

20 Příloha VII: Obsah Zprávy o certifikačním posouzení/hodnocení

1. Zpráva o certifikačním posouzení uvedená v EUDIW-CZ v čl. 7 odst. 5 musí:
 - (1) být doprovázena jasným rozhodnutím o certifikaci v souladu s bodem 7.6 normy EN ISO/IEC 17065:2012, které potvrzuje, zda držitel certifikátu a služba IKT, kterou poskytuje, splňují požadavky stanovené v nařízení (EU) 2024/1183.
 - (2) uvádět jméno držitele certifikátu a případně jeho registrační číslo uvedené v úředních záznamech, jeho oficiální poštovní adresu a elektronickou adresu, jakož i případně stejné informace pro všechny dceřiné společnosti, přidružené právní subjekty, dodavatele a subdodavatele, kteří vyrábějí, poskytují nebo provozují komponenty v rozsahu certifikátu jménem držitele certifikátu;
 - (3) obsahovat podrobný popis rozsahu služby IKT, na kterou se posouzení vztahuje, včetně všech produktových a procesních komponent, spolu s posouzením rizik a konkrétním plánem validace;
 - (4) obsahovat dostatečné důkazy prokazující, že držitel certifikátu a služba IKT, kterou poskytuje, splňují požadavky stanovené v nařízení (EU) 2024/1183;
 - (5) uvádět název subjektu posuzování shody, který certifikát vydal, a případně jeho registrační číslo uvedené v úředních záznamech, jeho registrovanou poštovní adresu a jeho elektronickou adresu;
 - (6) uvádět následující:
 - a. název a zemi národního akreditačního orgánu, který akreditoval subjekt posuzování shody;
 - b. jména fyzických osob zapojených do posuzování shody subjektem posuzování shody a jejich příslušnou roli v tomto posuzování;
 - c. odkaz na oficiální webové stránky národního akreditačního orgánu, na kterých je uveden certifikát o akreditaci vydaný národním akreditačním orgánem subjektu posuzování shody;
 - d. případně digitální akreditační symbol;
 - e. certifikační schéma, pro které byl subjekt posuzování shody akreditován v souladu s článkem 12(1);
 - f. provedené hodnotící činnosti, odůvodnění jejich výběru a použitá metodika, včetně metodiky výběru vzorků a zkušebních postupů;
 - g. certifikační schéma a příslušné dokumenty nebo odkaz na místo, kde je toto certifikační schéma a příslušné dokumenty k dispozici;
 - (7) obsahovat alespoň jeden kvalifikovaný elektronický podpis, pokud je zpráva poskytnuta v elektronické podobě, nebo vlastnoruční podpis, pokud je poskytnuta v listinné podobě, s uvedením jména a funkce odpovědné osoby nebo osob, které byly oprávněny přijmout rozhodnutí o certifikaci jménem subjektu posuzování shody;
 - (8) zahrnovat v souladu s bodem 2:
 - a. vyčerpávající seznam třetích stran, včetně subdodavatelů, které poskytují komponenty, s uvedením jejich názvu, jak je uvedeno v bodě 2;
 - b. údaj o tom, zda tyto třetí strany a komponenty byly podrobeny posouzení shody a v jakém rozsahu;
 - (9) v případě potřeby popsat obsah záznamu, který má být Komisí zahrnut nebo aktualizován v seznamu evropských peněženek digitální identity v souladu s výsledkem posouzení;

