Obsah

PRÍLOHA I – Predmet certifikácie

Národná certifikačná schéma euróskej peňaženky digitálnej identity občana (EUDIW-SK)

Informatívny text – *poznámka k vypracovaniu: táto príloha zachováva európsky návrh zoznamu komponentov prílohy I ako štrukturálny východiskový bod. Pôvodné európske prvky, popisy a odkazy sú zachované v prvých troch stĺpcoch tabuliek I-1 až I-3. Slovenské národné rozšírenie je pridané v samostatných stĺpcoch a v nasledujúcich ustanoveniach o predmete pôsobnosti, aby príloha zostala kompatibilná s neskoršími prílohami o dôkazoch, hodnotiacich kritériách, metódach, podávaní správ o certifikátoch a certifikačnom procese.*

I.0 Preambula, logika vypracovania a štruktúra zhora nadol

Informatívny text: Táto príloha definuje predmet certifikácie pre národnú certifikačnú schému euróskej peňaženky digitálnej identity občana (EUDIW-SK) . Stanovuje predmet certifikácie, európsky základný katalóg komponentov, slovenské národné moduly, architektonické profily, modifikátory prípadov použitia, závislosti, environmentálne predpoklady a minimálne hranice podávania správ pre certifikát, verejnú certifikačnú správu a správu o posúdení certifikácie.

Informatívny text: Príloha je zámerne štruktúrovaná zhora nadol. Začína spoločnou európskou návrhovou štruktúrou, potom definuje národný predmet certifikácie a následne rozkladá predmet na slovenské certifikačné moduly, architektonické profily a toky prípadov použitia. Tým sa zabráni zmiešavaniu požiadaviek na dôkazy, hodnotiacich kritérií a hodnotiacich metód priamo v prílohe o rozsahu. Namiesto toho príloha I poskytuje mapu, ktorú môžu neskoršie prílohy použiť na mapovanie dôkazov, metódy hodnotenia a kontrolu procesu.

Vrstva	Účel v prílohe I	Výstup používaný v neskorších prílohách
1. Katalóg základných komponentov EÚ	Udržuje tabuľky návrhu prílohy I EÚ ako spoločný východiskový bod pre všetky rozhodnutia o predmete pôsobnosti EUDIW-SK.	Taxonómia komponentov a procesov pre dôkazy v prílohe IV, kritériá v prílohe X a metódy v prílohe XI.
2. Slovenský certifikačný objekt	Definuje, že predmetom certifikácie je poskytovanie a prevádzka riešenia peňaženky a schémy eID, v rámci ktorého sa poskytuje.	Hranice certifikátu, štruktúra CAR, vyhlásenie o predmete pôsobnosti žiadateľa a predmet akreditácie.
3. Spoločné pravidlá predmetu	Definuje spoločné komponenty, konfigurácie, prevádzkové procesy, hranice funkčnej zhody, závislosti a slovenské zákonné povinnosti.	Priečny balík dôkazov a spoločné audítorské postupy.
4. Slovenské moduly	Oddeľuje riešenie EUDIW-SK, službu SK-PID a službu SK-Validácia, pričom umožňuje vydanie zastrešujúceho certifikačného záveru.	Modulárne plánovanie posudzovania, analýza závislostí a konsolidácia správ.
5. Profily architektúry a modifikátory prípadov použitia	Definuje, ako sa architektúry Remote WSCD, Local External WSCD, Local Internal WSCD a Local Native WSCD deklarujú a posudzujú s použitím prípadov použitia Online a Proximity.	Mapovanie rizík špecifické pre profily, výber testov, posúdenie zraniteľnosti a logika výberu vzoriek.
6. Vykazovanie a sledovateľnosť	Definuje, čo musí byť uvedené v certifikáte a ako príloha I slúži ako podklad pre ďalšie prílohy.	Predmet verejného certifikátu, verejná certifikačná správa, matica artefaktov v prílohe IV, mapovanie v prílohách X/XI.

