředí dodávané poskytovatelem“ zahrnuje prostředí poskytovaná třetími stranami smluvně najatými poskytovatelem (například poskytovatelem cloudových služeb nebo dodavatelem infrastruktury). Důkazy mohou zahrnovat existující certifikace dodavatele (zejména EN ISO/IEC 27001, SOC 2, EUCC), dohody o úrovni služby (SLA), auditní zprávy nebo výsledky inspekce na místě. Přijatelnost konkrétních forem důkazů je definována v příloze IX schématu.

ENV-03 [Sec]: Pokud je provozní prostředí dodáváno uživatelem peněženky, poskytovatel služby IKT musí:

- a) definovat vhodné kontroly k ověření předpokladů o prostředí;
- b) potvrdit dostatečnost těchto opatření;
- c) ověřit účinnost těchto opatření.

Poznámka k hodnocení: Tento třístupňový proces (definovat — potvrdit dostatečnost — ověřit účinnost) musí být prokazatelný certifikačnímu orgánu pro každý uplatněný předpoklad o uživatelském prostředí. Konkrétní předpoklady o uživatelském zařízení jsou specifikovány v kapitole X.10.2.

ENV-04 [Sec]: Pro každý předpoklad, který není podložen certifikátem shody nebo jinými přijatelnými informacemi o záruce, poskytovatel služby EUDI musí poskytnout:

- a) popis mechanismu používaného k prosazení předpokladu;
- b) odůvodnění, že tento mechanismus je dostatečný k zajištění ověření předpokladu.

Poznámka k hodnocení: Tento požadavek představuje dvojici „mechanismus + odůvodnění“. Pro každý nepodložený předpoklad certifikační orgán hodnotí jak samotný mechanismus, tak i odůvodnění jeho dostatečnosti.

X.10.2 Předpoklady o uživatelském zařízení

Mobilní zařízení uživatele (Android, iOS) je primárním provozním prostředím pro instanci peněženky v architekturním profilu schématu EUDIW-CZ. Poskytovatel peněženky toto prostředí přímo nekontroluje, ale musí definovat a prosazovat předpoklady o něm v souladu s požadavkem ENV-03.

ENV-UD-01 [Sec]: Poskytovatel peněženky musí definovat minimální požadavky na operační systém uživatelského zařízení, zahrnující minimálně:

- a) minimální verzi operačního systému (Android, iOS), která je aktuálně podporována výrobcem;
- b) dostupnost aktuálních bezpečnostních záplat operačního systému, s definovanou maximální tolerovanou prodlevou od vydání záplaty;
- c) přítomnost hardwarových bezpečnostních schopností uživatelského zařízení (například bezpečné enklávy, dostupnost prostředí důvěryhodného provádění TEE).

Poznámka k hodnocení: Tento požadavek navazuje na požadavek WIN-02 písm. a) v kapitole X.6.4.2 a na požadavek WPS-04 v kapitole X.7.1 (kontroly způsobilosti uživatelského zařízení). Hodnotitel ověří dokumentaci minimálních požadavků a mechanismus jejich prosazení během aktivace jednotky peněženky.

ENV-UD-02 [Sec]: Poskytovatel peněženky musí definovat předpoklad, že uživatelské zařízení nebylo neoprávněně upraveno (rooted, jailbroken) ani jinak modifikováno způsobem narušujícím bezpečnostní model operačního systému. Ověřovací mechanismus musí zahrnovat:

- a) kontroly integrity za běhu (například prostřednictvím Play Integrity API na Android, App Attest na iOS);
- b) kontroly známých indikátorů neoprávněných úprav (zejména přítomnost hookovacích frameworků, debuggerů, rooted/jailbreak nástrojů);
- c) periodické opětovné ověření po celou dobu životního cyklu jednotky peněženky.

Poznámka k hodnocení: Tento požadavek navazuje na požadavek WIN-02 písm. e) v kapitole X.6.4.2. Hodnotitel ověří implementaci ověřovacích mechanismů a jejich integraci do procesu monitorování dle požadavku WPS-08 v kapitole X.7.1.

ENV-UD-03 [Sec]: Poskytovatel peněženky musí definovat předpoklad, že uživatelské zařízení poskytuje adekvátní izolaci aplikací, brání ostatním aplikacím v přístupu k soukromým datům instance peněženky. Ověřovací mechanismus musí zahrnovat:

- a) ověření, že operační systém poskytuje izolaci na úrovni procesu (process-level isolation);
- b) ověření, že instance peněženky nezpřístupňuje data prostřednictvím nechráněných kanálů meziprocesové komunikace;
- c) ověření, že instance peněženky nezveřejňuje citlivá data prostřednictvím systémových mechanismů (zejména mezipaměti schránky, zálohovacích služeb operačního systému, sdílených souborových úložišť).

Poznámka k hodnocení: Tento předpoklad je jádrem bezpečnostního modelu instance peněženky. Hodnotitel ověří implementaci izolačních mechanismů formou inspekce a testování, v souladu s požadavkem WIN-01 v kapitole X.6.4.1.

ENV-UD-04 [Sec]: Poskytovatel peněženky musí definovat předpoklad, že uživatelské zařízení má aktivní mechanismus zámku obrazovky s adekvátní bezpečností. Ověřovací mechanismus musí zahrnovat:

- a) kontrolu konfigurace zámku obrazovky během aktivace jednotky peněženky;
- b) doporučení uživateli, pokud politika zámku obrazovky nesplňuje minimální požadavky;
- c) vynucení časového limitu pro opětovnou autentizaci v souladu s časovým limitem zámku obrazovky.

ENV-UD-05 [Sec]: Poskytovatel peněženky musí definovat chování jednotky peněženky v situacích, kdy jeden nebo více předpokladů o uživatelském zařízení nejsou splněny, zahrnující minimálně:

- a) zamítnutí aktivace jednotky peněženky, pokud nejsou splněny kritické předpoklady;
- b) pozastavení operací jednotky peněženky, pokud předpoklady přestanou být splněny během životního cyklu;
- c) oznámení uživateli s jasným vysvětlením problému a popisem požadované nápravy;
- d) zaznamenání nesplnění předpokladu v auditní stopě jednotky peněženky pro účely následného přezkumu.

Poznámka k hodnocení: Hodnotitel ověří definované chování jednotky peněženky formou testování scénářů, kdy jednotlivé předpoklady nejsou splněny (například verze operačního systému pod minimální požadovanou hranicí, detekce neoprávněné úpravy zařízení v průběhu provozu). Tento požadavek je propojen s požadavkem WPS-04 v kapitole X.7.1 a požadavkem WIN-02 písm. k) v kapitole X.6.4.2.

X.10.3 Předpoklady o infrastruktuře dodávané poskytovatelem

V architekturním profilu schématu EUDIW-CZ poskytovatel peněženky využívá několik infrastrukturních komponent dodávaných smluvními třetími stranami a externími službami. Pro tato prostředí musí poskytovatel poskytnout důkazy o souladu s předpoklady, nikoli pouze definovat ověřovací mechanismy.

ENV-INF-01 [Sec]: Poskytovatel služby EUDI musí definovat a prokázat platnost předpokladů na infrastrukturu hostující vzdálený WSCD a službu jednotky peněženky, zahrnující minimálně:

- a) fyzickou bezpečnost datového centra (perimetr, řízení přístupu, environmentální kontroly), v souladu s požadavkem PHY-03 v kapitole X.4.6;
- b) síťovou bezpečnost (segmentace, ochrana proti útokům odepření služby, redundantní konektivita);
- c) dostupnost (dohoda o úrovni služby s definovaným uptime, RTO a RPO), v souladu s požadavkem BCM-04 v kapitole X.4.11;
- d) logickou izolaci tenanta služby EUDI od ostatních tenantů sdílené infrastruktury.

Důkazy mohou zahrnovat: bezpečnostní certifikace dodavatele infrastruktury (zejména EN ISO/IEC 27001, SOC 2), dohody o úrovni služby, auditní zprávy nebo výsledky inspekce na místě dle kritérií přijatelnosti přílohy IX schématu.

ENV-INF-02 [Sec]: Poskytovatel služby EUDI musí definovat a prokázat platnost předpokladů na infrastrukturu poskytovatele prostředku elektronické identifikace použitého pro onboarding uživatelů, zahrnující minimálně:

- a) sílu autentizace poskytovanou prostředkem na deklarované úrovni záruky;
- b) integritu identifikačních údajů přijatých od poskytovatele prostředku;
- c) dostupnost služby poskytovatele prostředku během očekávaných špiček zatížení.

Důkazy mohou zahrnovat: stav notifikace prostředku elektronické identifikace dle čl. 9 eIDAS, výsledky testů interoperability, dohody o úrovni služby s provozovatelem prostředku.

Poznámka k hodnocení: Prostředek elektronické identifikace není smluvně najat poskytovatelem služby EUDI, ale je národní infrastrukturou poskytovanou členským státem. Model předpokladů se proto liší od ostatních dodavatelů — poskytovatel služby EUDI definuje předpoklady a ověřovací mechanismy, ale může spoléhat na notifikační status prostředku elektronické identifikace jako na informaci o záruce.

