

21 Příloha VIII: Požadavky na orgány posuzování shody

21.1 Kompetence

Zaměstnanci odpovědní za určení shody implementace technických komponent řešení peněženky poskytovatele musí mít následující specifické kompetence a znalosti a splňovat následující požadavky:

a) Požadavky:

- 1) formální akademická kvalifikace nebo odborné vzdělání nebo rozsáhlé zkušenosti prokazující obecnou schopnost určovat vlastnosti softwaru prostřednictvím zkoumání jeho návrhu a implementace; a
- 2) alespoň čtyři roky praxe na pracovišti na plný úvazek v činnosti související s vývojem softwaru, z toho alespoň dva roky v roli nebo funkci týkající se služeb poskytování identity nebo jiných citlivých služeb.
- 3) Zajištění testovacího prostředí pro testování, které může být vlastní, zajištěné pomocí subdodavatele nebo může být využito testovacího prostředí hodnoceného.
- 4) Pro testování může být využit *Functional Conformance Assessment Framework (FCAF)*. CAB musí být schopen vytvářet vlastní doplňkové testy, pokud FCAF nepokrývá danou oblast.

b) Znalosti:

- 1) CAB musí zajistit, že každý člen hodnoticího týmu disponuje prokazatelnou kvalifikací v oblasti bezpečnosti informačních technologií. Minimálním požadavkem je vysokoškolské vzdělání v IT/kybernetické bezpečnosti nebo ekvivalentní profesní certifikace (např. CISSP, CISA, CEH) a minimálně 3 roky aktivní praxe v oblasti penetračního testování, bezpečnostních auditů nebo hodnocení shody.
- 2) Vzhledem k provázanosti eIDAS2 certifikací s normou ISO/IEC 15408 (Common Criteria) musí minimálně jeden klíčový člen hodnoticího týmu prokázat hlubokou znalost metodiky CC a CEM (Common Methodology for Information Security Evaluation).
- 3) Hodnoticí tým musí být prokazatelně schopen provádět analýzu závislostí a kompozitní hodnocení v souladu s dokumentem CCDB-2012-04-001 (Composite Product Evaluation) nebo jeho ekvivalentem.
- 4) Minimální velikost hodnoticího týmu pro jeden certifikační projekt jsou 2 osoby plnící specifické role (kumulace rolí Vedoucího a Přezkoumatele je vyloučena):
 - Vedoucí hodnotitel: Odpovídá za řízení projektu, metodiku a finální hodnoticí zprávu (ETR). Splňuje požadavky na znalost Common Criteria a kompozitního hodnocení.
 - Technický hodnotitel / Analytik: Provádí samotné testování, analýzu zranitelností a revizi zdrojového kódu.
 - Přezkoumatel: Osoba, která provádí revizi kvality výstupů před jejich předáním certifikačnímu orgánu.
- 5) V případě, že vedoucí hodnotitel nedisponuje všemi potřebnými znalostmi, pak se tým rozšíří o experta disponujícího těmito znalostmi.
- 6) Další konkrétní znalosti:
 - a. Znalosti principů, postupů a technik zkoumání v oblasti kybernetické bezpečnosti IT služeb a služeb poskytování identity;

- b. Znalosti otázek souvisejících s různými bezpečnostními architekturami služeb Peněženky, různými typy WSCD a WSCA, včetně rizik a hrozeb uvedených v příloze I nařízení (EU) 2024/2981;
 - c. Znalosti platných norem, veřejně dostupných specifikací a regulačních požadavků na poskytovatele peněženek a dalších relevantních veřejně dostupných specifikací, včetně norem pro hodnocení IT produktů a IT služeb; a
 - d. Znalosti procesů orgánu pro posuzování shody;
- 21 Znalost ARF (*Architecture and Reference Framework*).
- c) Kompetence:
- 1) Osoby nebo výbory CAB odpovědné za přezkoumání a konečné rozhodnutí o certifikaci EUDIW musí disponovat prokazatelnou odborností v oblasti asymetrické kryptografie, PKI (Public Key Infrastructure) na národní i unijní úrovni, správy kryptografických klíčů a hodnocení zranitelností na vysoké úrovni útoku (odpovídající eIDAS LoA 'high' / AVA_VAN.5). Rozhodovací orgán musí garantovat schopnost posoudit specifika mobilní bezpečnosti i IT komponent řešení.
 - 2) Pokud CAB využívá subdodavatele (např. IT bezpečnostní laboratoře ITSEF pro penetrační testování), musí tito subdodavatelé splňovat akreditační požadavky pro úroveň záruky 'high' (např. uznání v rámci schématu typu EUCC). CAB musí v certifikačním plánu exaktně vymezit rozsah outsourcovaných úkonů, zajistit ochranu duševního vlastnictví a zdrojových kódů peněženky a nést plnou právní i procesní odpovědnost za finální posouzení shody dodaných zkušebních protokolů.
 - 3) CAB musí být schopen provádět rigorózní funkční testování zaměřené na klíčové schopnosti peněženky definované v ARF (Architecture and Reference Framework). To zahrnuje zejména ověření selektivního zveřejňování atributů (selective disclosure), cross-border interoperabilitu, mechanismy uživatelského souhlasu, vydávání PID (Person Identification Data), kvalifikovaných elektronických podpisů/pečetí a bezpečné fungování v offline režimu.
 - 4) Posuzovací tým CAB musí být povinně interdisciplinární. Musí se skládat z expertů na penetrační testování a hardwarovou bezpečnost (např. Secure Elements / vTPM v chytrých telefonech), specialistů na audit ochrany osobních údajů (GDPR se zaměřením na minimalizaci dat v eIDAS 2.0) a auditorů shody s technickými specifikacemi ENISA / ETSI.
 - 5) Proces posuzování musí obsahovat striktní pravidla pro uznávání předložených důkazů. CAB může akceptovat existující certifikáty pro dílčí komponenty EUDIW – typicky certifikace hardwarových čipů (Secure Elements podle Common Criteria) nebo certifikáty cloudových služeb (např. podle schématu EUCS). CAB však musí metodicky ověřit vazby, rozhraní a správnou integraci těchto předem certifikovaných prvků do celkové architektury konkrétní peněženky.