- (10) zahrnovat vyčerpávající seznam interních dokumentů veřejných a kvalifikovaných poskytovatelů důvěryhodných služeb, které jsou řádně identifikovány včetně verzí a které byly součástí rozsahu posouzení shody, včetně alespoň následující dokumentace uvedené v bodě 8, jejíž kopie musí být buď poskytnuta spolu se zprávou o posouzení shody, nebo jinak zpřístupněna příslušnému dozorovému orgánu na jeho žádost:
- a. podmínky týkající se smluv s uživateli peněženky;
 - b. plán ukončení certifikované služby IKT;
 - c. dokumentace, která se vztahuje k posouzení rizik a jejímž cílem je prokázat, že požadavky čl. 24 odst. 2 písm. fa) a fb) nařízení (EU) 2024/1183 byly splněny;
 - d. plán oznamování incidentů, jehož cílem je prokázat, že požadavky čl. 24 odst. 2 písm. fa) a fb) nařízení (EU) 2024/1183 byly splněny;
 - e. seznam všech interních dokumentů podporujících efektivní poskytování certifikovaných služeb IKT držitelem certifikátu;
 - f. důkaz, že držitel certifikátu v souladu s platnými vnitrostátními právními předpisy udržuje dostatečné finanční zdroje a případně má sjednané odpovídající pojištění odpovědnosti za poskytování certifikované služby IKT;
 - g. seznam norem, s nimiž je provoz služby v souladu;
 - h. seznam norem, s nimiž je provoz služby auditován, hodnocen, certifikován nebo posuzován jako vyhovující, spolu s podrobnostmi o interním auditu, hodnocení, certifikačním nebo hodnotícím schématu, pokud je to relevantní;
 - i. seznam WSCD a informace související s jejich certifikací, pokud držitel certifikátu dodá nebo zpřístupní tato zařízení svým uživatelům;
 - j. seznam zařízení používaných držitelem certifikátu jako důvěryhodný systém nebo produkt, včetně hardwarových kryptografických modulů nebo zabezpečených kryptografických zařízení, k ochraně klíčů, a informace související s jejich certifikací, pokud držitel certifikátu používá tato zařízení k zabezpečení procesů podporujících poskytovanou službu IKT;
- (11) obsahovat posouzení splnění požadavků, které se vztahují na příslušné služby IKT podle nařízení (EU) 2024/1183, a případně jak je stanoveno v prováděcích aktech a aktech v přenesené pravomoci, které se vztahují na danou službu IKT, jak byly přijaty v souladu s:
- a. článkem 5a(4) nařízení (EU) 2024/1183, pokud jde o funkce peněženky;
 - b. článkem 5a(5) nařízení (EU) 2024/1183, pokud jde o požadavky týkající se peněženek;
 - c. článkem 5a(8) nařízení (EU) 2024/1183, pokud jde o požadavky týkající se ověřovacích mechanismů;
 - d. článkem 5a(14) nařízení (EU) 2024/1183, pokud jde o požadavky týkající se logického oddělení;
 - e. článkem 5a(24) nařízení (EU) 2024/1183, pokud jde o normy a technické specifikace, případně.
- (12) obsahovat prohlášení, v němž se případně prohlašuje neexistence jakýchkoli neshod, bez ohledu na úroveň jejich závažnosti; pokud je ve zprávě zjištěna jakákoli neshoda, zpráva musí obsahovat plán nápravných opatření a jejich časový harmonogram, poskytnutý držitelem certifikátu a schválený subjektem posuzování shody, spolu s popisem plánovaných úkolů hodnocení, které subjekt posuzování shody provede, aby posoudil, zda byly tyto neshody opraveny;
- (13) obsahovat, pokud je to vhodné a nezbytné, uvedení možností zlepšení, pokud jde o plnění příslušných požadavků držitelem certifikátu a kvalifikovanými důvěryhodnými službami, které poskytuje;

- (14) uvést pro každou fázi posuzování shody, včetně auditu dokumentace, posouzení implementace a kontrol na místě, období, ve kterém bylo posouzení provedeno, a čas, který subjekt posuzování shody v osobo-dnech potřeboval k provedení posouzení;
- (15) uvést v odpovídající zprávě o specifických požadavcích podrobné kontroly a cíle kontroly posuzování shody, které byly provedeny během posouzení, nebo uvést odkaz na samostatně dostupné zprávy o posouzení, ve kterých jsou tyto informace uvedeny, za předpokladu, že tyto samostatné zprávy o posouzení jsou:
- vydány subjekty posuzování shody akreditovanými v souladu s nařízením (EU) 2024/1183;
 - schváleny subjekty posuzování shody, které vydávají zprávu o posouzení shody;
- (16) uvést rozsah, popis a výsledky významného souboru zkoušek nebo výrobních vzorků a jejich posouzení pro všechny relevantní a použitelné typy výstupů z posuzovaných kvalifikovaných důvěryhodných služeb;
- (17) uvést následující lhůty:
- lhůta, ve které musí být provedeno další dohledové hodnocení v souladu s certifikačním systémem;
 - lhůta, ve které musí být provedeno další posouzení shody v souladu s certifikačním systémem a s čl. 5c odst. 4 nařízení (EU) 2024/1183;
- (18) obsahovat výslovné prohlášení, že certifikační dokumenty, včetně zprávy o posouzení shody, jsou určeny také pro použití příslušným vnitrostátním orgánem dohledu.
- Popis návrhu služby IKT by měl zahrnovat prvky z popisu uvedeného v certifikační zprávě, doplněné o informace týkající se posouzení rizik pro každou komponentu a o konkrétní plán hodnocení, který je navržen pro každou komponentu a pro celkový předmět certifikace.
 - Zdůvodnění, že řešení peněženky splňuje požadavek úrovně záruky „vysoká“, musí být založeno na důkazech dostupných z hodnotících činností prováděných v tomto schématu, včetně analýzy informací o záruce zpřístupněných z jiných schémat. Je také třeba vytvořit propojení s registrem rizik definovaným v příloze I nařízení CIR (EU) 2024/2981.
- Popis výsledků posouzení musí prokázat, že služba IKT splňuje příslušné požadavky nařízení (EU) 2024/1183, takže pokud se používají normy a technické specifikace, které zahrnují mapování na tyto požadavky, je prokázání, že požadavky z těchto norem a technických specifikací jsou splněny, považováno za dostatečné.
 - Souhrn provádění plánu validace musí zahrnovat popis každé provedené činnosti posuzování shody, jakož i shrnutí jejích výsledků, včetně popisu neshod zjištěných během hodnocení, jakož i popisu provedených zmírňujících opatření a opatření posuzování shody, která mají být provedena v následných posuzováních shody.