ENV-INF-03 [Sec]: Poskytovatel služby EUDI musí definovat a prokázat platnost předpokladů na službu pečeti PID použitou pro elektronické pečeti PID, zahrnující minimálně:

- a) platnost a rozsah certifikace poskytovatele pečetí služby jako kvalifikovaného poskytovatele služeb vytvářejících důvěru (QTSP);
- b) bezpečnost správy pečetího klíče;
- c) dostupnost pečetí služby během vydávání PID.

Důkazem je existující zpráva o posouzení shody poskytovatele pečetí služby jako QTSP, podléhající kritériím přijatelnosti definovaným v příloze IX schématu (kapitola IX.6.7).

Poznámka k hodnocení: Existující QTSP certifikace poskytovatele pečetící služby je opětovně použitelná prostřednictvím analýzy závislosti dle přílohy IX schématu. Rozsah certifikace musí specificky pokrývat pečetění PID v ekosystému EUDIW.

ENV-INF-04 [Sec]: Poskytovatel služby EUDI musí definovat a prokázat platnost předpokladů na hardware WSCD (zejména hardware HSM v architektuře se vzdáleným WSCD), zahrnující minimálně:

- a) úroveň a rozsah certifikace WSCD dle EUCC nebo Common Criteria, v souladu s požadavkem WSCD-01 v kapitole X.6.6;
- b) soulad certifikované konfigurace WSCD s konfigurací nasazení v provozním prostředí;
- c) soulad s pokyny dodavatele pro bezpečnou administraci WSCD.

Důkazem je certifikát EUCC nebo Common Criteria dodavatele WSCD, související bezpečnostní cíl (security target) a certifikační zpráva, podléhající kritériím přijatelnosti přílohy IX schématu (kapitola IX.6.1).

Poznámka k hodnocení: Tento požadavek je požadavkem na kompozici (composition) — poskytovatel služby EUDI musí prokázat, že nasazený WSCD odpovídá certifikovanému produktu a je provozován v certifikované konfiguraci.

ENV-INF-05 [Sec]: Poskytovatel služby EUDI musí definovat a prokázat platnost předpokladů na autoritativní zdroj identitních údajů použitý pro validaci PID dle požadavku PIDR-09 v kapitole X.8.1, zahrnující minimálně:

- a) autoritativní status zdroje pro identifikaci fyzických osob v České republice dle právních předpisů;
- b) integritu a dostupnost rozhraní zdroje pro účely validace identitních údajů;
- c) postupy detekce změn v autoritativním zdroji a propagace těchto změn do procesu správy PID dle požadavku PIDM-03 v kapitole X.8.2.

Poznámka k hodnocení: Autoritativním zdrojem se rozumí registr veřejné správy stanovený právními předpisy České republiky pro účely identifikace fyzických osob (zejména registr obyvatel dle zákona č. 111/2009 Sb.). Předpoklady o autoritativním zdroji vycházejí z právního statusu zdroje a z technických parametrů jeho rozhraní.

X.10.4 Předpoklady prostředí WSCD

ENV-WSCD-01 [Sec]: Pokud se WSCA spoléhá na WSCD, který není zahrnut jako komponenta služby IKT (například lokální externí WSCD typu čipové karty), poskytovatel služby IKT musí definovat předpoklady o tomto WSCD, které jsou dostatečné pro to, aby WSCA splnila všechny aplikovatelné požadavky, a platnost těchto předpokladů musí být prokázána.

Poznámka k hodnocení: Schéma nedefinuje přímé požadavky na lokální externí WSCD, ale omezuje WSCD prostřednictvím potřeb WSCA (kompoziční model). Hodnotitel ověří, že předpoklady o WSCD pokrývají

všechny vlastnosti vyžadované WSCA, a že platnost předpokladů je doložena certifikací WSCD nebo jinými přijatelnými informacemi o záruce.

ENV-WSCD-02 [Sec, Cond]: V architektuře se vzdáleným WSCD je WSCD zahrnut jako komponenta služby IKT dodávaná poskytovatelem služby EUDI. Předpoklady o vzdáleném WSCD jsou pokryty požadavky ENV-INF-01 a ENV-INF-04 v kapitole X.10.3. Požadavky na samotný WSCD jsou definovány v kapitole X.6.6 (WSCD-01 až WSCD-03).

Poznámka k hodnocení: V architektuře se vzdáleným WSCD není WSCD externím předpokladem, ale komponentou dodávanou poskytovatelem se všemi důkazními povinnostmi dle požadavku ENV-02. Požadavek ENV-WSCD-01 se uplatní pouze pro scénář s lokálním externím WSCD.

ENV-WSCD-03 [Sec, Cond]: Pro architekturu s lokálním externím WSCD (například čipová karta pro offline scénáře) musí poskytovatel služby EUDI definovat předpoklady zahrnující minimálně:

- a) úroveň certifikace WSCD dle EUCC nebo Common Criteria;
- b) podporu WSCD pro požadované kryptografické operace (v souladu s požadavkem CRY-02 v kapitole X.4.5);
- c) bezpečný proces dodání WSCD uživateli a jeho aktivace;
- d) odolnost vůči fyzickým útokům na požadované úrovni AVA_VAN.

Poznámka k hodnocení: Architektura s lokálním externím WSCD je v profilu schématu EUDIW-CZ plánována pro budoucí fáze rozvoje. V okamžiku jejího nasazení musí poskytovatel služby EUDI prokázat vhodnost WSCD prostřednictvím analýzy závislostí vůči předpokladům WSCA Protection Profile.

X.10.5 Posouzení definovaných předpokladů

Pro účely posuzování shody s požadavky kapitoly X.10 certifikační orgán:

- a) ověří, že poskytovatel služby EUDI definoval explicitní předpoklady pro všechna provozní prostředí, která nejsou pod jeho přímou kontrolou (uživatelská zařízení, infrastruktura dodavatelů, externí služby), a že tyto předpoklady jsou trasovatelné na požadavky, které podporují;
- b) pro prostředí dodávaná poskytovatelem (požadavky ENV-INF-01 až ENV-INF-05): posoudí důkazy, že prostředí splňuje předpoklady; toto zahrnuje přezkum certifikací, dohod o úrovni služby, auditních zpráv a v případě potřeby i provedení inspekce na místě;
- c) pro prostředí dodávaná uživatelem (požadavky ENV-UD-01 až ENV-UD-04): posoudí třístupňový proces — vhodnost definovaných opatření, potvrzení jejich dostatečnosti a ověření jejich účinnosti formou testování;
- d) pro každý nepodložený předpoklad (požadavek ENV-04): posoudí jak prosazovací mechanismus, tak i odůvodnění jeho dostatečnosti;

- e) ověří chování jednotky peněženky v situacích, kdy předpoklady nejsou splněny (požadavek ENV-UD-05): testováním ověří zamítnutí aktivace, pozastavení operací a oznámení uživateli;
- f) ověří kompoziční model pro WSCD: pro architekturu se vzdáleným WSCD ověří, že nasazená konfigurace odpovídá certifikované konfiguraci (požadavek ENV-INF-04); pro architekturu s lokálním externím WSCD ověří analýzu závislostí (požadavky ENV-WSCD-01 a ENV-WSCD-03);
- g) v rámci ročních dozorových hodnocení ověří, že předpoklady zůstávají platné s ohledem na změny v prostředí hrozeb, aktualizace operačních systémů uživatelských zařízení a změny v infrastrukturách dodavatelů; ověří, že ověřovací mechanismy zůstávají účinné;
- h) zohlední, že CIR (EU) 2024/2981 příloha IV oddíl 4 definuje specifické hodnotící činnosti pro koncová uživatelská zařízení; tyto činnosti musí být zahrnuty do plánu hodnocení (Evaluation Plan) dle přílohy XI schématu.

Příloha X.A — Rozšíření registru rizik schématu EUDIW-CZ

Tato příloha obsahuje:

- a) Architekturně specifická rizika CZ-01 až CZ-10, která doplňují registr rizik v příloze I CIR (EU) 2024/2981 a vycházejí z architekturního profilu schématu EUDIW-CZ definovaného v příloze I schématu;
- b) Souhrn analýzy pokrytí TR1 až TR133 (prohlášení o aplikovatelnosti) zaznamenávající, jak schéma EUDIW-CZ pokrývá hrozby identifikované v registru rizik EU.

Vztah k registru rizik EU. Rizika CZ-01 až CZ-10 jsou rozšířením, nikoli náhradou registru rizik v příloze I CIR (EU) 2024/2981. Poskytovatel služby EUDI musí v rámci svého posouzení rizik specifického pro implementaci (dle požadavků RMF-02 a RMF-07 v kapitole X.2) adresovat jak rizika z registru EU (TR1 až TR133), tak rizika CZ-01 až CZ-10 z této přílohy.

Vztah k vrstvenému modelu rizik dle ENISA Guidance. Rizika CZ-01 až CZ-10 představují druhou vrstvu vrstveného modelu rizik — rizika zavedená národním certifikačním schématem a specifickou architekturou peněženky. První vrstvu představují rizika v registru rizik EU, třetí vrstvu představují rizika identifikovaná samotným poskytovatelem služby EUDI v rámci jeho posouzení rizik specifického pro implementaci.

