

22 Příloha IX: Kritéria pro posouzení přijatelnosti informací o záruce

IX.1 Úvod

Účelem této přílohy je poskytnout certifikačnímu orgánu (CB) závazný rámec pro posuzování, zda informace o záruce z existujících certifikátů, hodnocení a dalších zdrojů důkazů mohou být přijaty jako vstup do certifikačního rozhodnutí dle schématu EUDIW-CZ, a pokud ano, v jakém rozsahu.

Certifikace peněženky EUDI je ze své povahy kompozitní. Řešení peněženky zahrnuje produktové komponenty (WSCD, WSCA, instance peněženky), procesní komponenty (ISMS, řízení zranitelností, řízení změn) a komponenty poskytující služby (backend poskytovatele peněženky, služby vydavatele PID, externí služby, na nichž řešení peněženky závisí). Některé z těchto komponent mohou již disponovat platnými certifikáty nebo hodnoceními z jiných certifikačních schémat. Příkladem jsou certifikáty dle Společných kritérií (ISO 15408), EUCC, ISO/IEC 27001 pro systémy řízení bezpečnosti informací (ISMS) nebo hodnocení dle EN 17640 (FitCEM).

Aby se zabránilo duplicitě hodnotících činností a snížily se náklady na certifikaci, schéma EUDIW-CZ umožňuje opětovné využití existujících informací o záruce za předpokladu, že tyto informace splňují kritéria přijatelnosti definovaná v této příloze. Přijetí existujícího certifikátu se rozumí jako strukturovaný důkaz, který může být použit jako vstup do certifikačního rozhodnutí — nikoli jako automatické uznání plné shody řešení peněženky.

Kritéria přijatelnosti se zakládají na analýze závislostí (dependency analysis) dle přílohy B normy CEN TS 18072, která vyžaduje, aby CB pro každý předložený důkaz posoudil tři dimenze:

- (a) důvěryhodnost a akreditaci vydavatele,
- (b) rozsah existujícího certifikátu ve vztahu k potřebám schématu EUDIW-CZ a
- (c) úroveň záruky a rozsah provedených hodnotících činností.

Pokud analýza závislostí identifikuje mezery v pokrytí, CB stanoví zbytkové hodnotící činnosti nutné k jejich pokrytí.

IX.2 Rozsah přílohy

Tato příloha pokrývá následující oblasti:

- (a) metodu analýzy závislostí používanou CB při posuzování přijatelnosti informací o záruce (kapitola IX.3 Metoda analýzy závislostí);

(b) postup posouzení dostupnosti dokumentace o záruce předložené žadatelem o certifikaci (kapitola IX.4 Posouzení dostupnosti dokumentace o záruce);

(c) postup posouzení záruky ve vztahu k individuálním požadavkům schématu, včetně určení zbytkových hodnotících činností (kapitola IX.5 Posouzení záruky ve vztahu k individuálním požadavkům);

(d) specifická kritéria přijatelnosti pro uznávaná certifikační schémata:

- EUCC,
- CC/SOG-IS,
- EN 17640 (FitCEM),
- QSCD dle čl. 30 eIDAS — prostřednictvím podkladového hodnocení dle Společných kritérií,
- ISO/IEC 27001,
- SOC 2,
- ETSI EN 319 401;

Mimo rozsah této přílohy jsou:

(a) bezpečnostní požadavky na jednotlivé komponenty — ty jsou definovány v příloze X;

(b) metody a postupy hodnotících činností prováděných CB — ty jsou definovány v příloze XI;

(c) definice obsahu a struktury certifikačního posudku — ta je definována v příloze VII;

IX.3 Metoda analýzy závislostí

IX.3.1 Obecný postup

Za účelem posouzení celkové relevance každého prvku dokumentace o záruce certifikační orgány použijí metodu analýzy závislostí, kterou rozepisuje EUDIW-CZ schéma a která vychází z přílohy B normy CEN TS 18072.

Tam, kde jsou k dispozici specifická kritéria pro uznávaná certifikační schémata (kapitola IX.6 této přílohy), CB tato specifická kritéria použije jako zjednodušení generické metody. Specifická kritéria definují, které kroky generické metody lze vynechat nebo nahradit zjednodušeným postupem — například u EUCC certifikátů není nutné posuzovat odbornou způsobilost a nestrannost vydavatele, protože EUCC vyžaduje akreditaci všech certifikačních orgánů.

Analýza závislostí musí vycházet z posouzení rizik řešení peněženky a systému elektronické identifikace, v jehož rámci jsou služby peněženky poskytovány. Hodnocení musí určit, zda dokumenty o záruce dostupné pro dané řešení jsou dostatečné k poskytnutí záruky odpovídající cílové úrovni záruky „vysoká“ dle eIDAS.

IX.3.2 Dimenze posouzení

Pro každou předloženou informaci o záruce CB posoudí následující tři dimenze:

(a) Vydavatel

CB posoudí důvěryhodnost, odbornou způsobilost a nestrannost subjektu, který informaci o záruce vydal. Posuzuje se zejména:

- akreditace vydavatele u příslušného národního akreditačního orgánu (např. ČIA v případě českých certifikačních orgánů),
- autorizace pro příslušnou úroveň záruky (u EUCC: autorizace pro úroveň „vysoká“ dle nařízení (EU) 2019/881),
- osobní certifikace a odborné kvalifikace vedoucího hodnotitele a členů hodnotícího týmu.

Pokud certifikační schéma, z něhož informace pochází, vyžaduje akreditaci všech certifikačních orgánů (jako je tomu u EUCC), posouzení vydavatele je zjednodušeno — CB ověří pouze platnost akreditace a autorizace k datu hodnocení.

(b) Rozsah

CB posoudí, zda rozsah existujícího certifikátu nebo hodnocení pokrývá potřeby schématu EUDIW-CZ pro příslušnou komponentu. Posuzuje se zejména:

- vymezení předmětu hodnocení nebo rozsahu certifikace,
- mapování bezpečnostních požadavků existujícího schématu na požadavky přílohy X schématu EUDIW-CZ,
- pokrytí architekturně specifických aspektů a
- pokrytí relevantních hrozeb z registru rizik přílohy X schématu EUDIW-CZ (příloha I CIR 2024/2981 a CZ-specifická rizika CZ-01 až CZ-10).

Pokud existující certifikát spoléhá na profil ochrany (Protection Profile) uvedený v příloze X schématu EUDIW-CZ, mapování na bezpečnostní požadavky schématu je dostupné předem a CB nemusí provádět individuální mapování. Pokud certifikát spoléhá na jiný bezpečnostní cíl (Security Target), CB musí vytvořit explicitní mapování mezi bezpečnostními funkčními požadavky (SFR) uvedenými v bezpečnostním cíli a požadavky přílohy X schématu EUDIW-CZ.

(c) Záruka

CB posoudí, zda úroveň záruky a rozsah provedených hodnotících činností jsou dostatečné pro úroveň záruky „vysoká“ vyžadovanou schématem EUDIW-CZ. Posuzuje se zejména:

- úroveň hodnocení zranitelností (např. u CC/EUCC: úroveň AVA_VAN.5 pro WSCA v architektuře vzdáleného HSM (AVA_VAN.3 s přidáním dodatečných provozních opatření uvedených v příloze X schématu EUDIW-CZ)),
- hloubka a pokrytí funkčního testování,
- posouzení provozní účinnosti bezpečnostních opatření všech IKT služeb dle sekce 7.4.4.2.2.3 CEN TS 18072 (prověřování dodavatelského řetězce) a zda byly zjištěny a řešeny zranitelnosti nebo neshody, které mohou být problematické při použití komponenty v kontextu řešení peněženky.

IX.3.3 Identifikace mezer v pokrytí a zbytkových činností

Existující informace o záruce je uznávána výhradně v rozsahu a úrovni záruky, které skutečně atestuje. CB nesmí vlastním úsudkem přiznat záruku aspektům, které nebyly předmětem atestace existujícího certifikátu nebo hodnocení. Identifikace mezery v pokrytí proto neznamená akceptaci neúplného důkazu: nepokrytá část požadavku je vždy předmětem zbytkových hodnotících činností, které CB provede jako vlastní hodnocení dle metod přílohy XI schématu. Pokud mezeru v pokrytí nelze zbytkovými hodnotícími činnostmi pokrýt, informace o záruce se pro daný požadavek odmítne a provede se plné nové hodnocení (kapitola IX.5.3 písm. f)).

Pokud analýza závislostí identifikuje mezery v pokrytí v některé z výše uvedených dimenzí, CB stanoví zbytkové hodnotící činnosti potřebné k doplnění existující informace o záruce. Tyto zbytkové činnosti typicky zahrnují:

- ověření integrace a konfigurace komponenty v rámci celkového řešení peněženky,
- ověření, že poskytovatel služby IKT dodržuje provozní pokyny (*Operational user guide*) a přípravné postupy (*Preparative procedures*) poskytnuté s certifikovanou komponentou,
- posouzení systémové úrovně záruky (tj. aspektů, které nejsou pokryty na úrovni jednotlivé komponenty — např. interakce mezi komponentami, end-to-end bezpečnostní vlastnosti) a ověření, že v hodnotící technické zprávě (ETR) certifikované komponenty nebyly identifikovány problémy, které by mohly být problematické při použití komponenty v kontextu řešení peněženky.

CB zdokumentuje výsledky analýzy závislostí v certifikačním posudku dle přílohy VII schématu EUDIW-CZ. Dokumentace musí pro každou komponentu obsahovat:

- identifikaci předložené informace o záruce,
- výsledky posouzení ve všech třech dimenzích (vydavatel, rozsah, záruka),
- identifikované mezery v pokrytí a odpovídající zbytkové hodnotící činnosti a
- závěr o přijatelnosti informace o záruce (přijato / přijato s podmínkami / odmítnuto).

IX.3.4 Aktuálnost informací o záruce

Informace o záruce musí být aktuální. CB ověří platnost certifikátu nebo hodnocení k datu posouzení a zohlední výsledky průběžného dozoru nad existujícím certifikátem. Pokud existující certifikát vypršel nebo je v procesu obnovy, CB posoudí, zda je k dispozici překlenovací dopis (bridge letter) nebo obdobné prohlášení pokrývající přechodné období. Pokud takové prohlášení není k dispozici a certifikát je neplatný, informaci o záruce nelze přijmout.

CB zohlední také známé zranitelnosti zveřejněné po datu vydání existujícího certifikátu, které se týkají certifikované komponenty. Pokud takové zranitelnosti existují a nebyly řešeny v rámci průběžného dozoru nad existujícím certifikátem, CB stanoví dodatečné zbytkové hodnotící činnosti zaměřené na posouzení dopadu těchto zranitelností na řešení peněženky.

IX.3.5 Kompozice v rámci schématu EUDIW-CZ

V případě, že služba a její dílčí služba jsou obě certifikovány v rámci schématu EUDIW-CZ (tj. jedná se o kompozici v rámci jednoho schématu, nikoli o přepoužití z externího schématu), CB může postup analýzy závislosti dále zjednodušit. V takovém případě jsou relevantní informace zpravidla obsaženy ve zprávách vydaných s existujícím certifikátem EUDIW-CZ a CB nemusí provádět plný postup dle IX.3.1 Obecný postup až IX.3.4 Aktuálnost informací o záruce.

V případě kompozice s komponentou certifikovanou v rámci evropského certifikačního schématu kybernetické bezpečnosti (zejména EUCC), CB provádějící hodnocení služby IKT a CB, který provedl hodnocení certifikované komponenty, si vzájemně sdílejí relevantní informace potřebné pro analýzu závislostí.