I.1 Taxonómia predmetu

Informatívny popis: Nasledujúce tabuľky zachovávajú štruktúru komponentov európskeho návrhu prílohy I na vysokej úrovni a rozširujú ju o slovenské certifikačné použitie. Prvé tri stĺpce by sa mali považovať za európsku základnú líniu. Dodatočné slovenské stĺpce vysvetľujú, ako sa každý prvok používa v definícii predmetu EUDIW-SK a ako podporuje neskoršie prílohy.

Prvok európskeho základu	Popis európskeho základného prvku	Referencie európskeho základu	Použitie v slovenskom predmete	Použitie pre neskoršie prílohy
Systém IKT	IKT systém, na ktorom je poskytovanie IKT služby založené. Upozorňujeme, že IT systém je zahrnutý ako kompletný stack, takže sa očakáva, že dôkaz o zhode bude k dispozícii pre celý systém.	Odkaz: - ETSI EN 319 401 - NIS2 CIR (EÚ) 2024/2690 - CIR (EÚ) 2015/1502, na úrovni záruky vysokaúrovni záruky vysoká eIDAS Ďalšie: - CEN TS 18026, úroveň významná - ISO/IEC 27001	Pre každý slovenský modul zahŕňa systém IKT v predmete pôsobnosti backendové aplikácie, infraštruktúru, platformy, bezpečnostné služby, administračné rozhrania, API, úložiská dátových ov, protokoly, prevádzkové nástroje a miesta hostingu, ktoré podporujú certifikovanú službu IKT. CAB bude s týmto systémom zaobchádzať ako s hranicou služby typu full-stack, nie ako s izolovaným softvérom.	Príloha IV: architektúra, základné konfigurácie, umiestnenia hostingu, toky údajov, rozhrania, dôkaz o aktuálnej certifikovanej verzii. Príloha X/XI: ISMS, analýza závislostí, inšpekcia inštalácie, skúšanie zraniteľnosti, prevádzková účinnosť.
Proces vývoja	Proces, ktorý prevádzkuje poskytovateľ služieb IKT na vývoj svojich služieb IKT.	Odkaz: - ETSI EN 319 401 Iné: - NIS2 CIR (EÚ) 2024/2690 - CEN TS 18026, úroveň záruky významná - ISO/IEC 27001	Slovenský predmet zahŕňa životný cyklus bezpečného vývoja pre peňaženku, PID, validáciu a backendové komponenty, vrátane riadenia požiadaviek, bezpečného kódovania, revízie kódu, integrity zostavenia, schvaľovania vydania a oddelenia medzi demo, pilotnými a produkčnými zostaveniami.	Príloha IV: dôkazy o SDLC, dôkazy o zdrojovom kóde, ak je to potrebné, SBOM, pôvod zostavenia, interné skúšanie. Príloha XI: revízia návrhu, revízia zdrojového kódu na základe vzoriek, opätovné vykonanie testov vývojármi.
Proces riadenia zmien	Proces prevádzkovaný poskytovateľom služieb IKT na riadenie zmien v službe IKT.	Odkaz: - ETSI EN 319 401 Iné: - NIS2 CIR (EÚ) 2024/2690 - CEN TS 18026, úroveň záruky významná - ISO/IEC 27001	Predmet zahŕňa schvaľovanie zmien, riadenie konfigurácie, správu verzií, núdzové zmeny, posudzovanie vplyvu na certifikáciu a pravidlá na určenie, či zmeny vyvolávajú údržbu certifikátu, opätovné posúdenie alebo recertifikáciu.	Príloha IV: politika verzií, záznamy o zmenách, poznámky k vydaniu, opatrenia na riadenie certifikovaných verzií. Príloha XI: odber vzoriek prevádzkovej účinnosti a preskúmanie spúšťačov údržby certifikátu.
Proces riadenia zraniteľností	Proces prevádzkovaný poskytovateľom služieb IKT na riadenie a riešenie zraniteľností v službe IKT.	Odkaz: - ETSI EN 319 401 - CRA príloha I, oddiel 2 Iné: - NIS2 CIR (EÚ) 2024/2690 - CEN TS 18026, úroveň záruky významná - ISO/IEC 27001	Predmet zahŕňa identifikáciu zraniteľností, triedenie, nápravu, zverejňovanie zraniteľností, opravy, kompenzačné opatrenia, monitorovanie známych zraniteľností komponentov tretích strán a akceptáciu rizika v prípade nevyriešených zraniteľností.	Príloha IV: politika zraniteľnosti, proces CVD, správy o skenovaní, výsledky penetračných testov, záznamy o zraniteľnostiach. Príloha X/XI: posúdenie zraniteľností, skúšanie backendu, skúšanie mobilných zariadení, verifikácia nápravy.
Proces riadenia incidentov	Proces prevádzkovaný poskytovateľom služieb IKT na riadenie a riešenie incidentov v oblasti kybernetickej bezpečnosti v rámci služieb IKT.	Odkaz: - ETSI EN 319 401 Iné: - NIS2 CIR (EÚ) 2024/2690 - CEN TS 18026, úroveň záruky významná - ISO/IEC 27001	Predmet zahŕňa detekciu incidentov, eskaláciu, hlásenie, obmedzenie, obnovu, analýzu príčin, oznamovanie príslušným orgánom v prípade potreby a prepojenie medzi reakciou na incidenty a udržiavaním certifikátu.	Príloha IV: postupy reakcie na incidenty, protokoly, register incidentov, dôkazy o kontinuite/obnove. Príloha XI: preskúmanie prevádzkovej účinnosti a výber vzoriek incidentov.
Proces riadenia podvodov	Proces, ktorý prevádzkuje poskytovateľ služieb IKT na riadenie podvodov v službách IKT.	Odkaz: - Príloha X	Predmet slovenského práva zahŕňa prevenciu, odhaľovanie a riešenie nezákonného alebo podvodného používania európskej peňaženky, zneužitie registrácie dôveryhodnej	Príloha IV: scenáre podvodov, pravidlá monitorovania, postupy podávania správ, postupy v prípade podozrenia z nezákonného používania.