X.A.1 Architekturně specifická rizika

Následující rizika byla identifikována jako specifická pro architekturní profil schématu EUDIW-CZ definovaný v příloze I schématu. Pro každé riziko je uveden jeho dopad, cílová komponenta, úroveň rizika, opatření k jeho zmírnění a odůvodnění zařazení do registru rizik schématu.

CZ-01: Kompromitace centralizovaného WSCD

V architektuře se vzdáleným WSCD obsluhuje jeden WSCD (provozovaný ve formě HSM) kryptografická aktiva všech aktivních jednotek peněženky. Útočník, který získá přístup k tomuto centrálnímu úložišti

kryptografického klíčového materiálu, by mohl kompromitovat identitu všech uživatelů služby EUDI současně.

Související rizika EU / hrozby	SR1, R4, R5, R9; TR53, TR58, TR59, TR81, TR118, TR119, TR122, TR123, TR125, TR126
Cílová komponenta	WSCD (vzdálený HSM)
Úroveň rizika	Vysoká
Opatření ke zmírnění	ACC-02 (rozšířená opatření řízení přístupu k WSCD); CRY-04 (certifikace WSCD na úrovni EAL4 + AVA_VAN.5); PHY-03 (fyzická bezpečnost datového centra hostujícího WSCD); NET-02 (end-to-end ochrana komunikačního kanálu instance ↔ WSCD); WSCD-02 (multi-tenancy izolace); WSCD-03 (redundance a obnova WSCD); BCM-04 (kontinuita kritických komponent); ENV-INF-01 (důkazy o infrastruktuře hostující WSCD); ENV-INF-04 (certifikace hardwaru WSCD)
Odůvodnění	Architektura se vzdáleným WSCD soustředí kryptografická aktiva všech uživatelů do jediného fyzického umístění. To představuje architektonicky vynucený jediný bod selhání s maximálním dopadem. Zmírnění je realizováno obranou do hloubky: certifikace EUCC, fyzická bezpečnost datového centra, řízení přístupu na principu dvojité kontroly, síťová segmentace a kontinuální monitorování.

CZ-02: Výpadek konektivity mezi instancí peněženky a vzdáleným WSCD

Architektura se vzdáleným WSCD vyžaduje pro provádění kritických kryptografických operací aktivní síťové připojení mezi instancí peněženky na uživatelském zařízení a WSCD ve vzdáleném datovém centru. Výpadek konektivity (na straně sítě, na straně uživatele nebo na straně WSCD) způsobí dočasnou nedostupnost služby pro postižené jednotky peněženky.

Související rizika EU / hrozby	R13; TR65, TR80, TR81
Cílová komponenta	Komunikační kanál instance peněženky - WSCD
Úroveň rizika	Vysoká
Opatření ke zmírnění	BCM-04 (kontinuita činnosti, RTO/RPO pro WSCD); NET-02 (redundance síťových kanálů); WSCD-03 (geografická redundance WSCD); WUM-05 (chování jednotky peněženky při nedostupnosti vzdáleného WSCD); ENV-INF-01 (SLA s dodavatelem infrastruktury); VER-03 (dostupnost ověřovací služby)
Odůvodnění	Vzdálený WSCD vyžaduje online připojení pro všechny kritické kryptografické operace. V profilu schématu EUDIW-CZ není v první fázi k dispozici off-line alternativa formou lokálního externího WSCD. Zmírnění je realizováno prostřednictvím redundance, definovaných cílových dob obnovy a řízení chování jednotky peněženky při výpadku.

CZ-03: Kompromitace prostředku elektronické identifikace během onboardingu

Onboarding uživatele do služby EUDI v profilu schématu EUDIW-CZ se opírá o prostředek elektronické identifikace na úrovni záruky „vysoká“. Kompromitace tohoto prostředku (ať už kompromitací jeho

infrastruktury, nebo zneužitím konkrétního identifikačního kreditu) by umožnila útočnickovi obejít ověření identity a aktivovat jednotku peněženky pod cizí identitou.

Související rizika EU / hrozby	R1, R2; TR5, TR7, TR11
Cílová komponenta	Onboarding uživatele
Úroveň rizika	Vysoká
Opatření ke zmírnění	ONB-02 (specifické kontroly: vazba relace, ochrana proti opakovanému přehraní, detekce živosti, časové limity); ONB-03 (monitorování podvodů během onboarding); PIDR-02 (ověření identity na úrovni záruky „vysoká“); PIDR-09 (validace vůči autoritativnímu zdroji identitních údajů); PIDR-11 (anti-podvodné monitorování během vydávání PID); ENV-INF-02 (předpoklady o infrastruktuře poskytovatele prostředku); FRD-P03 písm. a) (scénář podvodu při onboarding)
Odůvodnění	Prostředek elektronické identifikace je sdílenou národní infrastrukturou, kterou poskytovatel služby EUDI přímo nekontroluje. Zmírnění je realizováno prostřednictvím dodatečných kontrol na straně poskytovatele peněženky a poskytovatele PID a prostřednictvím sekundárního ověření vůči autoritativnímu zdroji identitních údajů.

CZ-04: Kompromitace externí služby pečetení PID

V profilu schématu EUDIW-CZ je elektronické pečetení PID svěřeno externímu poskytovateli kvalifikované pečeticí služby. Kompromitace tohoto poskytovatele nebo jeho pečeticího klíče by umožnila útočnickovi vydávat falešně pečetená PID, která by jednotky peněženky a spoléhající se strany akceptovaly jako pravá.

Související rizika EU / hrozby	R3, R7; TR18, TR23
Cílová komponenta	Služba pečetení PID
Úroveň rizika	Vysoká
Opatření ke zmírnění	PIDR-10 (ověření integrity pečeti před uvolněním PID); SUP-06 (posouzení bezpečnostního stavu poskytovatele pečeticí služby); SUP-07 (úschova kódu); ENV-INF-03 (předpoklady o pečeticí službě s opětovným použitím existující QTSP certifikace); příloha IX schématu (kapitola IX.6.7, kritéria přijatelnosti QTSP certifikace)
Odůvodnění	Poskytovatel pečeticí služby je již kvalifikovaným poskytovatelem služeb vytvářejících důvěru — jeho stávající certifikace pokrývá obecné operace pečetení. Specifické použití pro pečetení PID v ekosystému EUDIW musí být explicitně v rozsahu QTSP certifikace, což je ověřeno prostřednictvím analýzy závislostí dle přílohy IX.

CZ-05: Hrozba zevnitř u poskytovatele peněženky a jeho subdodavatelů

Personál poskytovatele peněženky a jeho subdodavatelů má z povahy svých rolí privilegovaný přístup k produkčnímu zdrojovému kódu, ke konfiguraci WSCA, k administrativním rozhraním WSCD a k infrastruktuře hostující službu jednotky peněženky. Zneužití tohoto privilegovaného přístupu škodlivým insiderem by umožnilo přímou kompromitaci jednotek peněženky uživatelů.

Související rizika EU / hrozby	TR115, TR129, TR130
Cílová komponenta	Instance peněženky, WSCA, služba jednotky peněženky
Úroveň rizika	Vysoká
Opatření ke zmírnění	HR-02 (rozšířené prověrky personálu s privilegovaným přístupem); DEV-03 (oddělení vývojového, testovacího a produkčního prostředí); DEV-04 (důkazy o bezpečném vývoji); DEV-05 (požadavky na vývojový proces u subdodavatelů); WUG-05 (omezení přístupu poskytovatele peněženky k obsahu jednotky peněženky); WUS-01 a WUS-02 (oddělení služby jednotky peněženky od administrativní infrastruktury); ORG-02 (efektivní provoz ISMS); ACC-02 (řízení privilegovaného přístupu); FRD-P03 písm. c) (scénář podvodu zevnitř)
Odůvodnění	Personál poskytovatele peněženky a subdodavatelů má z povahy role privilegovaný přístup ke kritickým komponentám. Zmírnění je realizováno prostřednictvím rozšířených proverek personálu, oddělení prostředí, návrhu „nulové znalosti“ (zero-knowledge) na straně poskytovatele peněženky a kontinuálního monitorování.

CZ-06: Kaskádová kompromitace sdílené infrastruktury

V profilu schématu EUDIW-CZ je vícero komponent služby EUDI hostováno na společné infrastruktuře dodávané jediným dodavatelem (zejména WSCD a služba jednotky peněženky). Kompromitace této společné infrastruktury by měla kaskádový dopad na vícero komponent ekosystému současně.

Související rizika EU / hrozby	R13; SR2; TR65, TR80
Cílová komponenta	Sdílená infrastruktura kritických komponent
Úroveň rizika	Vysoká
Opatření ke zmírnění	PHY-03 (fyzická bezpečnost datového centra); NET-03 (segmentace administrativní sítě); ACC-02 (rozšířená opatření řízení přístupu); ENV-INF-01 (důkazy o infrastruktuře dodavatele: fyzická bezpečnost, síťová bezpečnost, dostupnost, izolace tenantů); SUP-06 (posouzení bezpečnostního stavu dodavatele infrastruktury); VER-12 (oddělení infrastruktury ověřovací služby od ostatních infrastruktur)
Odůvodnění	Společná infrastruktura hostuje vícero komponent služby EUDI — kompromitace má potenciálně kaskádový efekt. Zmírnění je realizováno prostřednictvím izolace tenantů, segmentace, nezávislého doložení bezpečnostního stavu dodavatele a oddělení infrastruktury ověřovací služby od ostatních.