IX.4 Posouzení dostupnosti dokumentace o záruce

IX.4.1 Inventarizace dokumentace

Hodnotitelé uvedou seznam dokumentace o záruce dostupné pro každou relevantní komponentu řešení peněženky a systému elektronické identifikace, v jehož rámci je peněženka poskytována. Seznam se sestavuje na základě podkladů předložených žadatelem o certifikaci v souladu s přílohou IV schématu (informace požadované při podání žádosti o certifikaci), zejména bod týkající se seznamu existujících certifikátů a hodnocení.

Hodnotitelé poté posoudí celkovou relevanci každého dokumentu o záruce pro přezkum závislostí.

Výsledkem inventarizace je strukturovaný soupis, který pro každou komponentu řešení peněženky uvádí:

- identifikaci komponenty dle přílohy X (např. WSCD, WSCA, instance peněženky, backend poskytovatele, ISMS procesy),
- dostupnou dokumentaci o záruce přiřazenou k dané komponentě a
- předběžné posouzení relevance každého dokumentu.

IX.4.2 Aspekty posouzení dokumentace

V analýze se zohlední následující aspekty:

(1) O dokumentaci o záruce samotné:

(a) Typ dokumentace o záruce s veškerými požadovanými podrobnostmi. Například:

- certifikáty shody dle EN ISO/IEC 27001:2022,
- zprávy ISAE typu 1 nebo typu 2,
- certifikáty EUCC s přiloženou hodnotící technickou zprávou (ETR),
- certifikáty CC/SOG-IS,
- zprávy o hodnocení dle EN 17640 (FitCEM) nebo dle národních schémat (CSPN, BSZ, LINCE, BSZA),
- zprávy o posouzení shody dle ETSI EN 319 401 / EN 319 403-1,
- zprávy SOC 2 typu I nebo typu II,
- atestace dle zákona 250/2017 Sb.

(b) Pokryté období nebo doba platnosti. Toto období může být doplněno překlenovacím dopisem nebo podobným prohlášením pokrývajícím přechodné období mezi koncem platnosti stávající zprávy a vydáním nové. CB posoudí, zda pokryté období zahrnuje datum hodnocení. Pokud certifikát vypršel a překlenovací dopis není k dispozici, dokument nelze přijmout jako platný vstup do analýzy závislostí (viz kapitola IX.3.4 Aktuálnost informací o záruce).

(c) Příslušný rámec — certifikační nebo hodnotící schéma, norma nebo technická specifikace, podle které byl dokument vydán (např. EUCC dle nařízení (EU) 2024/482, EN ISO/IEC 27001:2022, ETSI EN 319 401 v3.2.1, EN 17640).

(d) Zda dokumentace o záruce obsahuje mapování na požadavky schématu EUDIW-CZ. Pokud takové mapování není součástí dokumentace, CB posoudí, zda je mapování dostupné z jiného zdroje (např. z profilu ochrany uvedeného v příloze X schématu) nebo zda jej musí CB vytvořit jako součást analýzy závislostí.

(2) O odborné způsobilosti a nestrannosti vydavatele zprávy o záruce:

(a) Název certifikačního orgánu a, pokud je k dispozici, jméno vedoucího hodnotitele a členů hodnotícího týmu.

(b) Důkaz o odborné způsobilosti certifikačního orgánu a hodnotitele. Jako důkaz se přijímá zejména:

- akreditace u národního akreditačního orgánu (v České republice ČIA) pro příslušný rozsah,
- autorizace pro úroveň záruky „vysoká“ (u EUCC: dle nařízení (EU) 2019/881),
- osobní certifikace hodnotitelů (např. certifikace Common Criteria, certifikace ISMS auditorů dle ISO/IEC 27006),

- zápis v registru kvalifikovaných auditorů QTSP (u auditů dle ETSI EN 319 403-1).

(c) Důkaz o nestrannosti certifikačního orgánu a hodnotitele. Akreditace certifikačního orgánu dle příslušné normy řady EN ISO/IEC 17000 nebo dle příslušného sektorového akreditačního schématu (podle typu vydané dokumentace - např. EN ISO/IEC 17065 pro certifikaci produktů či služeb, EN ISO/IEC 17021-1 pro certifikaci systémů řízení, EN ISO/IEC 17025 pro testování, EN ISO/IEC 17020 pro inspekci, ETSI EN 319 403-1 pro audit poskytovatelů služeb vytvářejících důvěru) zahrnuje posouzení nestrannosti jako součást akreditačního procesu, a proto je pro akreditované subjekty dostačujícím důkazem. U neakreditovaných subjektů CB posoudí nestrannost individuálně.

IX.5 Posouzení záruky ve vztahu k individuálním požadavkům

IX.5.1 Obecný postup

Hodnotitelé ověří, že dokumentace o záruce je dostupná pro řešení peněženky a systém elektronické identifikace, v jehož rámci je peněženka poskytována, a že je přiměřená k tomu, aby bylo možné určit, že řešení peněženky splňuje očekávání vztahující se k individuálním požadavkům certifikačního schématu EUDIW-CZ definovaným v příloze X.

Toto posouzení se provede pro každou relevantní komponentu řešení peněženky a systému elektronické identifikace tak, že hodnotící tým formuluje předpoklad o bezpečnostních opatřeních řešení peněženky. Předpoklad vyjadřuje, jaká bezpečnostní opatření musí být zavedena, aby byl příslušný požadavek přílohy X splněn. Například, „WSCD zajišťuje generování a uložení kryptografických klíčů v bezpečném prostředí s úrovní odolnosti proti útokům odpovídající AVA_VAN.5.“

Pro každý takový předpoklad hodnotící tým určí, zda je záruka poskytnutá v dostupné dokumentaci o záruce přiměřená.

IX.5.2 Kritéria přiměřenosti

Určení, že záruka je přiměřená, se zakládá na jednom z následujících čtyř scénářů. Ve všech níže uvedených scénářích se existující informace o záruce uznává pouze v rozsahu a úrovni záruky, které skutečně atestuje (kapitola IX.3.3). Scénáře (2) až (4) neznamenalí akceptaci neatestovaných aspektů, ale určují zbytkové hodnotící činnosti, jimiž CB nepokryté aspekty hodnotí sám:

(1) **Plné pokrytí:** požadovaná informace je dostupná v dokumentaci o záruce s očekávanou úrovní záruky. Existující certifikát nebo hodnocení plně pokrývá příslušný požadavek přílohy X a nebyly identifikovány žádné mezery v rozsahu ani v úrovni záruky. V tomto případě CB neprovádí žádné zbytkové hodnotící činnosti ve vztahu k danému požadavku.

Příklad: “Certifikát EUCC pro HSM provozovaný u poskytovatele cloudu, vydaný na základě profilu ochrany uvedeného v příloze X, plně pokrývá požadavky WSCD-01 až WSCD-04 přílohy X” (mapování SFR na požadavky schématu je dostupné z profilu ochrany).

(2) **Částečné pokrytí s kompenzačními opatřeními:** Informace dostupná v dokumentaci o záruce nepokrývá plný rozsah požadavku (mezera v pokrytí), avšak v řešení peněženky nebo v systému elektronické identifikace jsou zavedena doplňková opatření nebo kompenzační opatření (tj. vnitřní opatření snižující riziko existující nebo potenciální slabiny). Informace o záruce se uznává pouze pro rozsah, který skutečně atestuje; přiměřenost pro zbývajících rozsah požadavku není výsledkem úsudku CB nad existujícím certifikátem, ale výsledkem zbytkových hodnotících činností, jimiž CB ověří existenci a účinnost kompenzačních opatření. Provedené zbytkové činnosti a jejich závěr CB zdokumentuje v certifikačním posudku. Pokud účinnost kompenzačních opatření nelze prokázat, informace o záruce se pro daný požadavek odmítne.

Příklad: “Certifikát ISO/IEC 27001 poskytovatele peněženky pokrývá obecné požadavky ISMS, ale neobsahuje specifické opatření pro řízení zranitelnosti WSCA dle požadavku VUL-05 přílohy X. Poskytovatel peněženky zavedl doplňkový proces pro sledování CVE a aktualizací WSCA” (CB ověří účinnost tohoto procesu jako zbytkovou hodnotící činnost).

(3) **Nižší úroveň záruky s monitorovacími opatřeními:** Informace dostupná v dokumentaci o záruce nenabízí očekávanou úroveň záruky (mezera v úrovni záruky). Tento scénář je typický pro situace, kdy existující hodnocení bylo provedeno na nižší úrovni záruky (např. „značná“ místo „vysoká“). Informace o záruce se uznává jen pro úroveň záruky, kterou skutečně atestuje. Rozdíl vůči očekávané úrovni záruky musí kompenzovat dodatečné monitorovací mechanismy poskytovatele peněženky. CB ověří, že tyto mechanismy existují a fungují, jako zbytkovou hodnotící činnost, a závěr s odůvodněním zapíše do certifikačního posudku. Pokud monitorovací mechanismy rozdíl v úrovni záruky nekompensují, CB informaci o záruce pro daný požadavek odmítne.

Příklad: “Hodnocení instance peněženky dle OWASP MASVS Level 2 (úroveň CSA „značná“ jako prozatímní alternativa k FitCEM dle WIN-03 přílohy X)” — CB posoudí, zda monitorovací opatření poskytovatele (detekce integrity, monitorování chování aplikace, reakce na incidenty) kompenzují rozdíl mezi úrovněmi „značná“ a „vysoká“.

(4) **Neshody s nápravnými opatřeními:** V případě, že dokumentace o záruce odhalí nesoulad mezi navrženým opatřením a skutečným plněním předpokladů, musí poskytovatel peněženky zavést nápravná opatření. Tato opatření musí být dostatečná k tomu, aby garantovala splnění všech požadavků. Úlohou CB je pak v rámci závěrečného hodnocení prověřit, zda jsou tato opatření funkční, a toto potvrzení uvést v certifikačním posudku.

Příklad: “Zpráva o posouzení shody poskytovatele pečetící služby identifikovala neshodu v konfiguraci řízení přístupu k podpisovým klíčům. QTSP zavedl nápravná opatření (zprůsnění pravidel RBAC a přidání principu čtyř očí)”. CB ověří implementaci nápravného opatření jako součást zbytkové hodnotící činnosti.

IX.5.3 Postup ověřování shody s požadavky

CB provede posouzení (dle kapitol IX.5.1 Obecný postup - IX.5.2 Kritéria přiměřenosti) systematicky pro každý požadavek přílohy X, přičemž využije matici trasovatelnosti (příloha X.B) jako strukturální nástroj. Pro každý požadavek CB zaznamená:

- (a) identifikátor požadavku (např. WSCD-01, CRY-02, ACC-01);
- (b) komponentu architektury, ke které se požadavek vztahuje;
- (c) identifikaci relevantní dokumentace o záruce z inventáře (kapitola IX.4 Posouzení dostupnosti dokumentace o záruce);
- (d) scénář přiměřenosti (1) až (4) dle odstavce IX.5.2 Kritéria přiměřenosti;
- (e) v případě scénářů (2), (3) nebo (4) — popis kompenzačních opatření, monitorovacích mechanismů nebo nápravných opatření a identifikaci odpovídajících zbytkových hodnotících činností;
- (f) v případě, že žádný ze scénářů (1) až (4) není splněn — závěr, že existující dokumentace o záruce je pro daný požadavek nedostatečná a je potřeba plné nové hodnocení.