			strany, podvodné vydávanie alebo predkladanie PID a zneužitie služieb validácie.	Príloha X/XI: posudzovanie rizík, audit procesov a skúšanie účinnosti opatrení.

Prvok riešenia európskej peňaženky	Popis európskej základnej úrovne	Odkazy na európsku základnú úroveň	Rozsah použitia na Slovensku	Použitie pre neskoršie prílohy
Inštancia peňaženky (všetky varianty)	Aplikácia, ktorá definuje používateľské rozhranie riešenia peňaženky. Môže existovať niekoľko variantov inštancie peňaženky, rôznych typov (webová, mobilná, pre PC atď.), určených pre rôzne architektúry.	Referencia: - CIR (EÚ) 2015/1502na úrovni záruky vysoká eIDAS, podľa potreby - Profil ochrany inštancie peňaženky FiTCEM - Príloha X	Všetky varianty inštancie peňaženky, ktoré sa uvádzajú pre slovenský certifikát, sú v predmete pôsobnosti. Varianta môže byť mobilná, webová, desktopová alebo iná implementácia, len ak je výslovne deklarovaná, verzionovaná a priradená k architektonickému profilu a modifikátoru prípadu použitia. Rôzne varianty sa nesmú skrývať pod jedným všeobecným tvrdením o inštancii peňaženky, ak zavádzajú podstatne odlišné bezpečnostné správanie.	Príloha IV: binárne súbory, SBOM, podporované platformy, ICS, preskúmanie ochrany súkromia už v štádiu návrhu, predpoklady týkajúce sa zariadení. Príloha XI: posúdenie zraniteľnosti mobilných zariadení alebo aplikácií, funkčné skúšanie, odôvodnenie výberu vzorky.
WSCA	Aplikácia, ktorá spravuje kritické aktíva prostredníctvom prepojenia s kryptografickým a nekryptografickým zariadením zabezpečujúcim peňaženku a využívaním funkcií, ktoré toto zariadenie poskytuje.	Odkaz: - CIR (EÚ) 2015/1502 na úrovni záruky vysoká eIDAS - Profil ochrany WSCA vo vývoji v rámci CEN TC224 WG17 - Príloha X	WSCA spadá do predmetu pôsobnosti vždy, keď ju poskytuje, integruje alebo na ňu spolieha poskytovateľ peňaženky. Ak je WSCA externá alebo samostatne certifikovaná, zostáva povinnou závislosťou a musí byť zahrnutá do analýzy závislostí a skúšania integrácie.	Príloha IV: Architektúra WSCA, ST/ETR alebo rovnocenné dôkazy, usmernenia k integrácii, predpoklady. Príloha X/XI: kritériá kryptografickej infraštruktúry, analýza závislostí, brána posudzovania zraniteľnosti.
Služba peňaženky	Služba hosťovaná v ICT systéme poskytovateľa peňaženky, ktorá podporuje jednotlivé jednotky peňaženky.	Odkaz: - CIR (EÚ) 2015/1502 na úrovni záruky vysoká eIDAS, podľa potreby - Príloha X	Služba peňaženky na Slovensku zahŕňa backendové funkcie podporujúce aktiváciu, poskytovanie, správu životného cyklu, zrušenie alebo pozastavenie, validáciu osvedčenia peňaženky a prepojenie s PID alebo inými národnými službami, ak je to relevantné.	Príloha IV: postupy životného cyklu, API, protokoly, dôkazy o validácii osvedčenia. Príloha X/XI: riadenie služieb, funkčná zhoda, posudzovanie rizík.