CZ-07: Nedostatečné oddělení prostředí u subdodavatele vývoje systému poskytovatele PID

V profilu schématu EUDIW-CZ je systém poskytovatele PID vyvíjen externím subdodavatelem. Nedostatečné oddělení vývojového, testovacího a produkčního prostředí u subdodavatele by umožnilo neoprávněný přenos dat mezi prostředími nebo zavedení škodlivého kódu do produkčního systému.

Související rizika EU /	R5, R6; TR115
--------------------------------	---------------

hrozby	
Cílová komponenta	Systém poskytovatele PID
Úroveň rizika	Střední
Opatření ke zmírnění	DEV-03 (oddělení vývojového, testovacího a produkčního prostředí); DEV-05 (soulad vývoje u subdodavatele s požadavky DEV-01 až DEV-04); SUP-04 (požadavky na třetí strany); SUP-06 (posouzení bezpečnostního stavu subdodavatele); SUP-07 (úschova kódu)
Odůvodnění	Subdodavatelský vývoj systému poskytovatele PID je řízen prostřednictvím standardních požadavků dodavatelského řetězce a požadavků na bezpečný vývoj. Riziko je klasifikováno jako střední, protože je adresováno standardními kontrolními mechanismy bez nutnosti specifických architektonických opatření.

CZ-08: Ztráta nebo krádež uživatelského zařízení

Ztráta nebo krádež uživatelského zařízení je reálnou a častou událostí. V architektuře se vzdáleným WSCD nejsou kryptografické klíče uloženy na uživatelském zařízení (snížení rizika krádeže klíčů), avšak proces obnovy jednotky peněženky na novém zařízení nesmí vytvořit příležitost pro krádež identity uživatele útočníkem, který získal přístup ke ztracenému zařízení.

Související rizika EU / hrozby	R4, R8; TR48, TR60
Cílová komponenta	Instance peněženky a WSCD
Úroveň rizika	Vysoká
Opatření ke zmírnění	WPS-05 (uživatelský účet s nezávislou autentizační metodou); WPS-09 (proces obnovy jednotky peněženky); REV-02 (revokace na žádost uživatele); REV-05 (notifikace nezávislým kanálem ve lhůtě 24 hodin); BCM-04 písm. c) (postupy obnovy jednotky peněženky); WUM-03 (bezpečné zničení kryptografického klíčového materiálu)
Odůvodnění	Ztráta nebo krádež zařízení je reálná a častá událost. Architektura se vzdáleným WSCD eliminuje krádež klíčů z fyzického zařízení, ale proces obnovy musí zajistit, že útočník se ztraceným zařízením nemůže získat kontrolu nad jednotkou peněženky uživatele. Nezávislá autentizační metoda registrovaná během aktivace je primární ochranou.

CZ-09: Útok na registr spoléhajících se stran

Registr spoléhajících se stran provozovaný v rámci ekosystému EUDIW je centrálním zdrojem informací o oprávněnosti spoléhajících se stran k požadování konkrétních atributů. Kompromitace registru (modifikace registračních údajů spoléhající se strany, vložení falešné spoléhající se strany) by umožnila útočníkovi cílit na uživatele s podvodnými žádostmi o údaje.

Související rizika EU / hrozby	TR74, TR102; R9
Cílová komponenta	Registr spoléhajících se stran
Úroveň rizika	Vysoká
Opatření ke zmírnění	VER-04 (ověření identity spoléhající se strany);

	VER-06 (integrita zveřejňovaných informací); VER-07 (řízení přístupu k registru, dvojité kontrola, auditní záznamy); VER-09 (vázanost vydávání přístupového certifikátu na registraci); WUP-05 a WUP-06 (jednotka peněženky ověřuje pověření spoléhající se strany vůči registru); FRD-P03 písm. d) (sociální inženýrství cílící na uživatele přes falešné spoléhající se strany)
Odůvodnění	Kompromitace registru spoléhajících se stran by ovlivnila všechny transakce mezi jednotkami peněženky a spoléhajícími se stranami v celé České republice. Registr představuje kritickou národní infrastrukturu vyžadující dvojitou kontrolu, auditní záznamy a robustní mechanismy zálohování a obnovy.

CZ-10: Kumulace rolí u jednoho subjektu ekosystému

V profilu schématu EUDIW-CZ jeden subjekt v ekosystému současně zastává více rolí — zejména role vlastníka schématu, orgánu dohledu, poskytovatele PID a registrátora spoléhajících se stran. Tato kumulace rolí vytváří potenciální střety zájmů mezi rolí regulovanou (poskytovatel PID) a rolí dohledovou (orgán dohledu) a riziko, že jedna kompromitovaná role ovlivní funkce ostatních rolí téhož subjektu.

Související rizika EU / hrozby	SR3
Cílová komponenta	Governance ekosystému
Úroveň rizika	Střední
Opatření ke zmírnění	ORG-05 (oddělení povinností u subjektu zastávajícího více rolí); VER-12 (oddělení infrastruktury ověřovací služby od ostatních infrastruktur); PIDR-R06 (nezávislost křížové kontroly mezi poskytovatelem PID a poskytovatelem peněženky); Sekce 4 hlavního textu schématu (Orgány posuzování shody - řešení střetu zájmů u certifikačního orgánu)
Odůvodnění	Kumulace rolí u jednoho subjektu vytváří potenciální střety zájmů. Zmírnění je realizováno prostřednictvím organizačního oddělení funkcí, dokumentovaných opatření řízení rizik střetu zájmů a nezávislého dohledu certifikačního orgánu. Uplatní se požadavky EN ISO/IEC 17065 na nestrannost.

X.A.2 Metodologický rámec pokrytí registru rizik

Tato kapitola definuje metodologický rámec, podle něhož je v rámci certifikace podle schématu EUDIW-CZ posuzováno pokrytí hrozeb z registru rizik (TR1 až TR133 z přílohy I CIR (EU) 2024/2981 a CZ-01 až CZ-10 z této přílohy X.A) bezpečnostními požadavky a dalšími prostředky kontroly.

Úplné prohlášení o aplikovatelnosti ve formě tabulky pokrývající každou jednotlivou hrozbu TR1 až TR133 a každé riziko CZ-01 až CZ-10 je udržováno jako doprovodný pracovní sešit schématu, nikoli jako součást tohoto normativního textu schématu. Tento sešit:

a) je udržován vlastníkem schématu jako referenční materiál pro certifikační orgány;

b) je aktualizován v reakci na změny v registru rizik EU, na nová zjištění z dozorových hodnocení a na změny v architektonickém profilu schématu;

c) je sdílen v rámci ENISA AHWG a EU Cooperation Group jako podpůrný dokument prokazující pokrytí registru rizik schématem.

Tento dělený přístup (normativní rámec ve schématu + udržovaná pracovní tabulka v doprovodném sešitu) odpovídá rozdělení odpovědností mezi vlastníkem schématu a žadatelem o certifikaci dle CIR (EU) 2024/2981, kdy úplné posouzení rizik specifické pro implementaci je deliverable žadatele dle čl. 4 odst. 4 písm. d) tohoto nařízení.

X.A.2.1 Kategorie pokrytí

Každá hrozba z registru rizik (TR1 až TR133 i CZ-01 až CZ-10) je v rámci schématu klasifikována jednou ze čtyř kategorií pokrytí. Tato klasifikace určuje, jakým způsobem je hrozba adresována a jaké metody hodnocení se uplatní.

Kategorie pokrytí	Popis	Způsob doložení
Opatření (Control)	Hrozba je pokryta jedním nebo více bezpečnostními požadavky definovanými v této příloze X. Konkrétní mapování na požadavky je uvedeno v příloze X.B.	Hodnocení relevantních požadavků certifikačním orgánem podle metod definovaných v příloze XI schématu (audit, inspekce, testování).
Certifikát (Certificate)	Hrozba je pokryta certifikátem třetí strany pro relevantní komponentu (zejména EUCC nebo Common Criteria certifikátem WSCD, FitCEM certifikátem instance peněženky), opětovně použitým prostřednictvím analýzy závislostí.	Posouzení existujícího certifikátu certifikačním orgánem podle kritérií přijatelnosti přílohy IX schématu.
Předpoklad (Assumption)	Hrozba je pokryta předpokladem o provozním prostředí, doplněným ověřovacím mechanismem definovaným v kapitole X.10.	Posouzení definovaných předpokladů, jejich dostatečnosti a účinnosti ověřovacích mechanismů certifikačním orgánem podle kapitoly X.10.5.
Neaplikovatelná (N/A)	Hrozba není aplikovatelná pro architektonický profil schématu EUDIW-CZ definovaný v příloze I schématu.	Odůvodnění neaplikovatelnosti vlastníkem schématu, validované certifikačním orgánem v rámci hodnocení žadatele.