IX.5.4 Zjednodušení pro certifikované komponenty

Pokud komponenta byla certifikována v rámci certifikačního schématu uznaného schématem EUDIW-CZ (viz kapitola IX.6 Specifická kritéria pro certifikované komponenty), postup definovaný v kapitolách IX.5.1 až IX.5.3 se zjednoduší uplatněním specifických kritérií:

- (a) Odborná způsobilost a nestrannost certifikačního orgánu, který komponentu certifikoval, nemusí být posuzována, pokud příslušné certifikační schéma vyžaduje akreditaci.
- (b) Zpráva o hodnocení může být považována za plně vyhovující pravidlům příslušného certifikačního schématu pro úroveň záruky uvedenou v certifikátu.
- (c) Mapování bezpečnostních požadavků příslušného certifikačního schématu na bezpečnostní požadavky schématu EUDIW-CZ může být provedeno jednou a opětovně použito pro všechny certifikáty vydané na základě téhož profilu ochrany nebo bezpečnostního cíle.

I v případě certifikovaných komponent CB vždy provede ověření integrace a konfigurace, tj. ověří, že poskytovatel služby IKT dodržuje provozní pokyny a přípravné postupy poskytnuté s certifikovanou komponentou, a ověří obsah hodnotící technické zprávy (ETR) za účelem vyloučení problémů identifikovaných během hodnocení, které by mohly být problematické v kontextu řešení peněženky (viz kapitola IX.3.3 Identifikace mezer v pokrytí a [zbytkových činností](#)).

IX.5.5 Výstup posouzení

Výstupem posouzení dle této kapitoly je strukturovaná tabulka (nebo součást certifikačního posudku dle přílohy VII EUDIW-CZ schématu), která pro každý požadavek přílohy X schématu uvádí výsledek posouzení přiměřenosti a identifikaci zbytkových hodnotících činností. Tato tabulka je klíčovým vstupem pro plánování hodnotících činností CB dle přílohy XI schématu a představuje hlavní nástroj řízení nákladů certifikace — přesná definice přijatelnosti existujících důkazů v této kapitole přímo určuje rozsah činností, které musí CB provést znovu.

IX.6 Specifická kritéria pro certifikované komponenty

Tato kapitola definuje specifická kritéria přijatelnosti pro certifikační schémata uznaná schématem EUDIW-CZ. Pro každé uznané schéma jsou specifikována kritéria ve třech dimenzích analýzy závislosti (vydavatel, rozsah, záruka) dle kapitoly IX.3.2 Dimenze posouzení, doplněná o identifikaci zbytkových hodnotících činností.

Struktura kritérií vychází z přílohy II CIR (EU) 2024/2981 (tabulka „Kritéria pro posouzení přijatelnosti informací o záruce“), která definuje normativní základ pro uznávaná schémata.

Schéma EUDIW-CZ uznává schémata uvedená v příloze II CIR (EU) 2024/2981 a dále schémata, která jsou pro architekturu schématu relevantní a splňují podmínky kapitoly IX.6.9. Schémata neuvedená v příloze II jsou v následujícím výčtu označena. Schéma EUDIW-CZ v souladu s uvedeným uznává následující schémata:

- (a) EUCC — Evropský systém certifikace kybernetické bezpečnosti dle nařízení (EU) 2024/482 (kapitola IX.6.1 EUCC — Evropský systém certifikace kybernetické bezpečnosti);
- (b) CC/SOG-IS — systémy založené na společných kritériích provozované v EU, včetně systémů výboru SOG-IS (kapitola IX.6.2 CC (SOG-IS) — Systémy založené na společných kritériích);
- (c) EN 17640 (FitCEM) — včetně národních schémat CSPN, BSZ, LINCE, BSZA (kapitola IX.6.3 EN 17640 (FitCEM) — včetně CSPN, BSZ, LINCE, BSZA);
- (d) Certifikace QSCD dle článku 30 nařízení (EU) č. 910/2014 - výhradně prostřednictvím podkladového hodnocení dle Společných kritérií (kapitola IX.6.4 Certifikace QSCD dle článku 30 eIDAS);
- (e) EN ISO/IEC 27001:2022 — ISMS (kapitola IX.6.5 EN ISO/IEC 27001:2022 — ISMS);
- (f) SOC 2 — zprávy o organizačních kontrolách (kapitola IX.6.6 SOC 2 — Organizace);
- (g) ETSI EN 319 401 — **IX.6.7 ETSI EN 319 401 — Posouzení shody dle eIDAS auditního rámce** posouzení shody dle eIDAS auditního rámce (kapitola IX.6.7);
- (h) Atestace dle zákona 250/2017 Sb. a zákona 365/2000 Sb. a vyhlášky č. 529/2006 Sb.

(i) Jiné systémy — záchytná kategorie pro budoucí schémata (kapitola IX.6.9 Jiné systémy).

Uznání schématu v této kapitole se vždy vztahuje ke komponentě řešení peněženky, pro kterou dané schéma poskytuje relevantní informaci o záruce. Neznamená, že služba, pro kterou bylo dané schéma původně určeno, spadá do rozsahu certifikace dle přílohy I schématu.

Schéma EUCS (*European cybersecurity certification scheme for cloud services*) je uvedeno v příloze II CIR 2024/2981 s poznámkou „je-li k dispozici“. K datu vydání této verze schématu EUDIW-CZ nebylo schéma EUCS přijato, a proto pro něj nejsou definována specifická kritéria. Po přijetí EUCS budou kritéria doplněna formou aktualizace této přílohy.

Struktura každé podkapitoly následuje jednotný formát:

- (1) Identifikace schématu a normativní základ;
- (2) Předmět certifikace a aplikovatelné komponenty CZ architektury;
- (3) Kontrola vydavatele — kritéria pro posouzení odborné způsobilosti a nestrannosti;
- (4) Kontrola rozsahu — kritéria pro posouzení pokrytí požadavků schématu EUDIW-CZ;
- (5) Kontrola záruky — kritéria pro posouzení úrovně záruky a provedených činností;
- (6) Zbytkové hodnotící činnosti — činnosti, které CB musí provést i v případě přijatelného existujícího certifikátu;

IX.6.1 EUCC — Evropský systém certifikace kybernetické bezpečnosti

Identifikace a normativní základ:

EUCC je evropský systém certifikace kybernetické bezpečnosti pro produkty IKT, zřízený prováděcím nařízením Komise (EU) 2024/482 na základě aktu o kybernetické bezpečnosti (nařízení (EU) 2019/881). EUCC vychází z ISO/IEC 15408 (Common Criteria) a definuje strukturovaný postup hodnocení a certifikace produktů IKT a profilů ochrany na dvou úrovních záruky — „značná“ a „vysoká“.

Předmět certifikace a CZ komponenty:

EUCC certifikuje produkty IKT. V kontextu české architektury EUDIW-CZ se EUCC certifikáty uplatní primárně na následující komponenty:

- (a) WSCD — certifikát vydaný výrobcem HSM na základě profilu ochrany pro WSCD (např. EN 419 221-5);
- (b) WSCA — pokud je WSCA hodnocena dle Common Criteria / EUCC na základě profilu ochrany pro WSCA (CEN TC224 WG17, v současnosti PP Wallet Instance draft v0.6 / PP Wallet Unit draft v0.4);

(c) Případně další produktové komponenty, pokud jsou certifikovány dle EUCC (např. TEE, secure element).

EUCC certifikáty se přijímají výhradně jako důkazy na úrovni komponenty. Nelze je použít jako implicitní certifikaci celého řešení peněženky.

(1) Kontrola vydavatele:

Odborná způsobilost a nestrannost certifikačního orgánu (CAB), který EUCC certifikát vydal, nemusí být posuzována. EUCC vyžaduje akreditaci všech CAB dle ISO/IEC 17065 a ISO/IEC 17025, přičemž pro hodnotící činnosti na úrovni záruky „vysoká“ je navíc vyžadována autorizace dle nařízení (EU) 2019/881. Národní akreditační orgány (NAB) dohlíží na shodu CAB. Vzájemné hodnocení (peer assessment) CAB je povinné každých pět let.

CB schématu EUDIW-CZ ověří pouze platnost akreditace a autorizace k datu hodnocení.

(2) Kontrola rozsahu:

(a) CB ověří profil ochrany (Protection Profile, PP) a bezpečnostní cíl (Security Target, ST), na jejichž základě byl certifikát vydán.

(b) Pokud EUCC certifikát spoléhá na jeden z profilů ochrany uvedených v příloze X schématu EUDIW-CZ (PP WSCD, PP WSCA), není nutné provádět individuální mapování na bezpečnostní požadavky schématu — mapování je dostupné přímo z profilu ochrany.

(c) Pokud EUCC certifikát spoléhá na jiný bezpečnostní cíl (ST), který není přímo navázán na PP uvedený v příloze X, CB musí vytvořit explicitní mapování mezi bezpečnostními funkčními požadavky (SFR) uvedenými v ST a požadavky přílohy X schématu EUDIW-CZ.

(d) CB ověří úroveň záruky hodnocení a použitá rozšíření (extensions). Pro schéma EUDIW-CZ je relevantní zejména úroveň hodnocení zranitelností (AVA_VAN). CIR (EU) 2024/2981 výslovně předpokládá analýzu úrovně AVA_VAN pro určení míry, do jaké EUCC certifikovaná komponenta splňuje požadavky úrovně záruky dle nařízení (EU) 2024/1183 (eIDAS 2.0). Pro WSCD schéma EUDIW-CZ vyžaduje minimálně EAL4+ AVA_VAN.5. Pro WSCA provozovanou v architektuře se vzdáleným WSCD je minimální přijatelnou úrovní AVA_VAN.3, a to výhradně za kompenzačních podmínek dle požadavku WSA-06 přílohy X. Splnění těchto podmínek CB ověří a zdokumentuje v certifikačním posudku.

(3) Kontrola záruky:

(a) Zpráva o hodnocení EUCC může být považována za dostatečnou. Úroveň AVA_VAN použitá při hodnocení zranitelností poskytuje dodatečnou indikaci pro určení míry splnění požadavků úrovně záruky „vysoká“ dle eIDAS.

(b) CB ověří omezení uvedená v uživatelské dokumentaci (Operational user guide, Preparative procedures) certifikované komponenty — tato omezení mohou definovat podmínky, za kterých je certifikát platný, a CB musí ověřit, že tyto podmínky jsou v české architektuře splněny.

(c) V případě kompozice (tj. certifikovaná komponenta je součástí většího řešení) může být vyžadován přístup k hodnotící technické zprávě (Evaluation Technical Report, ETR) za účelem ověření, že během hodnocení nebyly identifikovány problémy, které by mohly být problematické při použití komponenty v kontextu řešení peněženky.

(4) Zbytkové hodnotící činnosti:

I v případě přijatelného EUCC certifikátu CB provede následující zbytkové činnosti:

(a) Poskytovatel služby IKT (wallet provider) předloží odůvodnění, že jeho služba IKT dodržuje pokyny poskytnuté s EUCC certifikovanou komponentou (Operational user guide a Preparative procedures).

(b) CB ověří odůvodnění předložené poskytovatelem služby IKT.

(c) CB ověří obsah CR (Certification Report) EUCC certifikovaného produktu, aby zajistil, že během hodnocení nebyly identifikovány problémy, které by mohly být problematické při použití komponenty v kontextu řešení peněženky.

(d) Systémová integrace — CB posoudí správnost integrace a konfigurace certifikované komponenty v rámci celkového řešení peněženky, včetně interakcí mezi komponentami (např. rozhraní WSCA–WSCD, komunikační kanály instance peněženky s backendem).

(e) Organizační povinnosti — povinnosti na úrovni poskytovatele peněženky (governance, řízení rizik, řízení incidentů, dozorové požadavky) spadají mimo rozsah EUCC hodnocení na úrovni produktu a musí být posouzeny plně v rámci schématu EUDIW-CZ.