Proces načítania a aktualizácie	Procesy prevádzkované poskytovateľom služieb IKT na načítanie a aktualizáciu inštancie peňaženky a WSCA.	Odkaz: - ETSI EN 319 401 - Príloha X	Predmet slovenského riadenia zahŕňa bezpečné načítanie, počiatočné nastavenie, distribúciu aktualizácií, prevenciu vrátenia do predchádzajúcej verzie, vynútenie verzie, podpisovanie verzií, opatrenia v obchode s aplikáciami alebo podnikovej distribúcii a aktualizáciu komponentov WSCA alebo súvisiaceho firmvéru, ak je to relevantné.	Príloha IV: návrh bezpečnej aktualizácie, postup vydávania verzií, podpisové kľúče, protokoly aktualizácií. Príloha XI: inšpekcia procesu aktualizácie, posúdenie zraniteľnosti a preskúmanie riadenia zmien.
Služba poskytovania a správy peňaženky	Služba IKT prevádzkovaná poskytovateľom služieb IKT na účely poskytovania peňaženky EUDI a jej správy počas celého jej životného cyklu.	Odkaz: - CIR (EÚ) 2015/1502 na úrovni záruky vysoká eIDAS - ETSI EN 319 401 - Príloha X	Predmet slovenského overu zahŕňa registráciu, vytvorenie peňaženky, aktiváciu jednotky peňaženky, správu stavu životného cyklu, obnovenie, zrušenie, prípadné pozastavenie, podporu pri registrácii používateľov a rozhrania so službami validácie PID a spoliehajúcich sa strán.	Príloha IV: politika poskytovania, model stavu životného cyklu, dôkazy o procesoch, dôkazy o integrácii. Príloha X/XI: hodnotenie onboarding/registrácia/aktivácia, prevádzková účinnosť, skúšanie funkčnej integrácie.

Európsky základný prvok	Popis európskej základnej úrovne	Odkazy na európsku základnú úroveň	Použitie v slovenskom kontexte	Použitie pre neskoršie prílohy
WSCD	Zariadenie odolné proti manipulácii, ktoré poskytuje prostredie prepojené s bezpečnou kryptografickou aplikáciou peňaženky a používané touto aplikáciou na ochranu kritických aktív a poskytovanie kryptografických funkcií na bezpečné vykonávanie kritických operácií.	Odkaz: - CIR (EÚ) 2015/1502 na úrovni záruky vysoká eIDAS - Príslušné technické oblasti EUCC	WSCD môže byť vzdialené, lokálne externé, lokálne interné alebo založené na natívnej platforme, v závislosti od deklarovaného architektonického profilu. Môže byť priamo v predmete pôsobnosti alebo sa môže považovať za povinnú závislosť. Vo všetkých prípadoch musí žiadateľ identifikovať hranice WSCD, dôkazy o záruke, predpoklady, obmedzenia integrácie a zvyškové riziko.	Príloha IV: certifikáty, ST/ETR, usmernenia k integrácii, prevádzkové predpoklady. Príloha X/XI: kritériá kryptografickej infraštruktúry, analýza závislostí, skúšanie špecifické pre profil.
Služba peňaženky	Služba IKT poskytovaná poskytovateľom peňaženky na implementáciu niektorých funkcií jednotky peňaženky do jeho systémov IKT.	Odkaz: - CIR (EÚ) 2015/1502 na úrovni záruky vysoká eIDAS - Príloha X	Ak peňaženka závisí od funkcií hostovaných na backende, tieto funkcie sú zahrnuté v predmete služby peňaženky alebo sú identifikované ako závislosti. Certifikát nesmie implikovať offline alebo on-device záruku pre funkcie, ktoré sú skutočne implementované backendovými službami.	Príloha IV: diagramy architektúry a hraníc dôveryhodnosti, popis online/offline závislostí. Príloha X/XI: funkčné skúšanie, analýza závislostí, mapovanie rizík ONL/PRX.