Hrozba může být pokryta kombinací více kategorií (například kritická hrozba spojená s WSCD typicky kombinuje kategorii Certifikát pro samotný hardware a Opatření pro provozní řízení a izolaci).

X.A.2.2 Souhrn pokrytí (informativní)

Následující souhrn poskytuje orientační kvantitativní pohled na strukturu pokrytí hrozeb z registru rizik EU schématem EUDIW-CZ.

Kategorie pokrytí	Přibližný podíl hrozeb	Poznámka
Opatření	121 ze 133 (~91 %)	Většina hrozeb je primárně řešena bezpečnostními požadavky kapitol X.2 až X.10.
Certifikát	7 ze 133 (~5 %)	Týká se zejména hrozeb spojených s WSCD a kryptografickými komponentami, kde se opírá o existující EUCC/CC certifikace.
Předpoklad	5 ze 133 (~4 %)	Týká se zejména hrozeb spojených s uživatelským zařízením, které je mimo přímou kontrolu poskytovatele služby EUDI.
Neaplikovatelná	0 ze 133 (0 %)	V aktuální verzi schématu nebyla žádná hrozba registru rizik EU klasifikována jako neaplikovatelná.

Poznámka: Procentuální údaje jsou zaokrouhlené a odpovídají snímku stavu pokrytí v okamžiku zveřejnění této verze schématu. Aktuální distribuce může být ovlivněna probíhajícími změnami v registru rizik EU dle revizí přílohy I CIR (EU) 2024/2981 a vývojem schématu.

X.A.2.3 Údržba prohlášení o aplikovatelnosti

Doprovodný pracovní sešit schématu je živým dokumentem schématu, který vlastník schématu aktualizuje zejména v následujících situacích:

- finalizace nebo aktualizace kandidátského návrhu schématu ENISA a souvisejících standardů na úrovni EU;
- změny v registru rizik EU dle revizí přílohy I CIR (EU) 2024/2981 nebo dle výstupů governance procesu udržování registru rizik na úrovni EU Cooperation Group;
- identifikace nových rizik na úrovni schématu prostřednictvím ročního přezkumu (RMF-08 v kapitole X.2);
- změny v architektonickém profilu schématu EUDIW-CZ (zejména přidání lokálního externího WSCD nebo dalších architektonických variant);
- nová zjištění z dozorových hodnocení certifikovaných subjektů, která vedou k identifikaci nových hrozeb nebo ke změně klasifikace stávajících hrozeb;

f) nálezy z peer review schématu na úrovni EU Cooperation Group.

Žadatel o certifikaci ve své dokumentaci posouzení rizik musí vycházet z registru rizik dle přílohy I CIR (EU) 2024/2981, z architekturně specifických rizik CZ-01 až CZ-10 dle kapitoly X.A.1 a z matice trasovatelnosti v kapitole X.B (v souladu s požadavkem RMF-02) a doplnit je o:

- a) posouzení relevance jednotlivých hrozeb pro konkrétní implementaci poskytovatele služby EUDI;
- b) implementační rizika specifická pro konkrétního poskytovatele dle požadavku RMF-07 v kapitole X.2;
- c) mapování opatření poskytovatele na hrozby s vyhodnocením zbytkových rizik;
- d) odůvodnění úplnosti a dostatečnosti pokrytí.

Toto rozdělení odpovědností odpovídá vrstvenému modelu posouzení rizik (rozlišení mezi vrstvou registru rizik EU, vrstvou rizik schématu a vrstvou rizik specifických pro implementaci poskytovatele).

Příloha X.B — Mapování požadavků na registr rizik

Tato příloha poskytuje matici trasovatelnosti mezi bezpečnostními požadavky definovanými v příloze X a hrozbami z registru rizik (TR1 až TR133 z přílohy I CIR (EU) 2024/2981 a CZ-01 až CZ-10 z přílohy X.A schématu EUDIW-CZ), čímž prokazuje pokrytí rizik požadované článkem 3 odst. 5 písm. f) CIR (EU) 2024/2981.

Struktura matice

Každý řádek představuje jeden požadavek z přílohy X. Sloupce uvádějí identifikátor požadavku, podkapitolu přílohy X, pokryté hrozby (TR a/nebo CZ), cílovou komponentu a metodu hodnocení.

Legenda metod hodnocení

- A = Audit (přezkum dokumentace a politik);
- I = Inspekce (ověření implementace);
- T = Testování (funkční a bezpečnostní testy);
- C = Certifikát (opětovné použití existujícího certifikátu prostřednictvím analýzy závislostí dle přílohy IX).

X.B.1 Matice trasovatelnosti

ID požadavku	Podkapitola	Pokryté hrozby (TR / CZ)	Cílová komponenta	Metoda
X.2 Rámec řízení rizik				
GEN-5-01	X.2.1	Všechny TR (rámec)	Všichni poskytovatelé	A
GEN-5-02	X.2.1	Všechny TR (vstup registru rizik)	Všichni poskytovatelé	A
RMF-01	X.2.2	Všechny TR	Všichni poskytovatelé	A
RMF-02	X.2.2	TR1 až TR133, CZ-01 až CZ-10	Všichni poskytovatelé	A

RMF-03	X.2.2	TR1 až TR133, CZ-01 až CZ-10	Všichni poskytovatelé	A
RMF-04	X.2.3	Všechny TR (pøšetření)	Všichni poskytovatelé	A
RMF-05	X.2.3	Všechny TR (postupy)	Všichni poskytovatelé	A
RMF-06	X.2.3	Všechny TR (risk appetite)	Všichni poskytovatelé	A
RMF-07	X.2.3	CZ-01 až CZ-10 (implementační)	Všichni poskytovatelé	A
RMF-08	X.2.4	Všechny TR (pøezkum)	Všichni poskytovatelé	A
RMF-09	X.2.4	Všechny TR (schválení)	Všichni poskytovatelé	A
RMF-10	X.2.5	Všechny TR (monitorování)	Všichni poskytovatelé	A
RMF-11	X.2.6	Všechny TR (sdílení s CB)	Všichni poskytovatelé	A
RMF-12	X.2.6	Všechny TR (trasovatelnost)	Všichni poskytovatelé	A
X.3 Politiky a postupy				
POL-01	X.3.1	Všechny TR (Wallet Service Practice Statement)	Všichni poskytovatelé	A
POL-02	X.3.2	Všechny TR (Terms and Conditions)	Všichni poskytovatelé	A
POL-03	X.3.2	TR25, TR29 (privacy policy)	Všichni poskytovatelé	A
POL-04	X.3.2	TR38 (informování o změnách)	Všichni poskytovatelé	A
POL-05	X.3.2	TR38 (žádosti o informace)	Všichni poskytovatelé	A
POL-06	X.3.2	eIDAS čl. 5a(5)(g) (bezúplatné služby)	Všichni poskytovatelé	A
POL-07	X.3.2	CZ-specifické (český jazyk)	Všichni poskytovatelé	A
POL-08	X.3.3	Všechny TR (bezpečnostní politika)	Všichni poskytovatelé	A
POL-09	X.3.3	TR34, TR111, TR117, TR127, TR131	Poskytovatel peněženky	A
POL-10	X.3.3	CZ-01, CZ-02 (kanál instance ↔ WSCD)	Poskytovatel peněženky	A
X.4 Správa a provoz poskytovatele				
ORG-01	X.4.1.1	Všechny TR (vnitřní organizace)	Všichni poskytovatelé	A
ORG-02	X.4.1.1	Všechny TR (ISMS)	Všichni poskytovatelé	A
ORG-03	X.4.1.2	Všechny TR (spolehlivost)	Všichni poskytovatelé	A
ORG-04	X.4.1.3	Všechny TR (oddělení povinností)	Všichni poskytovatelé	A
ORG-05	X.4.1.3	CZ-10 (kumulace rolí)	Subjekt s více rolemi	A+I
HR-01	X.4.2	Všechny TR (lidské zdroje)	Všichni poskytovatelé	A
HR-02	X.4.2	CZ-05 (privilegovaný přístup)	Poskytovatel peněženky a subdod.	A+I
AST-01	X.4.3.1	Všechny TR (správa aktiv)	Všichni poskytovatelé	A
AST-02	X.4.3.2	Všechny TR (klasifikace aktiv)	Všichni poskytovatelé	A+I
AST-03	X.4.3.2	TR53, TR58, TR125 (kritická aktiva)	Všichni poskytovatelé	A+I
AST-04	X.4.3.2	TR34, TR127, TR131 (uživ. zařízení)	Poskytovatel peněženky	A
AST-05	X.4.3.2	TR53, TR58, TR60 (vazba na zařízení)	Všichni poskytovatelé	A+I
AST-06	X.4.3.3	Všechny TR (úložná média)	Všichni poskytovatelé	A+I
ACC-01	X.4.4	Všechny TR (řízení přístupu)	Všichni poskytovatelé	A+I
ACC-02	X.4.4	CZ-01, CZ-05, CZ-06 (PAM, dual control WSCD)	Provozovatel WSCD	A+I+T
CRY-01	X.4.5	TR116 (krypt. algoritmy ECCG)	Všichni poskytovatelé	A+I
CRY-02	X.4.5	TR116 (mechanismy ECCG)	Všichni poskytovatelé	A+I
CRY-03	X.4.5	TR53, TR58 (krypt. aktiva mimo WSCD)	Všichni poskytovatelé	A+I
CRY-04	X.4.5	CZ-01; TR53, TR58, TR59 (cert. WSCD)	WSCD (HSM)	C
CRY-05	X.4.5	CZ-01, CZ-02; TR50, TR105, TR119	Kanál instance ↔ WSCD	A+I
PHY-01	X.4.6	Všechny TR (fyzická bezpečnost)	Všichni poskytovatelé	A+I
PHY-02	X.4.6	TR53, TR58, TR125 (kritické komp.)	Provozovatel WSCD	A+I
PHY-03	X.4.6	CZ-01, CZ-06 (DC se vzdáleným WSCD)	Provozovatel WSCD	A+I
OPS-01	X.4.7	Všechny TR (provozní bezpečnost)	Všichni poskytovatelé	A+I
OPS-02	X.4.7	čl. 8(3)(g) CIR (certif. verze)	Všichni poskytovatelé	A+I
NET-01	X.4.8	Všechny TR (síťová bezpečnost)	Všichni poskytovatelé	A+I
NET-02	X.4.8	CZ-01, CZ-02; TR50, TR105, TR119, TR121	Kanál instance ↔ WSCD	A+I+T
NET-03	X.4.8	CZ-05, CZ-06 (admin síť)	Provozovatel kritických komp.	A+I
VIM-01	X.4.9	TR110 (monitorování, incidenty)	Všichni poskytovatelé	A+I