(f) Životní cyklus — CB rozliší mezi životním cyklem produktu/komponenty (pokrytým EUCC certifikátem) a životním cyklem řešení peněženky (pokrytým schématem EUDIW-CZ). Řízení změn, aktualizací a zranitelností na úrovni řešení peněženky vyžaduje samostatné posouzení.

(5) CZ-specifické poznámky:

(a) WSCD: Očekává se využití existujícího EUCC nebo CC/SOG-IS certifikátu předloženého výrobcem HSM. CB ověří, že PP použitý při certifikaci odpovídá PP uvedenému v příloze X a že provozní podmínky jsou kompatibilní s nasazením v prostředí poskytovatele cloudu. Zvláštní pozornost se věnuje topologii vzdáleného HSM — WSCA neběží uvnitř HSM, ale na přilehlém serveru (dedikovaném aplikačním serveru). CB posoudí, zda bezpečnostní předpoklady certifikátu HSM jsou v tomto nasazení splněny (zejména předpoklady o fyzickém a logickém zabezpečení komunikačního kanálu WSCA–HSM).

(b) WSCA: WSCA v architektuře vzdáleného HSM (WSCA běžící na serveru přilehlém k HSM, nikoli uvnitř HSM) se hodnotí minimálně na úrovni AVA_VAN.3 dle EUCC, za kompenzačních podmínek požadavku WSA-06 přílohy X. Odůvodnění přijatelnosti této úrovně (eliminace vektorů fyzického útoku provozním prostředím, soulad s přílohou V CIR (EU) 2024/2981) musí být zdokumentováno v certifikačním posudku.

(c) Pravidla pro kompozici: Pokud jsou WSCD i WSCA certifikovány dle EUCC a oba certifikáty spoléhají na PP uvedené v příloze X, pravidla pro kompozici jsou definována přímo v profilu ochrany a CB nemusí provádět individuální analýzu kompozice. V opačném případě CB provede plnou analýzu závislostí dle kapitoly IX.3 Metoda analýzy závislostí.

(d) Platnost certifikátu: EUCC certifikáty jsou platné po dobu pěti let a podléhají kontinuálnímu řízení zranitelností. CB ověří, že certifikát je platný k datu hodnocení a že nebyly identifikovány neřešené zranitelnosti, které by mohly ovlivnit bezpečnost řešení peněženky.

IX.6.2 CC (SOG-IS) — Systémy založené na společných kritériích

Identifikace a normativní základ:

Tato podkapitola pokrývá systémy založené na společných kritériích dle ISO/IEC 15408, provozované členskými státy EU, včetně systémů v rámci dohody o vzájemném uznávání výboru SOG-IS (SOG-IS Mutual Recognition Agreement, SOG-IS MRA). SOG-IS MRA umožňuje vzájemné uznávání CC certifikátů mezi signatářskými státy až do úrovně EAL4 (obecně) a do EAL7 pro vybrané technické domény (smart cards, HW zařízení).

Poznámka: Mohou být uznány pouze certifikáty v případě, že hodnotící laboratoř i certifikační orgán jsou usazeny v členském státě Evropské unie, resp. v Evropském hospodářském prostoru.

CIR (EU) 2024/2981 příloha II uvádí „Systémy založené na společných kritériích provozované v EU, včetně systémů výboru SOG-IS“ jako uznané schéma.

Předmět certifikace a CZ komponenty:

CC/SOG-IS certifikuje produkty IKT. V kontextu české architektury EUDIW-CZ se CC/SOG-IS certifikáty uplatní jako alternativa k EUCC primárně na:

- (a) WSCD — pro případy, kdy výrobce HSM disponuje CC/SOG-IS certifikátem, který předchází přijetí EUCC nebo byl vydán v rámci SOG-IS technické domény „Hardware Devices with Security Boxes“;
- (b) WSCA — pokud je WSCA certifikována dle CC v členském státě, který je signatářem SOG-IS MRA, na základě PP odpovídajícího PP WSCA uvedenému v příloze X schématu.

Vztah k EUCC: EUCC je z hlediska schématu EUDIW-CZ preferovaným schématem pro certifikaci produktových komponent, protože zajišťuje jednotný rámec akreditace CAB, autorizace pro úroveň „vysoká“

a průběžné řízení zranitelností na úrovni EU. CC/SOG-IS certifikáty jsou akceptovatelné jako alternativa za podmínek specifikovaných níže.

(1) Kontrola vydavatele:

Certifikáty CC/SOG-IS jsou vydávány národními certifikačními autoritami (NCCA) členských států, tj. subjekty s veřejnoprávním mandátem. V kontextu SOG-IS MRA není vyžadováno dodatečné posouzení odborné způsobilosti a nestrannosti vydavatele, protože certifikační proces je řízen státním orgánem a hodnocení provádějí ITSEF (IT Security Evaluation Facilities) akreditované příslušným NAB.

CB schématu EUDIW-CZ ověří, že:

(a) certifikát byl vydán NCCA členského státu EU, který je signatářem SOG-IS MRA (případně signatářem CCRA pro úroveň do EAL2);

(b) hodnotící laboratoř (ITSEF) byla akreditována příslušným NAB dle ISO/IEC 17025;

(c) pokud certifikát vyžaduje úroveň záruky odpovídající „vysoká“ dle eIDAS (tj. AVA_VAN.5 nebo odůvodněně AVA_VAN.3), hodnocení spadá do technické domény uznávané v rámci SOG-IS MRA.

(2) Kontrola rozsahu:

(a) CB ověří profil ochrany (PP) a bezpečnostní cíl (ST), na jejichž základě byl certifikát vydán.

(b) Pokud CC/SOG-IS certifikát spoléhá na PP uvedený v příloze X schématu EUDIW-CZ (PP WSCD, PP WSCA), mapování na bezpečnostní požadavky schématu je dostupné přímo z profilu ochrany a individuální mapování není vyžadováno.

(c) Pokud certifikát spoléhá na jiný ST, CB musí vytvořit explicitní mapování mezi SFR uvedenými v ST a požadavky přílohy X schématu EUDIW-CZ. Toto mapování může být provedeno jednou a opětovně použito pro všechny certifikáty vydané na základě téhož ST.

(d) CB ověří úroveň záruky hodnocení (EAL) a použitá rozšíření, zejména úroveň hodnocení zranitelností (AVA_VAN). Pro WSCD schéma EUDIW-CZ vyžaduje minimálně EAL4+AVA_VAN.5. Pro WSCA provozovanou v architektuře se vzdáleným WSCD je minimální přijatelnou úrovní AVA_VAN.3, a to výhradně za kompenzačních podmínek dle požadavku WSA-06 přílohy X.

(3) Kontrola záruky:

(a) CB ověří omezení uvedená v uživatelské dokumentaci certifikované komponenty (AGD_OPE — *Operational user guidance*, AGD_PRE — *Preparative procedures*). Tato omezení definují provozní podmínky, za kterých je certifikát platný.

(b) V případě kompozice (certifikovaná komponenta je součástí většího řešení) může být vyžadován přístup k hodnotící technické zprávě (ETR). CB ověří, zda ETR neobsahuje zjištění, která by mohla být problematická při použití komponenty v kontextu řešení peněženky.

(c) CB posoudí, zda certifikát pokrývá kryptografické mechanismy v souladu s ECCG ACM (*European Cybersecurity Certification Group — Approved Cryptographic Mechanisms*) nebo SOG-IS ACM (*SOG-IS Crypto Evaluation Scheme — Agreed Cryptographic Mechanisms*). Pokud certifikát odkazuje na kryptografické mechanismy, které nejsou pokryty aktuální verzí ACM, CB identifikuje toto jako mezeru v pokrytí vyžadující zbytkovou hodnotící činnost.

(4) Zbytkové hodnotící činnosti:

Zbytkové činnosti pro CC/SOG-IS certifikáty jsou shodné s činnostmi definovanými pro EUCC v kapitole IX.6.1 EUCC — Evropský systém certifikace kybernetické bezpečnosti, odstavec (4), tj.:

(a) Ověření, že poskytovatel služby IKT dodržuje provozní pokyny a přípravné postupy certifikované komponenty.

(b) Ověření obsahu ETR za účelem vyloučení problémů v kontextu řešení peněženky.

(c) Posouzení systémové integrace a konfigurace.

(d) Posouzení organizačních povinností na úrovni poskytovatele peněženky (mimo rozsah CC/SOG-IS hodnocení produktu).

(e) Rozlišení mezi životním cyklem produktu (pokrytým CC certifikátem) a životním cyklem řešení peněženky.

Navíc pro CC/SOG-IS certifikáty (na rozdíl od EUCC):

(f) CB ověří, zda certifikát podléhá pravidlům pro průběžné řízení zranitelností srovnatelným s EUCC. Některá národní CC schémata nemají formalizovaný proces řízení zranitelností po vydání certifikátu. Pokud takový proces neexistuje nebo je méně přísný než u EUCC, CB provede dodatečné posouzení známých zranitelností zveřejněných po datu certifikace a jejich dopadu na řešení peněženky.

(g) CB ověří platnost certifikátu — CC certifikáty mají obvykle dobu platnosti definovanou vydávající NCCA (typicky 3–5 let). Pokud certifikát vypršel, přijetí není možné bez překlenovacího opatření (viz IX.3.4 Aktuálnost informací o záruce).

IX.6.3 EN 17640 (FitCEM) — včetně CSPN, BSZ, LINCE, BSZA

Identifikace a normativní základ:

EN 17640:2022 (*Fixed-Time Cybersecurity Evaluation Methodology*, FitCEM) je evropská norma vyvinutá v rámci CEN-CENELEC, která umožňuje časově ohraničená hodnocení kybernetické bezpečnosti produktů IKT na úrovních záruky „nízká“, „značná“ a „vysoká“ dle aktu o kybernetické bezpečnosti. FitCEM definuje hodnotící bloky (*evaluation blocks*) zahrnující:

- přezkum dokumentace,
- funkční testování,
- hodnocení zranitelností a
- kryptografickou analýzu,

přizpůsobené rizikovému profilu a cílové úrovni záruky produktu.

FitCEM je základem pro národní certifikační schémata: CSPN (Francie, ANSSI), BSZ (Německo, BSI), LINCE (Španělsko, CCN) a BSPA (Nizozemsko, NCSC-NL). Mezi CSPN a BSZ existuje bilaterální dohoda o vzájemném uznávání.

CIR (EU) 2024/2981 příloha II uvádí „EN 17640:2018 (FITCEM, včetně CSPN, BSZ, LINCE, BSZA)“ jako uznané schéma.

ENISA AHWG vyvíjí specifický profil FitCEM pro instance peněženky EUDI (FitCEM Wallet Instance Protection Profile, v současnosti draft v0.6).

Předmět certifikace a CZ komponenty:

FitCEM certifikuje produkty IKT. V kontextu české architektury EUDIW-CZ se FitCEM hodnocení uplatní primárně na:

(a) Instance peněženky (wallet instance) — mobilní aplikace — toto je primární schéma pro hodnocení wallet instance dle požadavku WIN-07 přílohy X schématu;

(b) Jako prozatímní alternativa k FitCEM je dle WIN-03 přílohy X přijatelné i hodnocení na úrovni OWASP MAS s aplikací testovacích profilů MAS-L2 (Advanced Security) + MAS-R (Resilient Security) + MAS-P (Baseline Privacy) při úrovni záruky CSA „značná“ — v tomto případě se však nejedná o certifikát přijatelný dle této kapitoly, ale o scénář (3) kapitoly IX.5.2 Kritéria přiměřenosti (nižší úroveň záruky s monitorovacími kontrolami).

