

24 Příloha XI – Metody a postupy hodnotících činností

XI.1 Hodnotící činnosti

Tato kapitola definuje metody a postupy pro hodnotící činnosti, které jsou buď specifické pro schéma EUDIW-CZ, nebo mají specifickou definici v kontextu schématu. Prezentace těchto činností je volně inspirována definicí komponent bezpečnostní záruky (SAR) z Common Criteria a strukturuje pro každou činnost zvlášť povinnosti poskytovatele služby IKT, požadované výstupy a činnosti hodnotitele.

Klasifikace metod hodnocení

Certifikace kybernetické bezpečnosti v rámci schématu EUDIW-CZ se zaměřuje na tři hlavní aspekty:

- a) shodu s nefunkčními požadavky — požadavky, jejichž shodu nelze posoudit pouze testováním shody;
- b) odolnost implementace společných protokolů a rozhraní proti sekundárním hrozbám — hrozbám na implementaci protokolů, nikoliv přímo na aktiva peněženky;
- c) celkovou odolnost implementace proti hrozbám na aktiva peněženky identifikovaným v registru rizik dle přílohy I CIR (EU) 2024/2981 a v příloze X (kapitole X.A) schématu EUDIW-CZ.

Hodnotící činnosti definované v této příloze využívají čtyři základní metody hodnocení, označované zkratkami:

- **A = Audit** — přezkum dokumentace, politik a postupů poskytovatele služby IKT;
- **I = Inspekce** — ověření implementace bezpečnostních opatření, zpravidla na základě prohlídky konfigurace, zdrojového kódu nebo jiných implementačních artefaktů;
- **T = Testování** — funkční a bezpečnostní testy ověřující, že implementace funguje v souladu se specifikací a je odolná vůči předpokládaným hrozbám;
- **C = Certifikát** — opětovné využití existujícího certifikátu komponenty třetí strany prostřednictvím analýzy závislostí dle kritérií přijatelnosti definovaných v příloze IX schématu.

Většina bezpečnostních požadavků definovaných v příloze X 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 nebo testování provozního nasazení (I+T).

V příloze X je u jednotlivých požadavků uváděn orientační odkaz na použitou metodu pomocí výše uvedených zkratk.

XI.1.1 Posouzení návrhu

Posouzení návrhu je hodnotící činnost prováděná v první fázi hodnocení (příloha VIII, část “1. Fáze auditu”). Jejím účelem je vyhodnotit, jakým způsobem poskytovatel služby IKT tvrdí, že návrh jeho služby pokrývá

hodnotící kritéria schématu EUDIW-CZ a rizika z registru rizik dle přílohy I CIR (EU) 2024/2981, doplněné o rizika specifická pro architekturní profil schématu EUDIW-CZ (kapitola X.A), a identifikovat případné odchylky od těchto kritérií.

Činnosti poskytovatele

Poskytovatel předloží tvrzení o shodě návrhu své služby IKT, které zahrnuje:

a) určení hodnotících kritérií:

- (i) na základě posouzení rizik dle kapitoly XI.1.2 určí hodnotící kritéria schématu EUDIW-CZ, která jsou aplikovatelná na jeho službu IKT;
- (ii) na základě analýzy závislostí pro všechny komponenty, pro které jsou dostupné informace o záruce, vyloučí hodnotící kritéria, která jsou pokryta těmito informacemi o záruce, a doplní kritéria odpovídající předpokladům učiněným v rámci informací o záruce;

b) zpracování známých nedostatků a odchylek:

- (i) identifikuje a zdokumentuje všechny odchylky od aplikovatelných hodnotících kritérií schématu EUDIW-CZ a od hodnotících metod, včetně známých nedostatků;
- (ii) popíše a odůvodní, jakým způsobem je zachována záruka certifikace a jak jsou identifikovaná rizika zmírněna.

Výstupy poskytovatele

Dokumentace návrhu musí zahrnovat alespoň:

- a) dokumentaci návrhu služby IKT;
- b) seznam komponent služby IKT s odkazy na jejich hodnocení shody;
- c) matici křížových odkazů mezi komponentami a jejich hodnocením shody;
- d) seznam hodnotících kritérií vyplývajících z výsledků analýzy závislostí;
- e) popis známých nedostatků a odchylek od aplikovatelných hodnotících kritérií schématu EUDIW-CZ a od hodnotících metod;
- f) popis dotčených rizik z registru rizik;
- g) plány zmírňování dopadů rizik, včetně dodatečných kritérií a alternativních hodnotících činností k dosažení požadovaných úrovní záruky, a požadované kompetence CB pro tyto činnosti.

Činnosti hodnotitele

Hodnotitel provede následující činnosti:

a) vyhodnocení návrhu služby IKT:

- (i) identifikace architektury a hlavních komponent služby IKT;
- (ii) ověření seznamu hodnotících kritérií s výsledky analýzy závislostí;
- (iii) identifikace odchylek od aplikovatelných hodnotících kritérií schématu EUDIW-CZ a od hodnotících metod;

b) vyhodnocení odchylek:

- (i) vyhodnocení identifikovaných odchylek, souvisejících rizik, navržených opatření ke zmírnění a dodatečných hodnotících činností;
- (ii) prokázání, že opatření vedoucí ke zmírnění dopadu rizik jsou přiměřená;
- (iii) prokázání, že dodatečná kritéria a dodatečné hodnotící činnosti jsou adekvátní k dosažení požadované úrovně záruky v rámci schématu EUDIW-CZ.

XI.1.2 Posouzení rizik

Posouzení rizik je hodnotící činnost prováděná v první fázi hodnocení (příloha VIII, část “1. Fáze auditu”). Jejím účelem je vyhodnotit posouzení rizik provedené poskytovatelem služby IKT a porozumět tomu, jak bezpečnostní opatření pokrývají rizika identifikovaná v registru rizik dle přílohy I CIR (EU) 2024/2981 a rizika specifická pro danou službu IKT.