FRD-01	X.4.9.1	TR14, TR28, TR51, TR84, TR99 (informovanost o podvodech)	Všichni poskytovatelé	A+I
FRD-02	X.4.9.1	TR14, TR28, TR51, TR84, TR99 (analýza)	Všichni poskytovatelé	A+I
FRD-03	X.4.9.1	TR14, TR28 (řízení jako zranitel.)	Všichni poskytovatelé	A
FRD-04	X.4.9.1	TR14, TR28, TR51 (sdílení s CB)	Všichni poskytovatelé	A
FRD-05	X.4.9.1	CZ-03, CZ-09; TR5, TR28, TR51, TR84, TR99	Všichni poskytovatelé	A+I
EVD-01	X.4.10	TR49, TR52 (shromažďování důkazů)	Všichni poskytovatelé	A
EVD-02	X.4.10	TR49, TR52, TR62 až TR64 (kategorie záznamů)	Všichni poskytovatelé	A+I
BCM-01	X.4.11.1	TR65, TR80, TR81 (BCM)	Všichni poskytovatelé	A
BCM-02	X.4.11.2	TR65, TR80 (zálohování)	Všichni poskytovatelé	A+I
BCM-03	X.4.11.3	TR65, TR80 (krizové řízení)	Všichni poskytovatelé	A
BCM-04	X.4.11.4	CZ-01, CZ-02, CZ-08 (kontinuita kritických komp.)	Provozovatel kritických komp.	A+I+T
TRM-01	X.4.12	TR79 (ukončení činnosti)	Všichni poskytovatelé	A
TRM-02	X.4.12	CZ-08 (migrace, finanční zajištění)	Poskytovatel peněženky a PID	A
CMP-01	X.4.13	Všechny TR (shoda)	Všichni poskytovatelé	A
CMP-02	X.4.13	GDPR, NIS2, eID zákony ČR	Všichni poskytovatelé	A
SUP-01	X.4.14.1	Všechny TR (politika dod. řetězce)	Všichni poskytovatelé	A
SUP-02	X.4.14.2	TR114, TR115 (postupy dod. řetězce)	Všichni poskytovatelé	A
SUP-03	X.4.14.3	Všechny TR (SLA)	Všichni poskytovatelé	A
SUP-04	X.4.14.3	CZ-04 až CZ-07 (požadavky na třetí strany)	Všichni poskytovatelé	A+I
SUP-05	X.4.14.4	čl. 5(7) CIR; CRA příloha I (SBOM)	Poskytovatel peněženky	A+I
SUP-06	X.4.14.5	CZ-04, CZ-06, CZ-07 (klíčoví dodavatelé)	Poskytovatel peněženky a PID	A+I
SUP-07	X.4.14.5	CZ-04, CZ-07 (úschova zdrojového kódu)	Poskytovatel peněženky a PID	A+I
X.5 ISMS procesy				
DEV-01	X.5.1	TR115 (SSDLC)	Všichni poskytovatelé	A+I
DEV-02	X.5.1	TR115 (vývojové činnosti)	Všichni poskytovatelé	A+I
DEV-03	X.5.1	TR115; CZ-05, CZ-07 (oddělení prostředí)	Všichni poskytovatelé	A+I
DEV-04	X.5.1	CZ-05 (důkazy SSDLC)	Poskytovatel peněženky a PID	A+I
DEV-05	X.5.1	CZ-07 (subdodavatel vývoje)	Subdodavatelé vývoje	A+I
CHG-01	X.5.2	čl. 8(3)(c) CIR (řízení změn)	Všichni poskytovatelé	A+I
CHG-02	X.5.2	Příloha II.3.2 (významnost změn)	Všichni poskytovatelé	A
CHG-03	X.5.2	čl. 8(3)(c) CIR (procesní rámec)	Všichni poskytovatelé	A
CHG-04	X.5.2	čl. 16(3) schématu (notifikace CB)	Všichni poskytovatelé	A
CHG-05	X.5.2	Příloha II (dozorová hodnocení)	Všichni poskytovatelé	A+I
VUL-01	X.5.3	TR110; čl. 22 schématu	Všichni poskytovatelé	A+I
VUL-02	X.5.3	TR110; čl. 5(7) CIR (aktualizace)	Všichni poskytovatelé	A+I
VUL-03	X.5.3	čl. 22(3), 26 schématu (CVD příjem)	Všichni poskytovatelé	A
VUL-04	X.5.3	Příloha II.3.3 (významnost dopadu)	Všichni poskytovatelé	A
VUL-05	X.5.3	CZ-01, CZ-04, CZ-06, CZ-07 (rozsah)	Všichni poskytovatelé	A+I
VUL-06	X.5.3	Příloha II (dozorová hodnocení)	Všichni poskytovatelé	A+I
INC-01	X.5.4	TR110; čl. 5(2) CIR	Všichni poskytovatelé	A+I
INC-02	X.5.4	TR110 (procesní rámec)	Všichni poskytovatelé	A
INC-03	X.5.4	čl. 16(3) schématu (notifikace CB)	Všichni poskytovatelé	A
INC-04	X.5.4	eIDAS čl. 5a(10), čl. 5a(20), čl. 5e, čl. 46a; NIS2; GDPR	Všichni poskytovatelé	A
INC-05	X.5.4	TR110 (post-incident review)	Všichni poskytovatelé	A
INC-06	X.5.4	CZ-01, CZ-04, CZ-06 (koordinace)	Všichni poskytovatelé	A+I
INC-07	X.5.4	Příloha II (dozorová hodnocení)	Všichni poskytovatelé	A+I
FRD-P01	X.5.5	TR14, TR28, TR51 (proces)	Všichni poskytovatelé	A+I