FitCEM hodnocení se přijímá jako důkaz na úrovni komponenty. Nepokrývá povinnosti poskytovatele peněženky, systémovou integraci ani servisní komponenty.

(1) Kontrola vydavatele:

Na rozdíl od EUCC, kde je akreditace CAB zajištěna rámcem EU, u FitCEM/národních schémat CB schématu EUDIW-CZ musí posoudit certifikační systém a požadavky na certifikační subjekty příslušného národního schématu. Konkrétně:

- (a) CB ověří, že CAB, který hodnocení provedl, je akreditován dle ISO/IEC 17065 a že hodnotící laboratoř je akreditována dle ISO/IEC 17025 příslušným NAB.
- (b) U schémat, kde hodnocení provádí přímo státní certifikační autorita (např. ANSSI u CSPN, BSI u BSZ), je odborná způsobilost a nestrannost zaručena veřejnoprávním mandátem — v tomto případě CB ověří pouze, že se jedná o aktuální schéma provozované příslušným státním orgánem.
- (c) U schémat, kde hodnocení provádějí licencované soukromé laboratoře (ITSEF), CB ověří platnost licence a akreditace laboratoře.

(2) Kontrola rozsahu:

- (a) CB ověří popis produktu (product description), který definuje hranice hodnoceného předmětu (TOE). Pro přijatelnost dle schématu EUDIW-CZ musí TOE odpovídat komponentě definované v příloze X, tj. instanci peněženky s jasně vymezenými rozhraními.
- (b) CB ověří tvrzení o bezpečnosti hodnoceného produktu. Pokud hodnocení bylo provedeno na základě FitCEM Wallet Instance Protection Profile (nebo budoucího finálního PP), mapování na požadavky přílohy X je dostupné přímo z PP a individuální mapování není vyžadováno. Pokud hodnocení bylo provedeno na základě jiného bezpečnostního profilu nebo generického ST, CB musí vytvořit explicitní mapování bezpečnostních tvrzení na požadavky přílohy X.
- (c) CB ověří úroveň záruky hodnocení. Pro schéma EUDIW-CZ je vyžadována minimální úroveň odpovídající AVA_VAN.3 (tedy posouzení zranitelností se zaměřenou analýzou a odolností proti útočníkovi se „zvýšeným základním útokovým potenciálem“). Hodnocení na nižších úrovních (např. „basic“ nebo „značná“ bez ekvivalentu AVA_VAN.3) není přijatelné jako plný důkaz — lze jej přijmout pouze ve scénáři (3) kapitoly IX.5.2 Kritéria přiměřenosti s kompenzačními monitorovacími kontrolami.

(3) Kontrola záruky (assurance check):

- (a) CB ověří provedené hodnotící činnosti a zjištění uvedená ve zprávě o hodnocení. Kontrola zahrnuje: přezkum dokumentace (documentation review block), funkční testování (functional testing block), hodnocení zranitelností (vulnerability assessment block) a kryptografickou analýzu (cryptographic analysis block).
- (b) CB posoudí, zda rozsah a hloubka provedených hodnotících bloků odpovídají požadavkům schématu EUDIW-CZ pro úroveň záruky „vysoká“. FitCEM umožňuje škálování hloubky hodnocení v rámci každého

bloku — CB musí ověřit, že bylo použito škálování odpovídající úrovni „vysoká“ (nikoli „basic“ nebo „značná“).

(c) CB ověří, zda hodnocení zahrnuje testování odolnosti proti útokům na mobilní platformu (reverse engineering, tampering, obfuscation bypass) relevantní pro wallet instance na mobilních zařízeních.

(d) Pokud zpráva o hodnocení obsahuje zjištění (findings) — identifikované zranitelnosti nebo slabiny — CB posoudí, zda byly řešeny nápravnými opatřeními a zda zůstávají residuální rizika přijatelná v kontextu řešení peněženky.

(4) Zbytkové hodnotící činnosti (additional assessment):

(a) Systémová integrace — CB posoudí integraci hodnocené wallet instance s ostatními komponentami řešení peněženky (WSCA, WSCD, backend, onboarding). FitCEM hodnocení pokrývá pouze wallet instance jako izolovaný produkt — interakce s ostatními komponentami jsou mimo rozsah FitCEM.

(b) Shoda s CIR (EU) 2024/2981 — CB ověří, že celkové řešení splňuje požadavky prováděcího nařízení, které nejsou pokryty hodnocením na úrovni produktu (např. požadavky na poskytovatele peněženky, dozorové povinnosti, řízení incidentů).

(c) Verze a konfigurace — CB ověří, že hodnocená verze wallet instance odpovídá verzi nasazené v produkčním prostředí. Pokud od data hodnocení byly provedeny aktualizace, CB posoudí, zda tyto aktualizace ovlivnily bezpečnostní vlastnosti certifikované verze (dle principu „impact analysis“ pro delta hodnocení).

(d) Organizační povinnosti — povinnosti na úrovni poskytovatele peněženky (governance, řízení rizik, secure SDLC, řízení zranitelností wallet instance) spadají mimo rozsah FitCEM hodnocení produktu a musí být posouzeny plně v rámci schématu EUDIW-CZ.

(e) Životní cyklus — rozlišení mezi životním cyklem produktu (pokrytým FitCEM certifikátem, včetně delta hodnocení a re-certifikace) a životním cyklem řešení peněženky (pokrytým schématem EUDIW-CZ).

(5) CZ-specifické poznámky:

(a) Primární schéma pro wallet instance: V české architektuře EUDIW-CZ je FitCEM primárním schématem pro hodnocení mobilní wallet instance. Hodnocení bude pravděpodobně provedeno jako nové hodnocení (nikoli reuse existujícího certifikátu), protože wallet instance je vyvíjena specificky pro český EUDIW.

(b) Volba národního FitCEM schématu: Protože Česká republika nemá vlastní národní schéma založené na EN 17640, hodnocení bude provedeno v rámci zahraničního národního schématu (CSPN, BSZ, LINC nebo BSPA/BSZA) nebo přímo dle EN 17640 zahraničním CAB akreditovaným pro FitCEM. CB schématu EUDIW-CZ

přijme certifikáty z kteréhokoli národního FitCEM schématu uvedeného v příloze II CIR (EU) 2024/2981 za předpokladu splnění kritérií definovaných v odstavcích (1)–(3) výše.

(c) FitCEM Wallet Instance PP: ENISA AHWG v současnosti vyvíjí specifický profil ochrany pro wallet instance (PP Wallet Instance draft v0.6). Po finalizaci tohoto PP bude schéma EUDIW-CZ vyžadovat, aby FitCEM hodnocení wallet instance bylo provedeno na základě tohoto PP nebo na základě bezpečnostního profilu prokazatelně mapovaného na požadavky tohoto PP. Do finalizace PP jsou přijatelná hodnocení na základě generického ST, pokud CB provede explicitní mapování dle odstavce (2)(b).

(d) OWASP MAS jako prozatímní alternativa: Dle WIN-03 přílohy X schématu je hodnocení dle OWASP MAS s aplikací testovacích profilů MAS-L2 + MAS-R + MAS-P (úroveň CSA „značná“) přijatelné jako prozatímní alternativa k FitCEM. Při hodnocení dle OWASP MAS se použije katalog slabín OWASP MASWE jako referenční výčet bezpečnostních slabín, proti kterým jsou prováděny testovací činnosti dle OWASP MASTG. Toto hodnocení však nepředstavuje plný důkaz (scénář (1) kapitola IX.5.2 Kritéria přiměřenosti), ale spadá pod scénář (3) — nižší úroveň záruky s monitorovacími kontrolami. CB v tomto případě stanoví dodatečné zbytkové hodnotící činnosti zaměřené na kompenzaci rozdílu mezi úrovněmi „značná“ a „vysoká“.

(e) Vzájemné uznávání: Mezi CSPN a BSZ existuje bilaterální dohoda o vzájemném uznávání. Pro schéma EUDIW-CZ je toto uznávání transparentní — CB přijme certifikát z kteréhokoli z těchto schémat bez dalšího posouzení vzájemného uznávání.

IX.6.4 Certifikace QSCD dle článku 30 eIDAS

Identifikace a normativní základ:

Podle článku 30 nařízení (EU) č. 910/2014 potvrzují shodu kvalifikovaných prostředků pro vytváření elektronických podpisů a pečeti (QSCD) subjekty určené členskými státy. Potvrzené prostředky jsou uvedeny na seznamu podle článku 31 uvedeného nařízení. Postupy určených subjektů nejsou harmonizovány a potvrzení lze vydat i na základě alternativního procesu podle čl. 30 odst. 3 písm. b). Potvrzení statusu QSCD proto samo o sobě nevypovídá o metodě hodnocení, profilu ochrany ani o dosažené úrovni záruky, a neumožňuje provést analýzu závislostí ve všech třech dimenzích podle kapitoly IX.3.2.

Příloha II CIR (EU) 2024/2981 uvádí systémy certifikace QSCD jako schéma s předmětem certifikace „QSCD“. Schéma EUDIW-CZ tento řádek naplňuje tak, že informací o záruce není potvrzení statusu QSCD, nýbrž podkladové hodnocení dle Společných kritérií, na jehož základě bylo potvrzení vydáno.

Předmět certifikace a CZ komponenty:

Certifikace QSCD se vztahuje na hardwarové a softwarové prostředky pro vytváření elektronických podpisů a pečeti. V kontextu české architektury EUDIW-CZ se doklad o statusu QSCD může vztahovat na tyto komponenty:

- (a) WSCD — vzdálený kryptografický prostředek (typicky hodnocený proti profilu ochrany EN 419 221-5);
- (b) Lokální externí WSCD — pokud je v budoucnu zavedena architektura s lokálním externím WSCD (např. čipová karta), QSCD certifikace na základě PP EN 419 211 je relevantní;
- (c) WSCA provozovaná na serveru v architektuře se vzdáleným WSCD (profil ochrany EN 419 241-2).

IX.6.1 EUCC — Evropský systém certifikace kybernetické bezpečnosti
IX.6.2 CC (SOG-IS) — Systémy založené na společných kritériích
Skutečnost, že tentýž prostředek je současně používán pro poskytování kvalifikované služby vytvářející důvěru, nemá vliv na rozsah certifikace dle přílohy I schématu. Taková služba je mimo rozsah certifikace; certifikační orgán posuzuje výhradně funkce prostředku v roli WSCD, resp. WSCA, podle požadavků přílohy X schématu.

(1) Kontrola vydavatele:

- (a) CB určí, zda potvrzení statusu QSCD vychází z hodnocení dle Společných kritérií (ISO/IEC 15408) provedeného v rámci schématu EUCC podle nařízení (EU) 2024/482, nebo v rámci schématu založeného na Společných kritériích provozovaného v Evropské unii, včetně schémat výboru SOG-IS.
- (b) Pokud ano, informací o záruce je podkladový certifikát dle Společných kritérií. Kontrola vydavatele se provede podle kapitoly IX.6.1, resp. IX.6.2, a nikoli podle této kapitoly.
- (c) Pokud potvrzení statusu QSCD vychází z alternativního procesu podle čl. 30 odst. 3 písm. b) nařízení eIDAS, nebo pokud podkladový certifikát dle Společných kritérií není certifikačnímu orgánu předložen, nelze potvrzení statusu QSCD přijmout jako informaci o záruce. Komponenta se v takovém případě hodnotí v plném rozsahu podle přílohy X a přílohy XI schématu.
- (d) Uvedení prostředku na seznamu podle článku 31 nařízení eIDAS nezakládá přijatelnost informace o záruce.