Činnosti poskytovatele

Poskytovatel provede posouzení rizik navrhované služby IKT, zahrnující následující kroky:

a) kontrola relevance:

- (i) přezkum každého scénáře rizik z registru rizik a vyhodnocení jeho aplikovatelnosti pro architekturu a komponenty služby IKT;
- (ii) pokud scénář rizik není aplikovatelný, poskytnutí odůvodnění, proč (např. scénář rizik je aplikovatelný pouze v případě vzdáleného WSCD);
- (iii) pokud je scénář rizik aplikovatelný, ale obtížně interpretovatelný v závislosti na architektuře, navržení nové formulace rizika a vysvětlení, jak se na danou službu IKT aplikuje;

b) kontrola úplnosti:

- (i) ověření, že jsou pokryta všechna rizika, zejména rizika související se specifickými rozhraními, předpoklady a bezpečnostními mechanismy dané služby IKT;
 - (ii) doplnění o rizika specifická pro architekturu služby IKT, pokud je to nezbytné;
- c) vyhodnocení rizik:
- (i) pro každé riziko vyhodnocení dopadu a pravděpodobnosti;
 - (ii) určení úrovně rizika podle dopadu a pravděpodobnosti;
- d) bezpečnostní opatření:
- (i) pro každé riziko identifikace zavedených opatření v rámci služby IKT; tato opatření mohou být implementována jednou komponentou nebo sadou komponent služby IKT;
 - (ii) pro každé opatření vysvětlení, jak je ověřena jeho účinnost (certifikovaná komponenta, auditovaná služba/proces apod.);
 - (iii) určení zbytkových rizik a způsobu jejich monitorování.

Výstupy poskytovatele

Výstup posouzení rizik musí zahrnovat alespoň:

- a) seznam relevantních rizik a scénářů rizik, včetně odůvodnění relevance pro všechna rizika z registru rizik a pro rizika specifická pro službu IKT;
- b) vyhodnocení dopadu a pravděpodobnosti pro každé relevantní riziko;
- c) seznam opatření, včetně informací o záruce dostupných k ověření dostatečnosti a účinnosti každého opatření, nebo odkaz na stejný seznam v popisu služby IKT;
- d) mapování opatření na rizika s odůvodněním pokrytí a identifikací zbytkových rizik.

Činnosti hodnotitele

Hodnotitel provede následující činnosti:

- a) kontrola pokrytí registru rizik: pro každý scénář rizik z registru ověří, že
 - (i) má přímý ekvivalent v posouzení rizik poskytovatele, nebo
 - (ii) není aplikovatelný a odůvodnění je konzistentní s architekturou služby IKT, nebo

- (iii) je nahrazen specifictějším rizikem;
- b) kontrola úplnosti posouzení rizik:
 - (i) ověření, zda byla přidána rizika nad rámec registru rizik;
 - (ii) ověření pokrytí rozhraní služby IKT;
 - (iii) ověření konzistence s předpoklady;
 - (iv) ověření úplnosti vzhledem ke službě IKT;
- c) posouzení kvality vyhodnocení úrovně rizik: kontrola vyhodnocení úrovně rizika pro každé riziko;
- d) posouzení pokrytí rizik opatřeními:
 - (i) ověření relevance, tj. nezbytnosti, a úplnosti, tj. dostatečnosti opatření pro dané riziko;
 - (ii) ověření účinnosti opatření — pokud je opatření pokryto informacemi o záruce, posouzení, jakým způsobem je účinnost opatření pokryta; pokud opatření není pokryto nebo je pokryto pouze částečně informacemi o záruce, jeho zařazení na seznam opatření k ověření během hodnocení;
 - (iii) ověření seznamu zbytkových rizik, že odpovídá posouzení rizik a že proces monitorování je relevantní a zavedený;
- e) posouzení odůvodnění zbytkových rizik.

Poznámka: Vhodnost a účinnost opatření jsou ověřovány v hlavním auditu opatření v rámci druhé fáze hodnocení (příloha VIII, část “2. Fáze auditu”). Zaměřením posouzení rizik v první fázi je pokrytí rizik opatřeními s přijatelným tvrzením o záruce, nikoli ověřování implementace samotných opatření.

XI.1.3 Posouzení zranitelností

Posouzení zranitelností je hodnotící činnost prováděná v druhé fázi hodnocení (příloha VIII, část “2. Fáze auditu”). Jejím účelem je posoudit odolnost služby IKT proti útokům kvalifikovaného útočníka prostřednictvím identifikace potenciálních zranitelností a následného penetračního testování. Tato činnost je rovněž povinnou součástí dozorového hodnocení, a to nejméně jednou za dva roky (kapitola XI.3).

Struktura činnosti vychází z požadavků AVA_VAN definovaných v Common Criteria, avšak kvalifikátory úrovně analýzy zranitelností a potenciálu útočníka z Common Criteria nejsou přímo přeneseny, neboť tyto koncepty nelze jednoduše převést na hodnocení služeb IKT.

Činnosti a výstupy poskytovatele

Poskytovatel musí:

- a) poskytnout přístup ke službě IKT pod hodnocením ve verzi vhodné pro testování;
- b) poskytnout seznam komponent třetích stran použitých v implementaci služby IKT.

Tento seznam zahrnuje pouze položky specifické pro činnost posouzení zranitelností. Hodnotitel rovněž využije dokumentaci poskytnutou v rámci posouzení návrhu a další dokumentaci relevantní tomuto hodnocení.

Činnosti hodnotitele

Hodnotitel provede následující činnosti:

- a) potvrzení, že prvky poskytnuté poskytovatelem splňují všechny požadavky:
 - (i) přístup ke službě IKT je vhodný pro testování;
 - (ii) seznam komponent třetích stran zahrnuje všechny komponenty použité v implementaci služby IKT;
- b) vyhledávání ve veřejných zdrojích za účelem identifikace potenciálních zranitelností:
 - (i) ve službě IKT;
 - (ii) v komponentách uvedených v seznamu třetích stran;
 - (iii) ve specifických produktech a službách IKT v prostředí, na kterém služba závisí;
- c) provedení nezávislé analýzy zranitelností služby IKT s využitím dokumentace poskytovatele:
 - (i) uživatelská dokumentace;
 - (ii) specifikace, architektura, návrh a zdrojový kód služby IKT;
 - (iii) analýza rizik a popis bezpečnostních opatření;
- d) provedení penetračního testování na základě identifikovaných potenciálních zranitelností za účelem určení, že služba IKT je odolná proti útokům útočníka s požadovaným potenciálem útoku.

Organizace činnosti

Hodnotící činnost posouzení zranitelností je rozdělena na tři hlavní kroky:

- a) přezkum dokumentace — identifikace potenciálních zranitelností na základě vyhledávání ve veřejných zdrojích (bod b) činnosti hodnotitele) a analýzy dokumentace poskytovatele (bod c) činnosti hodnotitele);

b) hodnocení komponent — posouzení zranitelností jednotlivých komponent služby IKT, včetně komponent třetích stran, s přihlédnutím k výsledkům externích hodnocení dostupných prostřednictvím analýzy závislostí dle přílohy IX schématu;

c) posouzení integrace — ověření, že kombinace komponent nevytváří zranitelnosti, které neexistují v jednotlivých komponentách samostatně, se zvláštním zaměřením na rozhraní mezi komponentami a na předpoklady, za kterých byly jednotlivé komponenty hodnoceny.