Veřejné standardy uvedené v bodě b.3) musí zahrnovat alespoň standardy používané pro hodnocení komponent (např. ISO/IEC 15408, ISO/IEC 18045, CEN EN 17640) spolu s příslušnými profily ochrany a veřejně dostupné specifikace musí zahrnovat alespoň standard OWASP *Application Security Verification Standard*.

21.2 Procesní požadavky

Požadavky na proces auditu, jak jsou definovány v oddíle 7.4.4 normy ETSI EN 319 403-1, je třeba doplnit dalšími požadavky týkajícími se technických aspektů.

21.2.1 1. fáze auditu

V rámci přípravy na audit auditoři získají a přezkoumají dokumentaci o službě peněženky poskytovatele peněženky, včetně alespoň:

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb vč. jejich kapacitního plánování a komunikaci informací klientům veřejné správy, financovaného Evropskou unií NextGeneration. Reg. č.: CZ.31.5.0/0.0/0.0/23_106/0008503.

- specifikací technických komponent peněženky a služeb peněženky v rozsahu auditu;
- odůvodnění pro pokrytí certifikačních kritérií, zejména s ohledem na úroveň odolnosti proti útokům;
- analýzu rizik, která zahrnuje minimálně rizika a hrozby popsané v registru rizik v příloze I nařízení (EU) 2024/2981;
- identifikaci zranitelností;
- protokoly penetračních testování IT systémů.

Jedním ze specifických aspektů hodnocení peněženek je, že existují požadavky na odolnost vůči útokům, jejichž posouzení vyžaduje specifické dovednosti, zejména v souvislosti s identifikací zranitelností a posouzením odolnosti vůči útokům (penetrační testování).

U všech požadavků, které zmiňují odolnost vůči útokům, musí v rámci přípravy na fázi 2 fáze 1 zahrnovat přezkum odůvodnění poskytnutého poskytovatelem peněženky, které vysvětluje, jak je odolnost vůči útokům budována. Audit fáze 1 musí také ve specifikacích identifikovat body, kterým je třeba věnovat pozornost pro fázi 2.

Pro tyto úkoly musí auditorský tým zajistit, aby měl požadované technické kompetence, které pravděpodobně vyžadují pomoc technických expertů.

V 1. fázi může být vhodné použít jako technické experty osoby, které budou v 2. fázi hrát roli inspektora, protože by jim to umožnilo seznámit se se specifikacemi komponent produktu.

Zprávy z 1. fáze musí také obsahovat:

- a) popis komponent řešení peněženky;
- b) stručné posouzení vhodnosti specifikací pro splnění kritérií odolnosti vůči útokům provedené auditorem, včetně identifikace bodů, kterým je třeba věnovat pozornost, a potenciálních zranitelností pro 2. fázi;

21.2.2 2. fáze auditu

V případě technických kontrol jsou cíle 2. fáze auditu:

- a) potvrdit, že návrh a implementace komponent řešení peněženky splňují specifikace auditované v 1. fázi; a
- b) u požadavků, které zmiňují úroveň odolnosti proti útokům, potvrdit, že je dosaženo očekávané úrovně odolnosti;
- c) ověřit, že bylo řádně provedeno funkční testování.

Za tímto účelem se audit zaměří na shromažďování důkazů o službě Peněženky na základě inspekčních činností s ohledem na:

- a) návrh a implementaci služby Peněženky;
- b) zneužitelnost potenciálních zranitelností a požadovaný potenciál útoku;

Audit zahrnuje činnost posouzení zranitelností, jak je definováno v příloze XI.

21.2.3 Postupy

Subjekt posuzování shody definuje postupy, které provádí, a to alespoň pro ty, které jsou uvedeny v příloze XI.