(2) Kontrola rozsahu:

(a) CB ověří, že podkladové hodnocení dle Společných kritérií bylo provedeno proti profilu ochrany odpovídajícímu roli komponenty v architektuře posuzovaného řešení peněženky, nebo proti bezpečnostnímu cíli deklarujícímu vůči takovému profilu ochrany striktní shodu:

- **vzdálený WSCD (kryptografický modul):** EN 419 221-5,
- **WSCA provozovaná na serveru:** EN 419 241-2,
- **lokální externí WSCD:** EN 419 211, části 2 a 3.

Hodnocení provedené proti jinému profilu ochrany, nebo bez profilu ochrany, není podle této kapitoly přijatelné.

(b) CB ověří popis produktu a bezpečnostní tvrzení a posoudí, zda hodnocené bezpečnostní funkce zahrnují od komponenty v roli WSCD, resp. WSCA — zejména generování, uložení a použití kryptografických klíčů pro pečetění PID a pro elektronická potvrzení atributů.

(c) CB posoudí a v certifikačním posudku zdokumentuje rozdíl mezi rozsahem profilu ochrany a požadavky přílohy X schématu na WSCD, resp. WSCA. Uvedené profily ochrany jsou navrženy pro vytváření elektronických podpisů a pečeti a zpravidla nepokrývají zejména:

- správu více kryptografických klíčů pro elektronická potvrzení atributů,
- vazbu mezi WSCD a WSCA definovanou přílohou X,
- mechanismy autorizace uživatele specifické pro jednotku peněženky,
- atestaci jednotky peněženky.

Identifikované mezery v pokrytí jsou vstupem pro stanovení zbytkových hodnotících činností podle odstavce (4).

(d) CB ověří, že Bezpečnostní cíl (Security target) hodnoceného prostředku pokrývá konfiguraci a způsob nasazení odpovídající architektuře posuzovaného řešení peněženky, včetně předpokladů o provozním prostředí.

(e) CB posoudí, zda rozsah hodnocení zahrnuje scénář sdílení prostředku více jednotkami peněženky (multi-tenancy), je-li tento scénář v posuzovaném řešení relevantní. Profily ochrany podle písmene (a) pokrývají prostředek jako takový. **Izolace mezi jednotkami peněženky sdílejícími tentýž prostředek zpravidla není hodnocena a vyžaduje samostatné posouzení** v souladu s požadavky přílohy X na oddělení kryptografického materiálu.

(f) Funkce prostředku využívané pro poskytování služeb vytvářejících důvěru nejsou předmětem posouzení podle této kapitoly. **(3) Kontrola záruky:**

(a) CB ověří úroveň záruky hodnocení (EAL) a použitá rozšíření, zejména úroveň hodnocení zranitelností (AVA_VAN), podle kritérií kapitoly IX.6.1, resp. IX.6.2. Pro WSCD schéma EUDIW-CZ vyžaduje minimálně EAL4+AVA_VAN.5. Pro WSCA provozovanou v architektuře se vzdáleným WSCD je minimální přijatelnou úrovní AVA_VAN.3 za kompenzačních podmínek požadavku WSA-06 přílohy X. Deklarovaná úroveň v certifikátu QSCD se neověřuje odkazem na obvyklou praxi, ale výhradně z podkladového certifikátu dle Společných kritérií a jeho bezpečnostního cíle.

(b) Pokud podkladové hodnocení dle Společných kritérií bylo provedeno před přijetím EUCC (tj. v rámci národního schématu založeného na Společných kritériích), CB posoudí, zda hodnotící činnosti jsou srovnatelné s těmi vyžadovanými EUCC pro úroveň „vysoká“ — zejména úroveň hodnocení zranitelnosti (AVA_VAN.5) a dodržení kryptografických požadavků dle SOG-IS ACM nebo ECCG ACM.

(4) Zbytkové hodnotící činnosti:

IX.6.5 EN ISO/IEC 27001:2022 — ISMS Podkladové hodnocení dle Společných kritérií provedené proti profilu ochrany pro QSCD nepředstavuje plný důkaz o shodě komponenty s požadavky přílohy X (scénář (1) kapitoly IX.5.2). Jedná se vždy nejvýše o částečný důkaz podle scénáře (2) kapitoly IX.5.2. CB provede minimálně tyto zbytkové činnosti:

(a) mapování bezpečnostních funkcí popsaných v bezpečnostním cíli na požadavky přílohy X pro WSCD, resp. WSCA, a identifikaci nepokrytých požadavků;

(b) hodnocení nepokrytých požadavků v plném rozsahu podle přílohy XI schématu;

(c) ověření platnosti předpokladů profilu ochrany o provozním prostředí, včetně předpokladů ENV-WSCD-01 až ENV-WSCD-03 přílohy X;

(d) posouzení rozhraní mezi WSCD a WSCA a mezi WSCA a instancí peněženky, které profily ochrany podle odstavce (2)(a) nepokrývají, včetně souladu s bezpečnostními předpoklady bezpečnostního cíle;

(e) ověření, že provozovatel prostředku dodržuje provozní pokyny a přípravné postupy vyplývající z hodnocení;

(f) posouzení servisní vrstvy — hodnocení pokrývá produkt, nikoli službu provozovanou nad tímto produktem. Provoz prostředku, řízení přístupu, monitorování a zálohování klíčů se posuzují jako zbytková činnost; v architektuře schématu je tato vrstva částečně pokryta certifikací ISMS (kapitola IX.6.5) a požadavky přílohy X na infrastrukturu poskytovatele (ENV-INF-01).

IX.6.5 EN ISO/IEC 27001:2022 — ISMS

Identifikace a normativní základ:

Certifikace dle ISO/IEC 27001 prokazuje, že organizace uplatňuje rizikově orientovaný a auditovatelný bezpečnostní rámec napříč svými IKT systémy a provozními procesy.

CIR (EU) 2024/2981 příloha II uvádí „EN ISO/IEC 27001:2022“ jako uznané schéma s předmětem „ISMS“.

ISO/IEC 27001 certifikace pokrývá organizační, procedurální a procesní aspekty bezpečnosti informací, nikoli technické vlastnosti jednotlivých komponent. V kontextu certifikace EUDIW-CZ má proto odlišnou roli než produktově orientovaná schémata (EUCC, FitCEM). Slouží jako vstupní důkaz pro procesní komponenty, nikoli pro produktové komponenty.

Předmět certifikace a CZ komponenty:

ISO/IEC 27001 certifikuje ISMS organizace. V kontextu české architektury EUDIW-CZ se ISO 27001 certifikáty uplatní na:

(a) ISMS procesy poskytovatele peněženky — kapitola X.5 přílohy X definuje pět certifikovatelných ISMS procesů:

- proces vývoje (DEV),
- proces řízení změn (CHG),
- proces řízení zranitelností (VUL),
- proces řízení incidentů (INC) a
- proces řízení podvodů (FRD);

(b) ISMS provozovatele infrastruktury HSM — pokud provozovatel drží ISO 27001 certifikaci pokrývající provoz HSM infrastruktury;

(c) ISMS dalších subjektů zapojených do řešení peněženky — jako doplňkový důkaz vedle primárních schémat (ETSI EN 319 401, CIR 2015/1502).

ISO 27001 certifikát se přijímá jako částečný důkaz, nikoli jako plný důkaz splnění požadavků schématu EUDIW-CZ pro procesní komponenty.

(1) Kontrola vydavatele:

Odborná způsobilost a nestrannost certifikačního orgánu nemusí být posuzována nad rámec standardních požadavků. ISO/IEC 27001 certifikace je prováděna certifikačními orgány akreditovanými dle ISO/IEC 17021-1 příslušným národním akreditačním orgánem (v ČR: Český institut pro akreditaci (ČIA)).

CB schématu EUDIW-CZ ověří pouze platnost akreditace certifikačního orgánu k datu hodnocení.

(2) Kontrola rozsahu:

(a) CB ověří popis systému řízení — rozsah ISMS definovaný v certifikátu. Pro přijatelnost dle schématu EUDIW-CZ musí rozsah ISMS zahrnovat provoz služby peněženky, včetně všech komponent definovaných v

příloze I schématu. Pokud rozsah ISMS pokrývá pouze obecné IT operace organizace a nezahrnuje explicitně provoz peněženky, certifikát nelze přijmout jako relevantní důkaz.

(b) CB ověří prohlášení o aplikovatelnosti (*Statement of Applicability*, SoA). SoA musí pokrývat opatření z přílohy A normy ISO/IEC 27002:2022 relevantní pro provoz peněženky. CB zejména ověří pokrytí opatření v oblastech:

- řízení přístupu (A.5.15–A.5.18, A.8.2–A.8.5),
- kryptografie (A.8.24),
- bezpečnosti vývoje (A.8.25–A.8.31),
- řízení zranitelností (A.8.8),
- řízení incidentů (A.5.24–A.5.28),
- řízení dodavatelů (A.5.19–A.5.22) a
- kontinuity činností (A.5.29–A.5.30).

(c) CB posoudí, zda SoA pokrývá EUDIW-CZ specifické požadavky definované v příloze X schématu, které jdou nad rámec generické ISO 27001. Tyto zahrnují zejména:

- řízení podvodů (*fraud management*) dle požadavků FRD-P01 až FRD-P05 přílohy X. ISO/IEC 27001 explicitně neřeší fraud management. ISO/IEC 37003:2025 nebo ekvivalentní rámec je vyžadován jako doplněk;
- bezpečný životní cyklus vývoje SW (SDLC) specifický pro mobilní wallet instance (OWASP MAS s aplikací testovacích profilů MAS-L2 + MAS-R + MAS-P a s odkazem na katalog slabín OWASP MASWE, SAST/DAST v CI/CD pipeline);
- meziorganizační koordinační postupy pro procesy přesahující více subjektů, a
- specifické požadavky na řízení zranitelností WSCA a wallet instance (sledování CVE, koordinovaný disclosure).

(3) Kontrola záruky:

(a) CB ověří provedené hodnotící činnosti — ISO/IEC 27001 certifikace zahrnuje dvoustupňový audit (Stage 1: přezkum dokumentace, Stage 2: audit na místě) a průběžné dozorové audity (minimálně jednou ročně). CB ověří, že certifikace je aktuální — poslední dozorový audit nesmí být starší než 12 měsíců k datu hodnocení EUDIW-CZ.

(b) CB posoudí, zda auditní zpráva (certification assessment report, CAR) neobsahuje neuzavřené neshody relevantní pro provoz peněženky. Pokud CAR obsahuje neuzavřené neshody, CB posoudí nápravná opatření dle scénáře (4) kapitoly IX.5.2 Kritéria přiměřenosti.

(c) CB ověří, že certifikace byla provedena na základě aktuální verze normy — EN ISO/IEC 27001:2022. Certifikáty vydané na základě starší verze ISO/IEC 27001:2013 jsou přijatelné pouze v přechodném období a pokud certifikační orgán potvrdí shodu s požadavky verze 2022.