Dozorové aspekty posouzení zranitelností

V rámci dozorových hodnocení je posouzení zranitelností propojeno s dozorovými činnostmi definovanými v kapitole XI.3 následujícím způsobem:

a) hodnocení účinnosti politiky řízení zranitelností zahrnuje přezkum zacházení s nově identifikovanými zranitelnostmi, včetně jejich ošetření, což lze považovat za aktualizaci přezkumu zranitelností;

b) hodnocení změn v certifikované službě IKT zahrnuje cílenou analýzu zranitelností zaměřenou na tyto změny;

c) na základě výsledků aktualizovaného přezkumu zranitelností a cílené analýzy zranitelností může hodnotitel rozhodnout o provedení dodatečného penetračního testování.

Poznámka: Úroveň záruky požadovaná nemusí být stejná pro všechny funkce služby IKT. Funkce související se správou a prezentací údajů o totožnosti osoby (PID) vyžadují vyšší úroveň záruky než většina ostatních funkcí. Tato diferenciací musí být zohledněna při definici rozsahu a hloubky posouzení zranitelností.

XI.1.4 Funkční testování

Funkční testování je hodnotící činnost prováděná v druhé fázi hodnocení (příloha VIII, část “2. Fáze auditu”). Jejím účelem je prokázat, že služba IKT správně implementuje nezbytné bezpečnostní funkcionality v souladu s aktuálním stavem techniky.

Struktura činnosti je inspirována požadavky ATE (Assurance Testing — Evaluation) na úrovni EAL4 z Common Criteria, se dvěma výjimkami:

(1) hloubka testování (ATE_DPT) není pokryta, neboť není zřejmé, jak převést koncepty Common Criteria na službu IKT;

(2) je dána možnost pouze pozorovat opakované provedení testů poskytovatelem namísto nezávislého testování.

Činnosti a výstupy poskytovatele

Poskytovatel musí:

- a) poskytnout důkaz o pokrytí bezpečnostních funkcí testy;
- b) otestovat službu IKT a zdokumentovat výsledky;
- c) poskytnout testovací dokumentaci, včetně testovací strategie, testovacích plánů, očekávaných výsledků a skutečných výsledků testů;
- d) poskytnout službu IKT ve verzi vhodné pro testování.

Činnosti hodnotitele

Hodnotitel provede následující činnosti:

- a) analyzovat informace o pokrytí testy a potvrdit, že bezpečnostní funkce služby IKT jsou pokryty testy;
- b) analyzovat testovací dokumentaci a potvrdit, že testovací strategie je vhodná a že skutečné výsledky testů jsou konzistentní s očekávanými výsledky;
- c) potvrdit vhodnost poskytnuté služby IKT pro testování;
- d) provést jednu z následujících možností:
 - (i) otestovat podmnožinu služby IKT k potvrzení, že služba IKT funguje, jak je specifikováno; nebo
 - (ii) pozorovat provedení podmnožiny testů poskytovatelem a potvrdit, že výsledky jsou shodné s očekávanými výsledky.

Vztah k funkčnímu testování shody

Funkční testování v rámci této kapitoly se zaměřuje na bezpečnostní funkce služby IKT. Většina parametrů potřebných pro funkční testování shody (normy, technické specifikace, testovací sady a nástroje) je identifikována nebo vyvíjena pod vedením Evropské komise v rámci Harmonizovaného rámce pro hodnocení funkční shody EUDI (FCAF - Functional Conformance Assessment Framework) a není v této příloze reprodukována.

Rozsah, oblasti a postup funkčního testování shody, včetně využití referenčních testovacích sad FCAF a přechodného postupu do doby jejich finalizace, stanoví příloha I, kapitola „Funkční požadavky na řešení peněženky“. Provedení funkčního testování shody je povinnou součástí certifikace dle přílohy Ia a jeho

úplnost se ověřuje v rámci zastřešujícího certifikátu dle přílohy Ic. Pokrytí a výsledky testů se dokumentují v Certifikační zprávě dle přílohy VI.

Při plánování funkčního testování je třeba zohlednit následující:

- a) některá schémata použitá pro certifikaci komponent (např. EUCC) mohou zahrnovat požadavky na funkční testování; tyto výsledky by měly být využity ke snížení rozsahu testování v rámci hlavního schématu;
- b) normy a technické specifikace vyžadované Evropskou komisí představují jeden z pilířů bezpečnostních principů peněženky EUDI; jejich dodržování musí být vynuceno i mezi komponentami certifikované služby (např. mezi jednotkou peněženky a službami pro poskytování peněženky nebo PID);
- c) v závislosti na dostupných zdrojích může být účelné definovat pro funkční testování shody specifické dílčí schéma, které by se mohlo opírat o CB akreditovaný dle EN ISO/IEC 17025.

XI.2 Hodnotící činnosti komponent

Tyto hodnotící činnosti jsou specifické pro jednotlivé komponenty předmětu certifikace. Ve většině případů nebudou prováděny v rámci schématu EUDIW-CZ, neboť příslušné komponenty budou hodnoceny a certifikovány v rámci jiných schémat. Schéma EUDIW-CZ však definuje omezení a doporučení pro tato externí hodnocení, aby bylo zajištěno, že jejich výsledky jsou využitelné prostřednictvím analýzy závislostí dle přílohy IX schématu.

XI.2.1 Hodnocení WSCA

WSCA musí splňovat CIR (EU) 2015/1502, eIDAS úroveň „vysoká“.

Hodnocení WSCA se nepředpokládá v rámci schématu EUDIW-CZ, ale prostřednictvím jiného vhodného schématu, zejména EUCC. CB schématu EUDIW-CZ nemusí disponovat kompetencemi pro provádění hodnocení dle Common Criteria, ale musí být schopen porozumět certifikátu EUCC a ověřit správné nasazení WSCA v rámci služby IKT (kapitola XI.2.3).