FRD-P02	X.5.5	TR14, TR28, TR51, TR84, TR99 (definice procesu)	Všichni poskytovatelé	A+I
FRD-P03	X.5.5	CZ-01, CZ-03, CZ-05, CZ-09; TR5, TR87, TR98	Všichni poskytovatelé	A+I
FRD-P04	X.5.5	čl. 27 schématu (sdílení trendů)	Všichni poskytovatelé	A
FRD-P05	X.5.5	Příloha II (dozorová hodnocení)	Všichni poskytovatelé	A+I
X.6 Požadavky na jednotku peněženky				
WUG-01	X.6.1	TR8 (aktivace WUA)	Jednotka peněženky	A+I+T
WUG-02	X.6.1	TR8 (aktivace PID před EAA)	Jednotka peněženky	A+I+T
WUG-03	X.6.1	TR58, TR59 (klíče ve WSCA/WSCD)	WSCA/WSCD	I
WUG-04	X.6.1	CZ-01; TR60, TR119, TR123 (izolace uživ.)	WSCA/WSCD	I+T
WUG-05	X.6.1	CZ-05; TR129, TR130 (omezení přístupu)	Poskytovatel peněženky	A+I
WUG-06	X.6.1	CZ-01; TR60 (svázání jednotky s WSCD)	Jednotka peněženky/WSCD	I+T
WUG-07	X.6.1	TR79; eIDAS čl. 5a(8) (životní cyklus)	Jednotka peněženky	A+I
WUI-01	X.6.2.1	TR2, TR3 (aktivace PID)	Jednotka peněženky	A+I+T
WUI-02	X.6.2.1	TR10, TR12, TR13 (vydávání PID)	Jednotka peněženky	A+I+T
WUI-03	X.6.2.1	TR3, TR4, TR9 (validace PID)	Jednotka peněženky	A+I+T
WUI-04	X.6.2.1	TR55, TR98 (autentizace před vydáním)	Jednotka peněženky	A+I
WUI-05	X.6.2.1	TR25, TR28 (souhlas uživatele)	Jednotka peněženky	A+I+T
WUM-01	X.6.2.2	TR36, TR39 (Metoda A/B)	Jednotka peněženky	A
WUM-02	X.6.2.2	TR60 (re-issuance)	Jednotka peněženky	A+I
WUM-03	X.6.2.2	CZ-08; TR58 (zničení klíč. mat.)	Jednotka peněženky/WSCD	A+I
WUM-04	X.6.2.2	TR44, TR46, TR47 (kontrola revokace)	Jednotka peněženky	A+I
WUM-05	X.6.2.2	CZ-02 (chování při nedostupnosti WSCD)	Jednotka peněženky	A+I+T
WUP-01	X.6.2.3	CZ-09; TR26, TR74, TR102 (autent. RP)	Jednotka peněženky	A+I+T
WUP-02	X.6.2.3	CZ-09; TR25, TR28, TR51 (zobrazení RP)	Jednotka peněženky	A+I+T
WUP-03	X.6.2.3	TR25, TR29, TR40 (selektivní zveřejnění)	Jednotka peněženky	A+I+T
WUP-04	X.6.2.3	TR41, TR42 (integrita atributů)	Jednotka peněženky	A+I
WUP-05	X.6.2.3	CZ-09; TR74, TR102 (registrace RP)	Jednotka peněženky	A+I+T
WUP-06	X.6.2.3	CZ-09; TR74, TR102 (odmítnutí prezentace)	Jednotka peněženky	A+I+T
AUTH-01	X.6.3.1	TR55, TR98 (autentizace na úrovni aplikace)	Jednotka peněženky	A+I+T
AUTH-02	X.6.3.1	TR35, TR55, TR98 (dvoufaktorová)	Jednotka peněženky/WSCD	A+I+T
AUTH-03	X.6.3.1	TR55, TR98, TR113 (autent. ve WSCD)	WSCD	C
AUTH-04	X.6.3.1	TR98 (jedna autentizace na operaci)	WSCA/WSCD	A+I
AUTH-05	X.6.3.1	TR99, TR100, TR105 (proti-phishing)	WSCA/WSCD	A+I
UI-01	X.6.3.2	TR28, TR51, TR87, TR99, TR100	Jednotka peněženky	A+I+T
ORC-01	X.6.3.3	TR88, TR90 (orchestrace)	Jednotka peněženky	A+I
TRU-01	X.6.3.4	TR3, TR10, TR44, TR45, TR46, TR47	Jednotka peněženky	I+T
PRV-01	X.6.3.5	TR36, TR39, TR84, TR85 (pseudonymy)	Jednotka peněženky a backend	A+I
PRV-02	X.6.3.5	TR37 (privacy-preserving revokace)	Backend	A+I
PRV-03	X.6.3.5	eIDAS čl. 5a(5)(b)	Jednotka peněženky a backend	I+T
WIN-01	X.6.4.1	TR50, TR57, TR119, TR121 (ochrana aktiv)	Instance peněženky	I
WIN-02	X.6.4.2	TR56, TR107, TR111, TR112, TR114, TR127 (mob. apl.)	Instance peněženky	I+T
WIN-03	X.6.4.2	Všechny TR instance (FitCEM AVA_VAN.3)	Instance peněženky	C
WIN-04	X.6.4.3	OWASP ASVS L3 (web. apl., podmíněný)	Webová instance	A+I+T
WSA-01	X.6.5	TR55, TR58 (autentizace WSCA)	WSCA	C
WSA-02	X.6.5	CZ-01; TR60 (multi-uživ. WSCA)	WSCA	C+I+T

WSA-03	X.6.5	TR55, TR98 (autentizace uživatele)	WSCA	C
WSA-04	X.6.5	TR58, TR98 (operace s klíči)	WSCA	C
WSA-05	X.6.5	TR53, TR58, TR59 (zákaz exportu klíčů)	WSCA/WSCD	C
WSA-06	X.6.5	CZ-01 (AVA_VAN úroveň)	WSCA	C
WSCD-01	X.6.6	TR53, TR58, TR59, TR125, TR126	WSCD	C
WSCD-02	X.6.6	CZ-01; TR60, TR119, TR123 (multi-tenancy)	WSCD	C+I+T
WSCD-03	X.6.6	CZ-01, CZ-02 (redundance, DR)	WSCD	A+I
KST-01	X.6.6	TR53 (keystore AVA_VAN.3)	Keystore	C
X.7 Služby poskytovatele peněženky				
WPS-01	X.7.1	TR8, TR107 (WUA prezentace)	Poskytovatel peněženky	A+I+T
WPS-02	X.7.1	TR110 (monitorování zabezpečení)	Poskytovatel peněženky	A+I
WPS-03	X.7.1	TR111, TR112, TR114 (ověření pravosti instance)	Poskytovatel peněženky	A+I+T
WPS-04	X.7.1	TR117 (kontrola způsobilosti)	Poskytovatel peněženky	A+I+T
WPS-05	X.7.1	CZ-08 (uživ. účet, nezávislá autent.)	Poskytovatel peněženky	A+I
WPS-06	X.7.1	TR53, TR58 (ověření certifikace WSCD)	Poskytovatel peněženky	A+I
WPS-07	X.7.1	CZ-01, CZ-02; TR50 (autent. komunikace)	Poskytovatel peněženky	A+I
WPS-08	X.7.1	TR110, TR111, TR127 (monitorování)	Poskytovatel peněženky	A+I+T
WPS-09	X.7.1	CZ-08; TR48 (obnova jednotky peněž.)	Poskytovatel peněženky	A+I+T
WUA-01	X.7.2	TR114; ETSI 319 411-1 NCP+	Poskytovatel peněženky	A
WUA-02	X.7.2	TR36, TR39, TR84 (bez údajů uživatele)	Poskytovatel peněženky	A+I
WUA-03	X.7.2	TR36, TR39 (odstranění metadat)	Poskytovatel peněženky	A+I
WUA-04	X.7.2	TR47 (platnost ≥ 24h)	Poskytovatel peněženky	A+I
WUA-05	X.7.2	TR47 (jedinečný identifikátor)	Poskytovatel peněženky	A+I
REV-01	X.7.3	TR79, TR104 (nevratnost revokace)	Poskytovatel peněženky	A+I
REV-02	X.7.3	CZ-08 (revokace na žádost uživ.)	Poskytovatel peněženky	A+I+T
REV-03	X.7.3	TR104 (revokace na žádost PID)	Poskytovatel peněženky	A+I
REV-04	X.7.3	TR110; eIDAS čl. 5a(8) (další trigger)	Poskytovatel peněženky	A+I
REV-05	X.7.3	TR104 (notifikace 24h)	Poskytovatel peněženky	A+I+T
REV-06	X.7.3	TR65, TR80 (ochrana proti DoS)	Poskytovatel peněženky	A+I+T
WIA-01	X.7.4	TR47, TR112 (krátká platnost WIA)	Poskytovatel peněženky	A+I
WIA-02	X.7.4	TR8 (WIA prezentace)	Poskytovatel peněženky	A+I
WUS-01	X.7.5	CZ-05; TR129, TR130 (oddělení svc)	Poskytovatel peněženky	A+I
WUS-02	X.7.5	CZ-01, CZ-05, CZ-06 (vzdálená infra)	Poskytovatel peněženky	A+I+T
WUS-03	X.7.5	CIR 2015/1502 LoA vysoká	Poskytovatel peněženky	A+I
UPD-01	X.7.6	TR111, TR114; čl. 8(3)(g) CIR	Všichni poskytovatelé	A+I
UPD-02	X.7.6	TR111, TR112, TR114 (code signing)	Všichni poskytovatelé	A+I+T
UPD-03	X.7.6	čl. 5(7) CIR (oddělení bezp. aktualizací)	Všichni poskytovatelé	A+I
UPD-04	X.7.6	TR111, TR114 (distribuce aktualizací)	Poskytovatel peněženky	A+I+T
UPD-05	X.7.6	CZ-01 (aktualizace sdílené WSCA)	Provozovatel WSCA	A+I+T
DPR-01	X.7.7	eIDAS čl. 5a(14), čl. 5c(1)	Poskytovatel peněženky	A+I
DPR-02	X.7.7	eIDAS čl. 5a(14) (doplnění schématu)	Poskytovatel peněženky	A+I
DPR-03	X.7.7	eIDAS čl. 5a(14) (doplnění schématu)	Poskytovatel peněženky	A+I
X.8 Služby poskytovatele PID				
PIDR-01	X.8.1	ETSI 319 411-1 NCP+	Poskytovatel PID	A
PIDR-02	X.8.1	CZ-03; TR2, TR3, TR9 (LoA vysoká)	Poskytovatel PID	A+I
PIDR-03	X.8.1	TR4, TR9 (autent. WIA)	Poskytovatel PID	A+I+T
PIDR-04	X.8.1	TR12, TR13 (ověření obsahu WIA)	Poskytovatel PID	A+I
PIDR-05	X.8.1	TR116 (CSRNG)	Poskytovatel PID	A+I
PIDR-06	X.8.1	TR36, TR39 (časová razítka v dávce)	Poskytovatel PID	A+I