(4) Zbytkové hodnotící činnosti:

ISO/IEC 27001 certifikace poskytuje pouze částečný důkaz pro procesní komponenty schématu EUDIW-CZ. CB vždy provede následující zbytkové činnosti:

- (a) Ověření pokrytí EUDIW-specifických požadavků — CB pro každý z pěti ISMS procesů (DEV, CHG, VUL, INC, FRD) dle kapitoly X.5 přílohy X ověří, zda ISO 27001 certifikace pokrývá specifické požadavky schématu. Typicky ISO 27001 pokryje generické procesní požadavky (existence procesu, dokumentace, přezkum vedením), avšak EUDIW-specifické detaily vyžadují samostatné posouzení.
- (b) Fraud management — ISO/IEC 27001 explicitně neřeší řízení podvodů. CB posoudí implementaci procesu řízení podvodů (FRD) jako plně novou hodnotící činnost, bez ohledu na existenci ISO 27001 certifikace.
- (c) Meziorganizační koordinace — pokud procesy přesahují více subjektů, CB ověří, že meziorganizační koordinační postupy jsou definovány, dokumentovány a funkční. ISO 27001 certifikace jednotlivé organizace nepokrývá koordinaci mezi organizacemi.
- (d) Provozní účinnost EUDIW-CZ specifických kontrol — CB ověří provozní účinnost opatření specifických pro EUDIW dle CEN TS 18072 sekce 7.4.4.2.2.3 (prověřování dodavatelského řetězce), a to i v případě, že ISO 27001 certifikace potvrzuje provozní účinnost generických ISMS opatření.

IX.6.6 SOC 2 — Organizace

Identifikace a normativní základ:

SOC 2 (*System and Organization Controls 2*) je rámec pro zprávy o opatřeních v servisních organizacích, definovaný americkým institutem AICPA (*American Institute of Certified Public Accountants*). SOC 2 zprávy posuzují návrh a provozní účinnost opatření organizace ve vztahu k jednomu nebo více kritériím důvěryhodných služeb (Trust Services Criteria, TSC):

- bezpečnost (*Security*),
- dostupnost (*Availability*),
- integrita zpracování (*Processing Integrity*),
- důvěrnost (*Confidentiality*) a
- soukromí (*Privacy*).

SOC 2 rozlišuje dva typy zpráv:

- Type I (posouzení návrhu opatření k určitému datu) a
- Type II (posouzení návrhu i provozní účinnosti opatření za definované období, typicky 6–12 měsíců).

Pro účely schématu EUDIW-CZ je přijatelný pouze SOC 2 Type II, protože poskytuje důkaz o provozní účinnosti opatření za sledované období.

CIR (EU) 2024/2981 příloha II uvádí „SOC2“ jako uznané schéma s předmětem „Organizace“.

Předmět certifikace a CZ komponenty:

SOC 2 posuzuje opatření organizace poskytující služby. V kontextu české architektury EUDIW-CZ se SOC 2 zprávy uplatní na:

- (a) Infrastrukturu poskytovatele cloudu — pokud poskytovatel cloudové/hostingové infrastruktury disponuje SOC 2 Type II zprávou pokrývající služby hostingu relevantní pro EUDIW;
- (b) Backend poskytovatele peněženky — pokud využívají cloudovou infrastrukturu třetí strany, která disponuje SOC 2 Type II zprávou;
- (c) Případně další servisní organizace v dodavatelském řetězci řešení peněženky.

SOC 2 zpráva se přijímá jako částečný důkaz pro infrastrukturní a organizační opatření — nikoli jako důkaz pro produktové nebo funkční bezpečnostní vlastnosti.

(1) Kontrola vydavatele:

(a) CB ověří status vydavatele SOC 2 zprávy. SOC 2 zprávy jsou vydávány nezávislými auditory — oprávněnými veřejnými účetními (Certified Public Accountant, CPA) nebo auditorskými firmami. CB ověří, že vydavatel je oprávněným CPA nebo auditorskou firmou registrovanou u příslušného profesního orgánu.

(b) Na rozdíl od EUCC nebo ISO 27001 neexistuje u SOC 2 formální akreditační rámec srovnatelný s ISO/IEC 17065 nebo ISO/IEC 17021-1. Kvalita a důvěryhodnost SOC 2 zprávy závisí na profesních standardech AICPA a na dohledu nad CPA profesí. Namísto akreditace CB posoudí důvěryhodnost vydavatele na základě následujících ověřitelných kritérií:

- i. vydavatel je držitelem platné licence CPA nebo je auditorskou firmou registrovanou u příslušného dohledového orgánu účetní profese (v USA zejména u státní rady účetních (State Board of Accountancy) a v systému PCAOB, je-li aplikovatelné);
- ii. vydavatel podléhá pravidelnému externímu přezkumu kvality (peer review) v souladu s programem AICPA Peer Review Program nebo rovnocenným programem dohledu nad kvalitou;

iii. vydavatel prokáže zkušenost s prováděním zakázek SOC 2 pro poskytovatele IT služeb, například doložením referencí nebo počtu srovnatelných zakázek za posledních 24 měsíců.

Nesplní-li vydavatel kritérium i., zpráva není přijatelná jako vstup do analýzy závislostí. Kritéria ii. a iii. CB posoudí v rámci celkového vážení důvěryhodnosti; jejich nesplnění CB zohlední při určení rozsahu zbytkových hodnotících činností dle bodu (4).

(c) CB posoudí nestrannost vydavatele — zejména zda neexistuje konflikt zájmů mezi auditorskou firmou a posuzovanou organizací.

(2) Kontrola rozsahu:

(a) CB ověří prohlášení vedení (*management assertion*) a popis systému (*system description*) v SOC 2 zprávě. Popis systému musí zahrnovat služby relevantní pro EUDIW-CZ — tj. hostingové, provozní a infrastrukturní služby poskytované pro řešení peněženky.

(b) CB ověří, která kritéria důvěryhodných služeb (TSC) jsou zahrnuta v SOC 2 zprávě. Pro přijatelnost dle schématu EUDIW-CZ musí zpráva pokrývat minimálně kritérium Security (povinné pro všechny SOC 2 zprávy). Kritéria Availability a Confidentiality poskytují dodatečný důkaz relevantní pro požadavky přílohy X na dostupnost služby a ochranu důvěrnosti údajů.

(c) CB ověří prohlášení o aplikovatelnosti — zda SOC 2 scope pokrývá konkrétní služby poskytované pro EUDIW, nikoli pouze obecné operace organizace.

(d) CB posoudí, zda popis systému zahrnuje poddodavatele relevantní pro dodavatelský řetězec EUDIW. SOC 2 zprávy používají dva přístupy k poddodavatelům:

- „inclusive method“ (poddodatelská organizace je zahrnuta v rozsahu) a
- „carve-out method“ (poddodatelská organizace je vyloučena z rozsahu a pokryta vlastní zprávou).

CB ověří, která metoda byla použita, a v případě carve-out posoudí, zda existuje samostatná zpráva poddodatelské organizace.

(3) Kontrola záruky:

(a) CB ověří zjištění (findings) ve zprávě — zejména zda auditor identifikoval výjimky (exceptions) v provozní účinnosti opatření. Pokud zpráva obsahuje výjimky, CB posoudí jejich závažnost a relevanci pro provoz peněženky dle scénáře (4) kapitoly IX.5.2 Kritéria přiměřenosti.

(b) CB ověří periodu pokrytí SOC 2 Type II zprávy. Perioda musí zahrnovat datum hodnocení EUDIW-CZ nebo musí být doplněna překlenovacím dopisem pokrývajícím přechodné období mezi koncem pokryté periody a

datem hodnocení. SOC 2 Type I zprávy (posouzení k bodu v čase) nejsou přijatelné jako důkaz provozní účinnosti.

(c) CB ověří, zda zpráva je vydána na základě aktuálních standardů — AICPA SSAE 18 (Statement on Standards for Attestation Engagements No. 18) nebo novějšího.

(4) Zbytkové hodnotící činnosti:

SOC 2 zpráva poskytuje pouze částečný důkaz pro infrastrukturní opatření. CB vždy provede následující zbytkové činnosti:

(a) Mapování TSC na požadavky přílohy X — CB vytvoří mapování opatření popsaných v SOC 2 zprávě na specifické požadavky přílohy X schématu EUDIW-CZ (zejména NET-01, PHY-01, ACC-01, BCM-01, ENV-INF-01). SOC 2 TSC a požadavky přílohy X nemají přímý 1:1 vztah — CB musí posoudit pokrytí individuálně.

(b) EUDIW-CZ specifické požadavky — SOC 2 zpráva typicky nepokrývá požadavky specifické pro peněženku EUDI (řízení kryptografických klíčů, izolace wallet units v multi-tenancy prostředí, bezpečnost komunikačních kanálů WSCA–WSCD). Tyto požadavky vyžadují samostatné posouzení.

(c) Posouzení poddodavatelských organizací — pokud SOC 2 zpráva používá carve-out metodu, CB posoudí, zda vyloučené dodavatelské organizace jsou pokryty vlastními zprávami nebo zda vyžadují samostatné hodnocení.

(d) Regulatorní požadavky — SOC 2 je americký rámec a nepokrývá specifické regulatorní požadavky EU (eIDAS, NIS2, CIR 2024/2981). CB posoudí shodu s relevantními EU regulatorními požadavky jako samostatnou hodnotící činnost.

IX.6.7 ETSI EN 319 401 — Posouzení shody dle eIDAS auditního rámce

Identifikace a normativní základ:

ETSI EN 319 401 v3.2.1 definuje obecné požadavky na politiku pro poskytovatele služeb vytvářejících důvěru (Trust Service Provider, TSP). Norma je základem pro posuzování shody kvalifikovaných poskytovatelů služeb vytvářejících důvěru (QTSP) dle článku 20 a článku 24 nařízení (EU) č. 910/2014 (eIDAS). Posuzování shody provádějí certifikační orgány akreditované dle ETSI EN 319 403-1 (CAB pro posuzování shody TSP), která sama staví na ISO/IEC 17065.

ETSI EN 319 401 je doplněna řadou service-specific norem:

- ETSI EN 319 411-1 a 319 411-2 (pro vydavatele certifikátů),

- ETSI TS 119 431-1 (pro provozovatele komponent TSP, včetně provozovatele vzdáleného kryptografického prostředku) a
- ETSI TS 119 462 (pro rozhraní peněženky EUDI).

CIR (EU) 2024/2981 příloha II výslovně neuvádí ETSI EN 319 401 jako samostatný řádek, ale implicitně jej pokrývá v kategorii „Jiné systémy“. V kontextu schématu EUDIW-CZ je ETSI EN 319 401 audit klíčovým zdrojem informací o záruce pro servisní komponenty řešení peněženky a pro externí služby, na nichž řešení peněženky závisí.

Ekosystém auditu dle ETSI EN 319 401 je vyspělý a je částečně harmonizován prostřednictvím aktivit FESA (Forum of European Supervisory Authorities), ACAB'c (Accredited Conformity Assessment Bodies' Council) a EA (European Accreditation). Stávající certifikační schémata pro posuzování shody QTSP mohou být okamžitě použita i pro posuzování shody poskytovatelů identifikačních služeb (ISP) dle eIDAS 2.0.

Předmět certifikace a CZ komponenty:

Audit dle ETSI EN 319 401 posuzuje poskytovatele služeb, na které se vztahují obecné požadavky na politiku podle této normy. V kontextu architektury EUDIW-CZ se auditní výsledky uplatní na:

- (a) Službu pečetení PID — jako externí závislost mimo rozsah certifikace dle přílohy I schématu. Subjekt provozující tuto službu není předmětem certifikace EUDIW-CZ. Jeho existující zpráva o posouzení shody (CAR) dle ETSI EN 319 401 slouží jako důkaz platnosti předpokladu o prostředí dle požadavku ENV-INF-03 přílohy X. Není vyžadováno, aby tento subjekt byl kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Postačuje, že jeho shoda s ETSI EN 319 401 byla ověřena;
- (b) Ověřovací službu peněženek a spoléhajících se stran — jako komponentu v rozsahu certifikace dle přílohy Ia schématu, pokud je provozována subjektem posuzovaným dle ETSI EN 319 401. Existující auditní výsledky vstupují do analýzy závislostí jako částečný důkaz;
- (c) Potenciálně další servisní komponenty řešení peněženky, které mohou být posuzovány na základě rámce ETSI EN 319 401 — zejména službu jednotky peněženky, poskytování a správu peněženky a poskytování PID (služby, pro které příloha X definuje požadavky odvozené z klauzule 7 ETSI EN 319 401).