Pro WSCA, které nejsou hostovány na bezpečnostním prvku (Secure Element) nebo HSM, existuje specifický problém, neboť nejsou přiřazeny k žádné z technických domén definovaných v EUCC pro hodnocení na úrovních AVA_VAN.4 a AVA_VAN.5. V takovém případě jsou k dispozici následující alternativní přístupy:

- a) definice specifické metodologie, která bude buď zahrnuta v ochranném profilu, nebo přezkoumána NÚKIB a ECCG (European Cybersecurity Certification Group);
- b) posouzení WSCA jako služby IKT s použitím jiné hodnotící metodologie (přístup přijatý např. Rakouskem v návrhu národního certifikačního schématu);
- c) hodnocení WSCA na základě posouzení zranitelností AVA_VAN.3 s odůvodněním a prokázáním, že použití nižší úrovně nemá dopad na celkovou bezpečnost certifikované služby IKT, jak vyžaduje příloha IV CIR (EU) 2024/2981;

d) použití jiného schématu s ekvivalentní úrovní záruky, jako je jedno z dostupných schémat založených na FitCEM.

e) WSCA splňuje požadavky článku 30 nařízení eIDAS (EU 910/2014). Vyžaduje se předložení bezpečnostního cíle dle 419 241-2.

Schéma EUDIW-CZ pro verzi 1.0 přijímá přístup dle písmene c) — hodnocení WSCA na úrovni AVA_VAN.3 s odůvodněním dle požadavku WSA-06 přílohy X a s prokázáním, že snížení úrovně nemá dopad na celkovou bezpečnost certifikované služby IKT dle přílohy IV CIR (EU) 2024/2981. Přístup dle písmene a) (specifický profil ochrany) může být uplatněn po dokončení profilu ochrany pro server-side WSCA v rámci CEN TC224 WG17.

XI.2.2 Hodnocení WSCD

WSCD musí splňovat CIR (EU) 2015/1502, eIDAS úroveň „vysoká“.

Hodnocení WSCD (vzdáleného HSM) se nepředpokládá v rámci schématu EUDIW-CZ, ale prostřednictvím externího certifikačního schématu, primárně EUCC nebo CC/SOG-IS. CB schématu EUDIW-CZ nemusí disponovat kompetencemi pro provádění hodnocení dle Common Criteria, ale musí být schopen porozumět certifikátu EUCC/CC a prostřednictvím analýzy závislostí dle přílohy IX schématu ověřit správné nasazení WSCD v rámci služby IKT.

Relevantní profil ochrany pro HSM v české architektuře je CEN EN 419 221-5 (Protection Profile for HSM for Trust Services). Požadovaná minimální úroveň záruky je EAL4+ s AVA_VAN.5, v souladu s přílohou IV CIR (EU) 2024/2981 a požadavky přílohy X schématu (ENV-INF-04, WSCD-01 až WSCD-04). Pokud byl certifikát vzdáleného WSCD vydán v rámci národního CC schématu (SOG-IS MRA) před přijetím EUCC, CB posoudí rovnocennost hodnotících činností s požadavky EUCC, zejména úroveň AVA_VAN.5 a soulad s kryptografickými požadavky dle SOG-IS ACM nebo ECCG ACM.

CB při využití existujícího certifikátu vzdáleného WSCD prostřednictvím analýzy závislostí dle přílohy IX schématu provede následující zbytkové hodnotící činnosti:

- a) ověření, že certifikovaná konfigurace HSM odpovídá konfiguraci nasazené v českém prostředí, včetně souladu s pokyny pro bezpečnou administraci (AGD_OPE, AGD_PRE);
- b) ověření, že rozsah certifikátu vzdáleného WSCD pokrývá multi-tenancy scénář, tj. situaci, kdy jeden HSM obsluhuje kryptografické operace pro více wallet units současně — tento scénář nemusí být předmětem standardní certifikace vzdáleného WSCD; hodnocení musí zahrnout ověření, že klíčový materiál a kryptografické operace jednoho uživatele jsou důsledně izolovány od ostatních uživatelů sdílejících stejný HSM (WSCD-02 v příloze X schématu);

Poznámka: V případě vzdáleného WSCD (HSM) tato funkčnost může být zajištěna ve spolupráci s WSCA.

- c) ověření komunikačního kanálu mezi WSCA a vzdáleným HSM z hlediska důvěrnosti, integrity a autentizace (NET-01), včetně odolnosti proti útoku prostředníkem, odposlechu a modifikaci dat v přenosu — tento kanál

leží na hranici certifikovaného předmětu WSCD a necertifikovaného prostředí a musí být předmětem specifického testování;

d) ověření integrity a autentizace rozhraní mezi WSCA a vzdáleným WSCD se zvláštním zaměřením na autorizaci kryptografických operací;

e) ověření, že provozní povinnosti provozovatele HSM (fyzická bezpečnost, řízení přístupu, správa klíčů) jsou prokázány v souladu s ENV-INF-01 a ENV-INF-04.

Posouzení zranitelností dle kapitoly XI.1.3 musí v případě architektury vzdáleného HSM zahrnovat penetrační testování pokrývající vektory útoku specifické pro tuto architekturu, zejména útok na síťový kanál, pokus o extrakci klíčového materiálu z paměti HSM a pokus o eskalaci přístupu z jednoho tenanta na jiného.

XI.2.3 Hodnocení instance peněženky

Instance musí splňovat CIR (EU) 2015/1502, eIDAS úroveň „vysoká“.

Hodnocení instance peněženky nemusí probíhat v rámci schématu EUDIW-CZ, ale prostřednictvím schématu založeného na metodologii FitCEM (CEN EN 17640).

XI.2.4 Hodnocení IT systémů

Hodnocení IT systémů podporujících řešení peněženky (backendové služby, infrastruktura pro provozování peněženky, služby pro poskytování PID, validační služby) se provádí dle ETSI EN 319 401 a případné posouzení provozní účinnosti dle CEN TS 18026.

IT systémy nejsou hodnoceny izolovaně jako produkt, ale vždy v kontextu služby IKT, kterou podporují. Posouzení shody se zákonem č. 264/2025 Sb., o kybernetické bezpečnosti a příslušnými prováděcími vyhláškami, se proto neprovádí na úrovni IT systému jako takového, ale na úrovni regulovaného poskytovatele služby IKT a jeho organizačních, řídicích a provozních opatření vztahujících se k provozu daných IT systémů. Tyto regulační rámce se v hodnocení uplatňují prostřednictvím požadavků kapitol X.2 až X.5 přílohy X schématu a prostřednictvím komponentové struktury dle přílohy I schématu.