I.2 Predmet národnej certifikačnej schémy európskej peňaženky digitálnej identity občana (EUDIW-SK) a celkový predmet

Normatívna požiadavka: Predmetom certifikácie v rámci tejto národnej certifikačnej schémy MUSÍ byť poskytovanie a prevádzka riešenie peňaženky a systémov elektronickej identifikácie, v rámci ktorých sú poskytované, a to v rozsahu uvedenom v predmete certifikátu a potvrdenom certifikačným orgánom.

Normatívna požiadavka: Certifikácia v rámci tejto certifikačnej schémy MUSÍ pokrývať celý životný cyklus certifikovaných služieb IKT na úrovni záruky vysoká, vrátane registrácie používateľov, zapojenia, správy prostriedkov elektronickej identifikácie, správy životného cyklu peňaženiek, poskytovania, prevádzky, údržby, aktualizácie, riešenia incidentov, riešenia zraniteľností a organizačných opatrení potrebných na udržanie certifikovaného stavu.

Normatívna požiadavka: Predmet certifikácie MÔŽE byť hodnotený ako zložený objekt pozostávajúci z koordinovaných modulov. Ak je modul certifikovaný samostatne alebo sa opiera o samostatne certifikované komponenty, záver certifikácie na najvyššej úrovni MUSÍ zostať v súlade s hranicami modulu, predpokladmi, závislosťami a zdieľanými auditovateľnými procesmi zaznamenanými v tejto prílohe.

Hodnotiaca činnosť CAB: CAB MUSÍ overiť certifikačný cieľ, deklarovaný predmet, deklarovaný modul alebo moduly, deklarovaný architektonický profil alebo profily, modifikátory prípadov použitia ONL a PRX, externé závislosti, predpoklady týkajúce sa prostredia a navrhovaný plán hodnotenia. CAB MUSÍ určiť, či implementácia zodpovedá deklarovanej architektúre a či navrhovaný plán hodnotenia zodpovedá predmetu špecifickému pre profil a vystaveniu riziku.

Hodnotiaca činnosť CAB: CAB MUSÍ vydať alebo podporiť súhrnnú správu o posúdení certifikácie, ktorá konsoliduje hodnotené moduly, a MUSÍ zabezpečiť, aby akýkoľvek záver certifikácie na najvyššej úrovni bol v súlade so zloženou maticou a s analýzou závislostí vykonanou pre opätovne použiteľné informácie o zabezpečení.

I.2.1 Zložená certifikačná matica

Informatívny popis: Nasledujúca matica definuje minimálnu slovenskú modulárnu štruktúru. Slúži ako pomôcka pri implementácii na definovanie hraníc certifikátov, povinných závislostí a spoločných auditovateľných procesov. Nezabraňuje vlastníkovi schémy definovať ďalšie moduly, ak sa národná architektúra vyvíja.