ETSI EN 319 401 auditní výsledky se přijímají jako důkaz na úrovni služby. Podporují kompozici a opětovné využití — výsledky certifikace již eIDAS-certifikovaných „servisních modulů“ nebo „technických komponent“ mohou být opětovně použity a považovány za „black box“.

(1) Kontrola vydavatele:

- (a) CB ověří, že audit dle ETSI EN 319 401 byl proveden certifikačním orgánem akreditovaným dle ETSI EN 319 403-1. ETSI EN 319 403-1 staví na ISO/IEC 17065 a definuje specifické požadavky pro CAB posuzující TSP.

(b) CB ověří platnost akreditace CAB u příslušného NAB (v ČR: ČIA). Akreditace zahrnuje posouzení odborné způsobilosti i nestrannosti — žádné dodatečné posouzení vydavatele není vyžadováno.

(c) CB ověří, že auditor má prokazatelné zkušenosti s auditem poskytovatelů služeb dle ETSI EN 319 401 v oblasti relevantní pro EUDIW (zejména služby pečetení, vydávání certifikátů, provoz RQSCD).

(2) Kontrola rozsahu:

(a) CB ověří rozsah posouzení shody — služby uvedené v osvědčení a v auditní zprávě (CAR). Pro přijatelnost dle schématu EUDIW-CZ musí rozsah zahrnovat explicitně službu pečetení PID pro EUDIW. Pokud posuzovaný subjekt držel osvědčení pouze pro služby vydávání kvalifikovaných certifikátů (bez explicitního zahrnutí pečetení PID pro EUDIW), CB posoudí, zda služba pečetení PID je pokryta implicitně (jako podmnožina stávající služby pečetení) nebo zda vyžaduje rozšíření rozsahu certifikace.

(b) CB ověří, které klauzule ETSI EN 319 401 byly auditovány. Pro přijatelnost musí audit pokrývat minimálně:

- klauzuli 5 (obecné požadavky na politiku),
- klauzuli 6 (požadavky na řízení rizik, aktiv a incidentů),
- klauzuli 7 (provozní bezpečnostní požadavky — fyzická bezpečnost, řízení přístupu, síťová bezpečnost, řízení kryptografických klíčů, řízení zranitelností, bezpečný vývoj).

(c) CB ověří, zda audit zahrnoval požadavky service-specific norem relevantních pro posuzovanou službu: zejména ETSI EN 319 411-1 nebo 319 411-2 (pro vydávání certifikátů) a ETSI TS 119 431-1 (pro provoz komponent TSP, včetně provozovatele vzdáleného QSCD).

(d) CB posoudí, zda rozsah auditu pokrývá integraci posuzované služby s řešením peněženky — zejména rozhraní pro příjem žádostí o pečetení PID od poskytovatele peněženky, formát a obsah elektronických pečeti, a vazbu na důvěryhodnou infrastrukturu (trust anchors, trust lists).

(3) Kontrola záruky:

(a) CB ověří výsledky poslední auditní zprávy (Conformity Assessment Report, CAR). CAR je primárním výstupem auditu QTSP a obsahuje zjištění, neshody a celkový závěr auditora.

(b) CB ověří, že audit je aktuální — poslední auditní zpráva nesmí být starší než 12 měsíců k datu hodnocení EUDIW-CZ. Pokud od data posledního auditu uplynulo více než 12 měsíců, CB nemůže přijmout auditní výsledky jako platný vstup do analýzy závislostí.

(c) CB ověří, zda CAR neobsahuje neuzavřené neshody (non-conformities) relevantní pro operace EUDIW. Pokud CAR obsahuje neuzavřené neshody, CB posoudí jejich závažnost a relevanci dle scénáře (4) kapitoly IX.5.2 Kritéria přiměřenosti.

(d) CB posoudí, zda auditní činnosti zahrnovaly posouzení provozní účinnosti opatření (operating effectiveness) — nikoli pouze posouzení návrhu opatření (design effectiveness). ETSI EN 319 403-1 vyžaduje dvoustupňový audit (Stage 1 a Stage 2) srovnatelný s přístupem ISO/IEC 17021-1, který zahrnuje audit na místě s posouzením provozní účinnosti.

(4) Zbytkové hodnotící činnosti:

(a) EUDIW-CZ specifické požadavky — ETSI EN 319 401 audit dle ETSI EN 319 401 pokrývá obecné požadavky na TSP, avšak ne specifické požadavky schématu EUDIW-CZ. CB posoudí jako zbytkové činnosti zejména: shodu s požadavky přílohy X kapitoly X.8 (požadavky na PID provider), požadavky na fraud management dle kapitoly X.5.5, požadavky na integraci s NIA (onboarding) a specifické požadavky na formát a obsah PID dle ARF.

(b) Integrace QTSP s řešením peněženky — CB ověří správnost integrace pečeticí služby s backendem poskytovatele peněženky. Toto zahrnuje: ověření komunikačních protokolů a bezpečnostních kanálů, ověření formátu žádostí o pečetení a odpovědí, ověření mechanismů pro zajištění integrity a autenticity pečeti a ověření dostupnosti a odolnosti služby pečetení.

(c) Dozorové požadavky eIDAS 2.0 — CIR (EU) 2024/2981 může definovat dozorové požadavky nad rámec stávajícího eIDAS 1.0 rámce. CB posoudí, zda stávající audit pokrývá tyto dodatečné požadavky, nebo zda jsou potřeba zbytkové činnosti.

(d) Shoda s CIR (EU) 2015/1502 — posouzení shody systému elektronické identifikace s CIR 2015/1502 musí být provedeno CB jako součást certifikace EUDIW-CZ a nemůže být nahrazeno auditem dle ETSI EN 319 401 (CIR 2015/1502 conformity musí být posouzena CB, nemůže být nahrazena smluvními závazky).

IX.6.8 Atestace dle zákona 250/2017 Sb.

Může být uznána pouze atestace inspekčního orgánu akreditovaného dle ISO 17020 pro systémy elektronické identifikace dle zákona 250/2017 Sb.

(1) Kontrola vydavatele:

(a) CB ověří, že atestace byla provedena atestujícím orgánem akreditovaným dle EN ISO/IEC 17020 pro oblast „Informační systémy veřejné správy“ a „Systémy elektronické identifikace“ (pro oblast relevantní pro danou komponentu) v souladu se zákonem 250/2017 Sb.

(b) CB ověří platnost akreditace atestujícího orgánu u příslušného národního akreditačního orgánu (v ČR: ČIA) k datu vydání atestace.

(2) Kontrola rozsahu:

(a) CB ověří, že rozsah atestace pokrývá komponentu české architektury EUDIW-CZ, pro kterou je informace o záruce předkládána — zejména registraci a správu uživatelů s ověřením totožnosti (onboarding) dle přílohy Ib schématu.

(b) CB ověří, že atestace byla provedena pro úroveň záruky „vysoká“ ve smyslu prováděcího nařízení (EU) 2015/1502; atestace provedená pouze pro úroveň „značná“ není dostatečná pro komponenty vyžadující úroveň „vysoká“ a zakládá zbytkovou hodnotící činnost dle bodu (4).

(c) CB ověří, které oblasti akreditace atestující orgán při atestaci uplatnil — „Systémy elektronické identifikace“, „Informační systémy veřejné správy“, nebo obě; rozsah skutečně pokrytých oblastí určuje rozsah zbytkových činností dle bodu (4).

(d) CB posoudí mapování požadavků, na jejichž základě byla atestace provedena, na příslušné požadavky přílohy X schématu (zejména kapitoly X.8 pro onboarding a správu PID) a identifikuje požadavky přílohy X, které atestace nepokrývá.

(3) Kontrola záruky:

(a) CB ověří platnost atestace k datu hodnocení EUDIW-CZ a soulad doby platnosti s požadavky na kontinuitu dle přílohy II schématu; propadlá atestace není přijatelná jako důkaz.

(b) CB ověří, zda atestace vychází z posouzení provozní účinnosti zavedených opatření, nikoli pouze z posouzení návrhu opatření; není-li provozní účinnost atestací pokryta, posoudí ji CB jako zbytkovou činnost dle bodu (4).

(c) CB ověří, zda atestační zpráva neobsahuje neuzavřené neshody relevantní pro provoz peněženky; pokud takové neshody obsahuje, CB posoudí jejich závažnost a relevanci dle scénáře (4) kapitoly IX.5.2 Kritéria přiměřenosti.

(d) CB posoudí, zda atestace pokrývá požadavky prováděcího nařízení (EU) 2015/1502 relevantní pro danou komponentu; posouzení shody s CIR (EU) 2015/1502 nemůže být plně nahrazeno atestací dle zákona 250/2017 Sb. a v částech nepokrytých atestací je provedeno CB.

(4) Zbytkové hodnotící činnosti:

(a) Pokud atestující orgán byl akreditován pouze pro oblast „Systémy elektronické identifikace“, provede CB dodatečnou inspekci v oblasti „Informační systémy veřejné správy“, nebo jí pověří třetí stranu akreditovanou pro tuto oblast dle EN ISO/IEC 17020.

(b) Pokud atestující orgán byl akreditován pouze pro oblast „Informační systémy veřejné správy“, provede CB dodatečnou inspekci v oblasti „Systémy elektronické identifikace“, nebo jí pověří třetí stranu akreditovanou pro tuto oblast dle EN ISO/IEC 17020.

(c) Zbytkové hodnotící činnosti vyplývající z rozsahu a záruky dle bodů (2) a (3) — zejména nepokrytí úrovně „vysoká“, nepokrytí provozní účinnosti nebo požadavků přílohy X a CIR (EU) 2015/1502 — provede CB v souladu s kapitolou IX.5 této přílohy.

IX.6.9 Jiné systémy

Pro certifikační schémata neuvedená v kapitolách IX.6.1 až IX.6.8 CB provede úplnou analýzu závislostí dle generické metody definované v kapitole IX.3 Metoda analýzy závislostí a dle generických kritérií kapitol IX.4 Posouzení dostupnosti dokumentace o záruce a IX.5 Posouzení záruky ve vztahu k individuálním požadavkům — tj. bez zjednodušení dostupných pro uznaná schémata. CB zdokumentuje v certifikačním posudku odůvodnění přijatelnosti, včetně posouzení ve všech třech dimenzích (vydavatel, rozsah, záruka) a identifikace zbytkových hodnotících činností.

Tato kategorie je určena zejména pro budoucí schémata, která mohou být relevantní po jejich přijetí — zejména EUCS (European Cybersecurity Certification Scheme for Cloud Services) po jeho přijetí, MDSCert (GSMA Mobile Device Security Certification) po jeho dostupnosti a případná budoucí národní nebo sektorová schémata.

Podmínky pro zařazení nového schématu do kategorie „uznaných schémat“ (tj. pro přidání specifických kritérií do kapitoly IX.6 Specifická kritéria pro certifikované komponenty) jsou:

- schéma je uvedeno v příloze II CIR (EU) 2024/2981 nebo je formálně uznáno na úrovni EU;
- existuje alespoň jedna komponenta české architektury EUDIW-CZ, na kterou se schéma uplatní;
- jsou k dispozici dostatečné informace pro definici specifických kritérií ve třech dimenzích.

Doplnění specifických kritérií pro nové schéma se provede formou aktualizace této přílohy.