Pokud pro IT systém existuje relevantní certifikace nebo atestace, je tato využita jako vstupní důkaz prostřednictvím analýzy závislostí dle přílohy IX schématu. Typickými vstupními důkazy jsou:

- a) EN ISO/IEC 27001:2022 — pokud rozsah ISMS pokrývá provoz hodnoceného IT systému;
- b) atestace ISVS dle zákona č. 365/2000 Sb. a vyhlášky č. 529/2006 Sb. — pro IT systémy provozované v režimu informačních systémů veřejné správy;
- c) doklady o splnění povinností dle zákona č. 264/2025 Sb. a jeho prováděcích vyhlášek — pokud je poskytovatel regulovanou entitou dle uvedeného zákona, doklady o shodě s povinnostmi vyplývajícími z

transpozice NIS2 (zavedení opatření, hlášení incidentů, řízení rizik) se přijímají jako částečný důkaz pokrytí požadavků na úrovni poskytovatele služby;

d) SOC 2 Type II — pro infrastrukturní a cloudové komponenty.

CB v takovém případě posuzuje pouze reziduální aspekty, které nejsou pokryty existujícími důkazy, se zaměřením na EUDIW-specifické požadavky a na integraci a kompatibilitu s ostatními komponentami řešení peněženky.

XI.2.5 Hodnocení procesů

Procesy bezpečné provozní správy definované v příloze X schématu (vývoj, řízení změn, řízení zranitelností, řízení incidentů, řízení podvodů) jsou hodnoceny v rámci hlavního auditu schématu EUDIW-CZ. Procesy jsou hodnoceny na úrovni poskytovatele služby IKT jako regulovaného subjektu, nikoli izolovaně. Hodnocení procesů zahrnuje:

a) při počátečním hodnocení a hodnocení recertifikace — posouzení návrhu procesů a jejich souladu s požadavky přílohy X schématu;

b) při dozorových hodnoceních — posouzení provozní účinnosti procesů a ověření, že procesy byly konzistentně aplikovány tak, jak byly navrženy, po celé specifikované období (kapitola XI.3.3).

Pokud pro procesy existují relevantní vstupní důkazy, jsou využity prostřednictvím analýzy závislostí dle přílohy IX schématu. Typickými vstupními důkazy jsou:

a) EN ISO/IEC 27001:2022;

b) doklady o splnění povinností dle zákona č. 264/2025 Sb. a jeho prováděcích vyhlášek. Doklady prokazují organizační a procesní soulad poskytovatele jako regulovaného subjektu, nikoli technickou implementaci procesu v rámci konkrétní služby IKT. Hodnocení kybernetické bezpečnosti dle § 16 vyhlášky 409/2025 Sb. (provedené auditorem kybernetické bezpečnosti dle zákona) je přijatelným formátem dokladu;

c) ETSI EN 319 401 auditní zpráva — pokud je poskytovatel současně QTSP.

Proces řízení podvodů (FRD) není pokryt žádným z výše uvedených vstupních důkazů (ISO/IEC 27001 fraud management explicitně neřeší, zákon 264/2025 jej neupravuje) a posuzuje se vždy jako plně nová hodnotící činnost dle požadavků FRD-P01 až FRD-P05 přílohy X schématu.

XI.3 Dozorové hodnotící činnosti

Tyto činnosti jsou specifické pro dozorová hodnocení a pro udržování záruky v průběhu životního cyklu certifikátu. Jejich účelem je posoudit významnost změn v certifikované službě IKT a v prostředí hrozeb a ověřit trvalou účinnost bezpečnostních opatření.

XI.3.1 Posouzení dopadu změn služby

Při každém dozorovém hodnocení nebo hodnocení recertifikace musí být popsány změny provedené v certifikované službě IKT od posledního hodnocení a musí být posouzen jejich dopad na bezpečnost certifikované služby.

Posouzení dopadu změn služby poskytnuté poskytovatelem zohlední:

- a) dopad na posouzení rizik spojený s provedenými změnami, zejména když jsou změny provedeny v definici nebo implementaci bezpečnostního opatření;
- b) dodatečné komponenty třetích stran a související potenciální zranitelnosti.

Poskytovatel poté odhadne významnost změny a předá posouzení dopadu změny CB, pokud je změna považována za významnou. CB poté přezkoumá posouzení a rozhodne, zda je potřeba zvláštní hodnocení, a pokud ano, jaké hodnotící činnosti mají být provedeny. Změna může vyvolat zvláštní hodnocení, pokud je její dopad na bezpečnost celkové služby považován za významný.

Poznámka: Posouzení dopadu se provádí v rámci procesu řízení změn (CHG-01 až CHG-05 v příloze X kapitole X.5.2), jehož účinnost musí být přezkoumávána ročně. Posouzení dopadu se standardně předkládá CB, pouze pokud je dopad považován za významný. V prvním roce certifikace nebo při zjištěných neshodách však CB může vyžadovat předložení všech posouzení dopadu.

XI.3.2 Posouzení dopadu změn prostředí hrozeb

Prostředí hrozeb je definováno v registru rizik specifickém pro řešení peněženky. Dva hlavní zdroje informací pro identifikaci změn v prostředí hrozeb:

- a) aktualizace registru rizik dle CIR (EU) 2024/2981;
- b) identifikace zranitelností nebo nových hrozeb ovlivňujících specifickou implementaci řešení peněženky.

Když je registr rizik zahrnutý v CIR (EU) 2024/2981 aktualizován, registr rizik specifický pro řešení peněženky musí být odpovídajícím způsobem aktualizován.

Když proces řízení zranitelností identifikuje zranitelnost nové povahy nebo kategorie, která může vést k obecnější změně v prostředí hrozeb (např. když se teoretický útok stane skutečně využitelným), registr rizik specifický pro řešení peněženky musí být aktualizován o toto nové riziko a/nebo hrozbu. Hodnotitel by měl rovněž monitorovat potenciální dopad zbytkových zranitelností.

Když je registr rizik specifický pro řešení peněženky aktualizován, změna se považuje za významnou, pokud poskytovatel služby není schopen v posouzení dopadu prokázat, že nově identifikovaná rizika nejsou pro jeho službu aplikovatelná, nebo že jsou plně zmírněna opatřeními, která jsou již zavedena.

XI.3.3 Posouzení účinnosti opatření

Posouzení účinnosti opatření je dozorová hodnotící činnost, jejímž účelem je ověřit, že bezpečnostní opatření definovaná v příloze X schématu jsou provozně účinná po celé období od posledního hodnocení. Tato činnost je povinnou součástí každého dozorového hodnocení a hodnocení recertifikace v souladu s čl. 18 odst. 1 CIR (EU) 2024/2981.

Kritéria provozní účinnosti

Opatření je provozně účinné, pokud splňuje obě následující podmínky:

- a) bylo konzistentně aplikováno tak, jak bylo navrženo, po celé specifikované období;
- b) v případě manuálních opatření bylo aplikováno osobami s odpovídající kompetencí a oprávněním.