Názov modulu	Spracovanie certifikátu	Povinné profily / kvalifikátory predmetu	Povinné závislosti	Spoločné auditovateľné procesy
Riešenie EUDIW-SK	Riešenie peňaženky Certifikát alebo modul tvoriaci súčasť zastrešujúceho certifikátu	Jeden alebo viac deklarovaných architektonických profilov A, B, C alebo D pre deklarované toky transakcií v predmete; musia byť deklarované modifikátory prípadov použitia ONL a/alebo PRX.	Inštancia peňaženky, komponenty WSCA a WSCD poskytované priamo alebo nepriamo poskytovateľom peňaženky. Externé komponenty WSCA/WSCD, PID, validácia, QTSP, infraštruktúry alebo platformy sa musia identifikovať ako závislosti alebo predpoklady a vyhodnotiť prostredníctvom analýzy závislostí a posúdenia vhodnosti.	Vývoj, riadenie zmien, riadenie zraniteľností, riadenie incidentov, riadenie podvodov, bezpečná aktualizácia, riadenie verzií, riadenie životného cyklu peňaženky.
Služba SK-PID	Certifikát poskytovateľa PID alebo modul tvoriaci súčasť zastrešujúceho certifikátu	Neplatí pre architektonické profily WSCD, pokiaľ nie je vydávanie PID technicky viazané na kryptografické komponenty peňaženky. Pre vydávanie PID a overovanie totožnosti sa musí preukázať úroveň záruky vysoká.	Backend ISMS, schéma eID, úroveň záruky vysoká, rozhrania zdrojového registra, osvedčenie peňaženky alebo ekvivalentné overenie s vysokou úrovňou záruky, národné formáty údajov PID.	Zaregistrovanie používateľa, verifikácia identity, poskytovanie PID, správa životného cyklu PID, správa zraniteľností a incidentov.
Služba validácie SK	Certifikát služby pre validáciu alebo modul tvoriaci súčasť zastrešujúceho certifikátu	Neplatí pre architektonické profily WSCD, pokiaľ validácia nie je technicky viazaná na kryptografickú architektúru alebo architektúru overovateľa špecifickú pre peňaženku.	Backend ISMS, register dôveryhodných strán, validačné mechanizmy, kotvy dôvery, závislosti od národnej infraštruktúry a bezplatné mechanizmy validácie.	Prevádzka validačných mechanizmov, overovanie identity spoliehajúcej sa strany, riadenie dostupnosti, riadenie zraniteľností a incidentov.
Spoločné alebo externé závislosti	Závislosť alebo opakovane použiteľný vstup záruky, nie nevyhnutne samostatný certifikát v rámci tejto schémy	Podľa toho, čo sa vzťahuje na modul, ktorý sa spolieha na závislosť.	Stav alebo zmluva QTSP, certifikovaný HSM/WSCD, dôkazy podľa ISO/IEC 27001 alebo ETSI, certifikáty EUCC alebo Common Criteria, výsledky FCAF, výstupy z národných auditov kybernetickej bezpečnosti.	Analýza závislostí, klasifikácia prípustnosti, integračné skúšanie, verifikácia kompenzačných opatrení.

I.3 Spoločný predmet pre všetky certifikované služby EUDIW-SK

I.3.1 Komponenty, konfigurácie a hranice celého stacku

Normatívna požiadavka: Predmet certifikácie MUSÍ zahŕňať všetky softvérové komponenty certifikovanej služby IKT, vrátane ich nastavení, základných konfigurácií, parametrov nasadenia, identifikátorov verzií a bezpečnostných možností zostavenia alebo behu.

Normatívna požiadavka: Predmet certifikácie MUSÍ zahŕňať hardvérové komponenty a platformy, na ktorých bežia certifikované softvérové komponenty alebo na ktorých závisia pri kritických operáciách, ak sú tieto komponenty poskytované priamo alebo nepriamo riešením peňaženky, službou PID, službou validácie, schémou elektronickej identifikácie alebo iným poskytovateľom v predmete certifikácie a ak sa od nich vyžaduje, aby spĺňali požadovanú úroveň záruky.

Normatívna požiadavka: Ak hardvérové komponenty alebo platformy neposkytuje poskytovateľ peňaženky ani iný poskytovateľ v predmete pôsobnosti, predmet certifikácie MUSÍ zaznamenať bezpečnostné predpoklady, za ktorých je možné zabezpečiť odolnosť proti útočníkom s vysokým útočným potenciálom. Predmet MUSÍ tiež identifikovať hodnotiace činnosti potrebné na potvrdenie týchto predpokladov.