PIDR-07	X.8.1	TR36 (odstranění unikátních prvků)	Poskytovatel PID	A+I
PIDR-08	X.8.1	TR36, TR39 (metody prezentace)	Poskytovatel PID	A
PIDR-09	X.8.1	CZ-05; TR2, TR9, TR14 (validace vůči autoritativnímu zdroji)	Poskytovatel PID	A+I
PIDR-10	X.8.1	CZ-04 (integrita pečeti)	Poskytovatel PID	A+I+C
PIDR-11	X.8.1	CZ-03, CZ-05; TR5, TR14 (anti-fraud)	Poskytovatel PID	A+I
PIDM-01	X.8.2	TR2 (validita atributů)	Poskytovatel PID	A+I
PIDM-02	X.8.2	TR60 (znovuvydání téže jednotce)	Poskytovatel PID	A+I
PIDM-03	X.8.2	CZ-specifické (detekce změn v autorit. zdroji)	Poskytovatel PID	A+I
PIDR-R01	X.8.3	TR79 (politika revokace PID)	Poskytovatel PID	A
PIDR-R02	X.8.3	TR68, TR69, TR82 (revokační trigger)	Poskytovatel PID	A+I+T
PIDR-R03	X.8.3	TR104 (jediná odpovědná strana)	Poskytovatel PID	A
PIDR-R04	X.8.3	TR37 (privacy-preserving revokace)	Poskytovatel PID	A+I
PIDR-R05	X.8.3	TR82 (revokace navázaná na peněž.)	Poskytovatel PID	A+I+T
PIDR-R06	X.8.3	CZ-09, CZ-10 (křížová kontrola)	Poskytovatel PID a peněženky	A+I+T
ONB-01	X.8.4	TR5, TR6, TR7, TR11 (LoA vysoká)	Poskytovatel PID	A+I+T
ONB-02	X.8.4	CZ-03 (specifické kontroly prostředku)	Poskytovatel PID	A+I+T
ONB-03	X.8.4	CZ-03; TR5 (monitorování podvodů)	Poskytovatel PID	A+I
ONB-04	X.8.4	ETSI TS 119 461 kap. 8.5 (důkaz o ověření totožnosti)	Poskytovatel PID	A+I
X.9 Ověřovací služba				
VER-01	X.9.2	TR79, TR107 (platnost peněženky)	Provozovatel ověř. služby	A+I+T
VER-02	X.9.2	TR41, TR42 (integrita informací)	Provozovatel ověř. služby	A+I
VER-03	X.9.2	CZ-02; TR65, TR66, TR80 (dostupnost)	Provozovatel ověř. služby	A+I+T
VER-04	X.9.3	CZ-09; TR74, TR102 (identita RP)	Provozovatel ověř. služby	A+I+T
VER-05	X.9.3	TR25, TR40 (politika zpřístupnění)	Provozovatel ověř. služby	A+I
VER-06	X.9.3	CZ-09; TR74, TR102 (integrita registru RP)	Provozovatel ověř. služby	A+I
VER-07	X.9.3	CZ-09, CZ-10 (řízení přístupu k registru RP)	Provozovatel ověř. služby	A+I
VER-08	X.9.4	TR74, TR102 (společný mechanismus)	Provozovatel ověř. služby	A+I+T
VER-09	X.9.4	CZ-09; TR4, TR102 (vázanost na registraci)	Provozovatel ověř. služby	A+I
VER-10	X.9.5	Všechny TR (ISMS služby)	Provozovatel ověř. služby	A+I
VER-11	X.9.5	TR65, TR66, TR80 (redundance)	Provozovatel ověř. služby	A+I
VER-12	X.9.5	CZ-10 (oddělení od ostatních infra)	Provozovatel ověř. služby	I
VER-13	X.9.5	eIDAS čl. 5a(8) (strojový formát)	Provozovatel ověř. služby	I+T
VER-14	X.9.5	TR39, TR84 (ochrana soukromí)	Provozovatel ověř. služby	A+I
X.10 Předpoklady provozního prostředí				
ENV-01	X.10.1	Všechny TR (rámeček předpokladů)	Všichni poskytovatelé	A
ENV-02	X.10.1	Všechny TR (důkazy pro prostředí dod. poskyt.)	Všichni poskytovatelé	A+I
ENV-03	X.10.1	TR34, TR111, TR117, TR127, TR131	Poskytovatel peněženky	A+I+T
ENV-04	X.10.1	Všechny TR (nepodložené předpoklady)	Všichni poskytovatelé	A
ENV-UD-01	X.10.2	TR117 (OS uživ. zařízení)	Poskytovatel peněženky	A+I+T
ENV-UD-02	X.10.2	TR111, TR127 (rooting/jailbreak)	Poskytovatel peněženky	A+I+T
ENV-UD-03	X.10.2	TR34, TR127 (izolace aplikací)	Poskytovatel peněženky	A+I+T
ENV-UD-04	X.10.2	TR131 (zámek obrazovky)	Poskytovatel peněženky	A+I
ENV-UD-05	X.10.2	TR111, TR131 (chování při nesplnění)	Poskytovatel peněženky	A+I+T
ENV-INF-01	X.10.3	CZ-01, CZ-02, CZ-06 (vzdálený WSCD)	Provozovatel WSCD	A+I+C
ENV-INF-02	X.10.3	CZ-03 (prostředek eID)	Poskytovatel peněženky a PID	A+C
ENV-INF-03	X.10.3	CZ-04 (služba pečeti PID)	Poskytovatel PID	A+C
ENV-INF-04	X.10.3	CZ-01 (hardware WSCD)	Provozovatel WSCD	A+C
ENV-INF-05	X.10.3	CZ-05 (autoritativní zdroj identitních)	Poskytovatel PID	A

		údajů)		
ENV-WSCD-01	X.10.4	TR53, TR58, TR59 (lokální ext. WSCD)	Provozovatel WSCD	A+C
ENV-WSCD-02	X.10.4	CZ-01 (vzdálený WSCD = komponenta)	Provozovatel WSCD	A
ENV-WSCD-03	X.10.4	TR53 (lokální ext. WSCD, podmíněný)	Provozovatel WSCD	A+C

X.B.2 Statistika pokrytí architekturně specifických rizik CZ-01 až CZ-10

Následující tabulka uvádí, kterými požadavky je každé architekturně specifické riziko CZ-01 až CZ-10 pokryto. Každé riziko je pokryto kombinací požadavků z různých kapitol (vrstvená bezpečnost).

Riziko	Počet opatření	Pokrývající požadavky
CZ-01	22	ACC-02, CRY-04, CRY-05, PHY-03, NET-02, WUG-04, WUG-06, WSA-02, WSA-06, WSCD-02, WSCD-03, BCM-04, WPS-07, WUS-02, UPD-05, ENV-INF-01, ENV-INF-04, ENV-WSCD-02, POL-10, VUL-05, INC-06, FRD-P03
CZ-02	9	CRY-05, NET-02, WUM-05, BCM-04, WPS-07, WSCD-03, ENV-INF-01, POL-10, VER-03
CZ-03	7	ONB-02, ONB-03, PIDR-02, PIDR-11, ENV-INF-02, FRD-05, FRD-P03
CZ-04	7	PIDR-10, SUP-04, SUP-06, SUP-07, ENV-INF-03, VUL-05, INC-06
CZ-05	12	HR-02, DEV-03, DEV-04, WUG-05, WUS-01, WUS-02, PIDR-09, PIDR-11, ACC-02, NET-03, FRD-P03, ENV-INF-05
CZ-06	10	PHY-03, NET-03, ACC-02, SUP-04, SUP-06, ENV-INF-01, WUS-02, INC-06, VUL-05, VER-12
CZ-07	6	DEV-03, DEV-05, SUP-04, SUP-06, SUP-07, VUL-05
CZ-08	7	WPS-05, WPS-09, REV-02, REV-05, BCM-04, WUM-03, TRM-02
CZ-09	11	VER-04, VER-06, VER-07, VER-09, WUP-01, WUP-02, WUP-05, WUP-06, PIDR-R06, FRD-05, FRD-P03
CZ-10	4	ORG-05, VER-07, VER-12, PIDR-R06

X.B.3 Statistika dle metody hodnocení

Celkový počet požadavků v matici (informativní údaj): 239

Metoda hodnocení	Počet požadavků	% z celku
A — Audit (přezkum dokumentace a politik)	218	91 %
I — Inspekce (ověření implementace)	161	67 %
T — Testování (funkční a bezpečnostní)	54	23 %
C — Certifikát (opětovné použití cert.)	19	8 %

Poznámka: Statistiky v kapitolách X.B.2 a X.B.3 jsou informativní a odpovídají stavu matice X.B v této verzi schématu. Součet procent přesahuje 100 %, protože většina požadavků je hodnocena kombinací více metod (například A+I, I+T, A+I+T). Architekturně specifické požadavky (zejména pro architekturu se vzdáleným WSCD) se opírají o kombinaci certifikátu komponenty (C) a inspekce/testování provozního nasazení (I+T).