Činnosti hodnotitele

Hodnotitel provede pro každé opatření v rozsahu hodnocení následující činnosti:

- a) určení, jak bylo opatření aplikováno;
- b) ověření konzistence aplikace opatření v průběhu specifikovaného období;
- c) určení, kým nebo jakými prostředky bylo opatření aplikováno;
- d) posouzení na základě objektivních důkazů, že opatření dosahuje zvýšené úrovně záruky.

Rozsah posouzení

Posouzení účinnosti se při dozorových hodnoceních zaměřuje především na procesy údržby definované v příloze X schématu:

- a) proces vývoje (DEV-01 až DEV-05);
- b) proces řízení změn (CHG-01 až CHG-05);
- c) proces řízení zranitelností (VUL-01 až VUL-05);
- d) proces řízení incidentů (INC-01 až INC-06);
- e) proces řízení podvodů (FRD-P01 až FRD-P04).

V prvním roce certifikace je hodnocen návrh procesů, avšak provozní účinnost dosud nemůže být posouzena z důvodu absence provozního období. Od druhého roku je hodnocena provozní účinnost procesů za uplynulé období.

XI.4 Doplnky k hodnotícím činnostem specifické pro českou architekturu

Následující doplňky reflektují specifika české architektury řešení peněženky a musí být zohledněny při hodnotících činnostech v rámci schématu EUDIW-CZ. Tyto doplňky nenahrazují obecné hodnotící činnosti definované v kapitolách XI.4 až XI.6, ale rozšiřují je o aspekty vyplývající z konkrétní architektury a infrastruktury národního řešení.

XI.4.1 Posouzení procesu onboarding

Onboarding uživatelů do řešení peněženky může být v české architektuře realizován prostřednictvím více nezávislých procesů ověření identity, které mají odlišnou povahu a podléhají odlišnému certifikačnímu režimu. CB musí hodnotit každý typ onboardingového procesu zvlášť.

XI.4.1.1 Onboarding prostřednictvím národního systému elektronické identifikace

Onboardingový proces využívající prostředek elektronické identifikace a systém elektronické identifikace, který byl podle zákona 250/2017 Sb. akreditován pro úroveň „vysoká“. Hodnocení této varianty probíhá ve dvou rovinách:

a) národní systém elektronické identifikace jako sdílená národní infrastruktura podléhá notifikaci dle eIDAS a hodnocení dle CIR (EU) 2015/1502 — toto hodnocení probíhá mimo rámec schématu EUDIW-CZ a CB jej přijímá jako vstupní důkaz prostřednictvím analýzy závislostí dle přílohy IX schématu. Samostatná externí certifikace této infrastruktury v rámci schématu EUDIW-CZ není požadována;

b) integrace národního systému elektronické identifikace s procesem onboarding peněženky je hodnocena v rámci schématu EUDIW-CZ.

CB při hodnocení provede zejména:

(i) ověření, že výsledek hodnocení oznamovaného prostředku pokrývá metody ověření identity relevantní pro českou architekturu onboarding, a aplikaci analýzy závislostí dle přílohy IX schématu na toto hodnocení;

(ii) testování integračních bodů mezi národním systémem elektronické identifikace a procesem vydávání PID (ONB-02), zejména: vazby relace mezi autentizací a aktivací peněženky — ověření, že autentizační relace je kryptograficky svázána s procesem vydání PID a nelze ji zneužít pro jiný účel; anti-replay mechanismů zabraňujících opětovnému použití autentizačních tokenů; časových limitů platnosti výsledku ověření identity před dokončením aktivace peněženky;

(iii) ověření implementace monitorování podvodů v onboardingovém procesu (ONB-03) v souladu s FRD-P03(a) přílohy X schématu.

XI.4.1.2 Level-up proces

Onboarding se provádí prostředkem národního prostředku elektronické identifikace za využití systému elektronické identifikace, který byl akreditován podle zákona 250/2017 Sb. pro úroveň „značná“.

Musí být splněny následující požadavky ETSI TS 119 461 V2.1.1 (2025-02) přílohy CIR (EU) 2026/798, zejména:

- Důkazy použité ke zlepšení ověření identity z úrovně „značná“ na „vysoká“ musí prokazovat stejnou identitu jako identita získaná z ověření identity podle úrovně „značná“.
- Žadatel se autentizuje pomocí prostředku a systému elektronické identifikace úrovně „značná“ dle zákona 250/2017 Sb.
- Musí být proveden ověřovací dialog, který na úrovni spolehlivosti „značná“ použitého eID potvrzuje, že držitel eID byl úspěšně ověřen a že použitý eID je platný (nevypřel, není pozastaven ani zrušen) – aplikace VAL-8.3.4-01X.
- Musí být použit digitální doklad totožnosti, akceptují se pouze digitální doklady totožnosti s eMRTD podle normy ICAO 9303 část 10:
 - Musí být ověřen elektronický podpis struktury LDS1 (podpis *Document signer*).
 - Musí být vzdáleně ověřena ochrana proti vložení kopie digitálního dokladu (*chip authentication*). Tj. toto ověření neproběhne na zařízení žadatele, ale vzdáleným systémem.
- Pořízení snímku obličeje musí splňovat požadavky kapitoly 8.4.2 standardu ETSI TS 119 461 V2.1.1 (2025-02).
- Vazba na žadatele musí splňovat požadavky kapitoly 8.4.3 standardu ETSI TS 119 461 V2.1.1 (2025-02).

XI.4.1.3 Alternativní onboardingové procesy

Vedle onboardingu prostřednictvím národního systému elektronické identifikace mohou být v české architektuře zavedeny alternativní onboardingové procesy, které do ekosystému dodává koncesionář řešení peněženky. Tyto procesy mohou zahrnovat zejména:

a) level-up proces z úrovně záruky „značná“ na úroveň „vysoká“ prostřednictvím NFC čtení dokladu totožnosti a biometrické verifikace;

b) proces využívající fyzické ověření identity za přítomnosti žadatele, zejména na místech, kde se vydávají doklady totožnosti, nebo u pověřených agentů oprávněných k ověření totožnosti;

Alternativní onboardingové procesy mají být dostupné i dalším případným poskytovatelům jednotky peněženky. Poskytovatel PID se při jejich využití spoléhá na dodávku koncesionáře řešení peněženky.

Na rozdíl od onboardingu prostřednictvím národního systému elektronické identifikace se nepředpokládá, že alternativní onboardingové procesy budou oznámeny jako prostředky elektronické identifikace na úrovni

záruky „vysoká“ dle CIR (EU) 2015/1502. Z toho vyplývá, že pro tyto procesy nelze využít analýzu závislostí opírající se o notifikaci dle eIDAS.

CB proto musí:

(i) identifikovat relevantní požadavky z CIR (EU) 2015/1502 aplikovatelné na příslušný alternativní onboardingový proces a posoudit shodu s těmito požadavky v rámci schématu EUDIW-CZ;

(ii) posoudit, zda alternativní onboardingový proces dosahuje úrovně záruky „vysoká“ pro ověření identity, i přestože není oznámen jako prostředek eID;

(iii) pro každý alternativní onboardingový proces provést samostatné hodnocení bezpečnostních aspektů, zejména:

- odolnost biometrické verifikace a mechanismů detekce živosti proti známým útokům (pokud je aplikovatelné);
- bezpečnost procesu čtení dokladu totožnosti prostřednictvím NFC;
- bezpečnost procesu fyzického ověření identity (pokud je aplikovatelné);
- anti-replay mechanismy a časové limity;

(iv) ověření implementace monitorování podvodů (ONB-03) v souladu s FRD-P03(a) přílohy X schématu, včetně detekce hromadných pokusů o onboarding z podobných profilů zařízení, opakovaných neúspěšných pokusů o ověření identity ze stejného zdroje a anomálních geografických vzorů v žádostech o onboarding;

(v) ověření, že poskytovatel peněženky a poskytovatel PID mají zdokumentovány předpoklady o infrastruktuře alternativního onboardingového procesu (ENV-INF-02) a mechanismy pro případ jeho nedostupnosti.

XI.4.1.4 Hodnotící kritéria pro vzdálené ověření identity dle ETSI TS 119 461

Pro hodnocení onboardingových procesů, které využívají vzdálené ověření identity (ať už prostřednictvím notifikovaného prostředku eID, nebo level-up procesem ze značné na vysokou úroveň záruky), CB ověří shodu s ETSI TS 119 461, doplněnou požadavky přílohy CIR (EU) 2026/798. Posuzované oblasti jsou strukturovány následovně:

a) Autentizace prostřednictvím eID na úrovni „vysoká“ (notifikovaný prostředek dle zákona č. 250/2017 Sb.)

CB ověří splnění zejména požadavků COL-8.2.2.1-01X (autentizace), VAL-8.3.4-01X (ověřovací dialog na úrovni „vysoká“ potvrzující platnost eID) a VAL-8.3.4-02 (vazba ověřených atributů na žadatele). Jako doplňkový důkaz se v souladu s USE-9.2.4-04 použije důvěryhodný registr (zákon č. 269/2021 Sb., o občanských průkazech, § 5 odst. 1 písm. a body 1–8). Výsledkem ověření musí být strukturovaný důkaz dle kap. 8.5 ETSI TS 119 461, opatřený kvalifikovaným elektronickým časovým razítkem zajištěným ze strany

poskytovatele PID v souladu s požadavkem ONB-04 přílohy X schématu. Jedno časové razítko může pokrývat i více takových záznamů.

b) Level-up ze „značná“ na „vysoká“ — vzdálené automatické ověření bez dohledu

Pro tuto variantu, která je v české architektuře primární, CB ověří splnění požadavku USE-9.5.1-02 (důkazy pro level-up musí prokazovat tutéž identitu) a celé řady požadavků pro nedohlížený automatizovaný proces, zejména USE-9.2.3.1-01 (automatické pokyny), USE-9.2.3.1-02 (zpracování odchylek), USE-9.2.3.1-04 (digitální doklad totožnosti jako směrodatný důkaz) a INI-8.1-05 (poskytnutí opravných prostředků v případě selhání). CB rovněž ověří soulad s COL-8.2.1-08 (privacy by design dle čl. 25 GDPR pro zpracování biometrie).

c) Ověření digitálního dokladu totožnosti

CB ověří implementaci požadavků VAL-8.3.2-01 až VAL-8.3.2-06, zejména:

- zachování autenticity, integrity a důvěrnosti při přenosu dat z dokladu;
- ověření digitálního podpisu vydavatele (podpis tzv. *Document Signer*);
- ochranu proti vložení dříve získané kopie dokladu;
- opětovné čtení čipu při přerušení procesu;
- extrakci referenční fotografie obličeje pro biometrickou vazbu.

Jako digitální doklad se v souladu s COL-8.2.3-06X přijímá pouze eMRTD dle ICAO 9303 části 10 nebo doklady s prokazatelně srovnatelnou úrovní záruky.

d) Pořízení snímku obličeje — Presentation Attack Detection (PAD) a injection attacks

CB posoudí splnění požadavků BIN-8.4.2-01 až BIN-8.4.2-09X, které zahrnují:

- zachycení video streamu živé osoby v dostatečné kvalitě (např. 25 fps, 1280×720) s prevencí presentation attacks (BIN-8.4.2-02X) a uměle generovaného obsahu (BIN-8.4.2-03X);
- ochranu před biometric injection attacks (BIN-8.4.2-04A) s povinným testováním dle TS 18099 úrovně High (úroveň 3) akreditovanou laboratoří nejpozději do konce roku 2026 (BIN-8.4.2-04C); opakování hodnocení nejméně každé dva roky (BIN-8.4.2-04D);
- systematické testování PAD dle ISO/IEC 30107-3 s metrikami APCER a BPCER (BIN-8.4.2-06X), s povinným hodnocením akreditovanou laboratoří dle ISO/IEC 19989-3 nejpozději do konce roku 2026 (BIN-8.4.2-07X) opakovaným nejméně každé dva roky;
- soulad cílových hodnot APCER/BPCER s Prováděcím prohlášením IPSP (BIN-8.4.2-05D, -05E) a jejich aktualizaci na základě threat intelligence.

e) Biometrická vazba na žadatele (face matching)

CB ověří splnění požadavků BIN-8.4.3-01X až BIN-8.4.3-09X, zejména:

- automatizované porovnání obrazu z dokladu s živým obrazem provedené v prostředí kontrolovaném IPSP (BIN-8.4.3-03);
- systematické testování algoritmů dle ISO/IEC 19795-1 s ohledem na cíle FAR a FRR stanovené v Prováděcím prohlášení IPSP (BIN-8.4.3-06X, -07X, -08X);
- ověření, že cílové hodnoty FAR/FRR byly stanoveny dle metodiky ENISA „Methodology for Sectoral Cybersecurity Assessments“ nebo ekvivalentní (USE-9.2.3.4-04);
- aplikaci prostředků pro detekci morfovaných fotografií v dokladech (BIN-8.4.3-09X).

Pokud je proces vzdáleného ověření identity (nebo jeho komponenty — PAD, biometrický algoritmus) certifikován akreditovaným subjektem posuzování shody dle čl. 2 bodu 13 nařízení (ES) č. 765/2008, případně prošel vzájemným hodnocením v rámci eIDAS (USE-9.5.3-01 přílohy CIR (EU) 2026/798), CB tyto výsledky využije jako vstupní důkaz prostřednictvím analýzy závislostí dle přílohy IX schématu EUDIW-CZ a hodnotí pouze reziduální aspekty (integrace, konfigurace, předpoklady).

XI.4.2 Posouzení integrace s kvalifikovaným poskytovatelem služeb vytvářejících důvěru

Tato komponenta má kombinovaný charakter — zahrnuje servisní aspekty hodnocené dle ETSI EN 319 401 a CIR (EU) 2015/1502 i CZ-specifické aspekty vyplývající z kumulace rolí DIA a integrace s QTSP zajišťujícím pečetení PID.

Hodnocení neprobíhá prostřednictvím externího certifikačního schématu, ale jako součást hlavního auditu schématu EUDIW-CZ. Pokud QTSP provádějící pečetení PID drží existující certifikaci dle ETSI EN 319 401, CB aplikuje analýzu závislostí dle přílohy IX schématu (kapitola IX.6.7) k určení, které hodnotící činnosti mohou být zjednodušeny — zejména pro pečetení PID (PIDR-10). CB posoudí reziduální aspekty nezakryté existující certifikací QTSP, se zaměřením na explicitní pokrytí pečetení PID pro EUDIW v rozsahu certifikace QTSP, integrační rozhraní mezi poskytovatelem PID a QTSP a integrační rozhraní mezi QTSP a jednotkou peněženky. Zbývající aspekty jsou hodnoceny přímo v rámci auditu.

CB při hodnocení provede zejména následující činnosti:

- a) audit politiky vydávání PID (PIDR-01) z hlediska souladu s CIR (EU) 2015/1502 na úrovni záruky „vysoká“ a s požadavky na NCP+ dle ETSI EN 319 411-1;
- b) audit procesu ověření identity při vydávání PID (PIDR-02) a ověření souladu s CIR (EU) 2015/1502 oddílem 2.2.2, včetně inspekce integrace s NIA a validace vůči základním registrům (ROB) dle PIDR-09;
- c) ověření integrity řetězce PID → QTSP → wallet unit pro pečetení PID (PIDR-10), včetně aplikace analýzy závislostí na existující certifikaci QTSP s ověřením, že rozsah certifikace explicitně pokrývá pečetení PID pro EUDIW;

- d) audit mechanismů správy PID (PIDM-01 až PIDM-03), zejména detekce změn v základních registrech a jejich promítnutí do platnosti vydaných PID;
- e) audit a testování procesu revokace PID (PIDR-R01 až PIDR-R06), včetně mechanismu křížové kontroly stavu revokace wallet unit mezi DIA a koncesionářem (PIDR-R06) a ověření soukromí zachovávajících mechanismů revokace (PIDR-R04);
- f) ověření implementace anti-fraud monitoringu pro vydávání PID (PIDR-11) v souladu s FRD-P03(a) přílohy X schématu;
- g) ověření organizačního oddělení funkcí (ORG-02) — více v kapitole XI.4.3.

XI.4.3 Posouzení kumulace rolí

V české architektuře může jeden subjekt současně působit ve více rolích (vlastník schématu, orgán dohledu, poskytovatel PID, registrátor spoléhajících se stran). Tato kumulace rolí je dokumentována jako riziko CZ-10 v registru rizik schématu.

CB musí ověřit organizační oddělení funkcí u příslušného subjektu (ORG-02 v příloze X schématu). Hodnocení zahrnuje:

- a) přezkum organizační dokumentace — ověření existence formálně definovaného organizačního oddělení funkcí, včetně organizačních schémat, popisů rolí a odpovědností;
- b) rozhovory s relevantními pracovníky — ověření, že oddělení funkcí je v praxi dodržováno;
- c) ověření reportovacích linií — ověření, že reportovací linie pro jednotlivé role jsou nezávislé a nepodléhají střetu zájmů;
- d) ověření omezení sdílení informací — ověření, že informace získané v rámci jedné role nejsou neoprávněně sdíleny s jinými rolemi.

XI.4.4 Posouzení předpokladů prostředí

CB musí ověřit dvoustupňový model předpokladů definovaný v příloze X schématu kapitole X.10:

- a) Tier A — prostředí poskytovatele (datová centra, HSM infrastruktura). Hodnotitel vyhodnotí důkazy o splnění předpokladů prostředí, včetně fyzické bezpečnosti, řízení přístupu a provozních postupů. Hodnocení může zahrnovat inspekci na místě v datovém centru;
- b) Tier B — uživatelská zařízení. Hodnotitel vyhodnotí třístupňový proces:
 - (i) definice opatření — ověření, že poskytovatel definoval opatření pro zmírnění rizik vyplývajících z nedůvěryhodného uživatelského prostředí;
 - (ii) validace dostatečnosti — ověření, že definovaná opatření jsou dostatečná pro zmírnění identifikovaných rizik;

(iii) ověření účinnosti — ověření, že opatření jsou implementována a provozně účinná.

XI.4.5 Meziorganizační koordinace

Vzhledem k distribuované povaze české architektury, kde se na provozu řešení peněženky podílí více organizačně nezávislých subjektů (koncesionář, vlastník schématu, provozovatel HSM infrastruktury, QTSP, poskytovatel identity), musí CB ověřit funkčnost meziorganizačních koordinačních postupů, zejména:

- a) koordinovaná reakce na bezpečnostní incidenty (INC-06 v příloze X schématu) — ověření, že existují a jsou testovány postupy pro koordinovanou reakci na incident, který zasahuje více subjektů;
- b) koordinované řízení zranitelností (VUL-05 v příloze X schématu) — ověření, že existují postupy pro sdílení informací o zranitelnostech a koordinovanou nápravu mezi subjekty;
- c) koordinované řízení změn — ověření, že změny provedené jedním subjektem, které mohou ovlivnit bezpečnost celého řešení, jsou komunikovány a koordinovány s dotčenými subjekty.

Hodnocení může zahrnovat simulační cvičení (table-top exercise) koordinované reakce na incident s účastí zástupců všech relevantních subjektů.