Hodnotiaca činnosť CAB: CAB MUSÍ identifikovať každú softvérovú zložku v predmete pôsobnosti, základnú konfiguráciu, hardvérovú závislosť, platformovú závislosť a predpoklad týkajúci sa prostredia, ktoré sú potrebné na dosiahnutie vysokého stupňa záruky. Ak platformu poskytujú zariadenia koncových používateľov, CAB MUSÍ overiť, či existujú zdokumentované predpoklady a či žiadateľ implementuje opatrenia na potvrdenie týchto predpokladov v praxi.

I.3.2 Prevádzkové procesy vrátane zákonných povinností v Slovenskej republike

Normatívna požiadavka: Predmet certifikácie MUSÍ zahŕňať procesy podporujúce poskytovanie a prevádzku riešenia peňaženky a súvisiacich služieb, vrátane aspoň registrácie používateľov, zapojenia, správy prostriedkov elektronickej identifikácie a organizácie podľa oddielov 2.1, 2.2 a 2.4 prílohy I k vykonávaciemu nariadeniu (EÚ) 2015/1502, ak sú relevantné pre certifikovaný modul.

Normatívna požiadavka: Predmet posudzovania zhody MUSÍ výslovne zahŕňať prevádzkové procesy a technické schopnosti vyžadované slovenským zákonom č. 272/2016 Z. z. o dôveryhodných službách v znení neskorších predpisov, ak sa takéto povinnosti vzťahujú na poskytovateľa peňaženky, príslušný vnútroštátny orgán, poskytovateľa PID alebo inú úlohu v rozsahu pôsobnosti.

Normatívna požiadavka: Žiadateľ MUSÍ identifikovať konkrétne ustanovenia slovenského zákona č. 272/2016 Z. z. o dôveryhodných službách v znení neskorších predpisov, ktoré zakladajú každú z nižšie uvedených uplatniteľných povinností. Ak z balíka dôkazov nie je zrejmý presný právny základ, žiadateľ MUSÍ predložiť právne mapovanie potvrdené príslušným slovenským orgánom alebo právnym poradcom, skôr ako sa CAB bude opierať o túto povinnosť pre predmet certifikácie.

- na žiadosť orgánu poskytnúť informácie potrebné na monitorovanie dodržiavania predpisov alebo zhody;
- prijať nápravné opatrenia uložené orgánom s cieľom odstrániť nesúlad s predpismi alebo zhodou;
- pozastaviť alebo zrušiť registráciu spoliehajúcej sa strany na základe rozhodnutia úradu;
- bezodkladne nahlásiť spoliehajúce sa strany Ministerstvu vnútra automatizovaným spôsobom počas procesu registrácie;
- bezodkladne nahlásiť orgánu akékoľvek podozrenie z nezákonného alebo podvodného používania európskej peňaženky;
- bezodkladne umožniť spoliehajúcim sa stranám aktualizovať certifikáty a prostriedky vzájomnej autentifikácie s európskou peňaženkou.

Hodnotiaca činnosť CAB: CAB MUSÍ preskúmať zdokumentované prevádzkové postupy, technické rozhrania, logovanie, postupy eskalácie, komunikačné kanály s orgánom a dôkazy o prevádzke pre každú príslušnú povinnosť. CAB MUSÍ overiť, či sú zodpovednosti, rozhodovacie právomoci, mechanizmy vynútiteľnosti a auditové stopy implementované a auditovateľné.

I.3.3 Hranica funkčnej zhody

Normatívna požiadavka: Skúšanie funkčnej zhody v rámci tejto schémy SA MUSÍ posudzovať oddelene od hodnotenia zabezpečenia kybernetickej bezpečnosti, vrátane penetračných testov, analýzy zraniteľnosti podľa spoločných kritérií a auditov ISMS. Funkčné skúšanie SA NESMIE používať ako náhrada za činnosti hodnotenia bezpečnosti požadované pre úroveň záruky vysoká.

Normatívna požiadavka: Rámec Európskej komisie pre posudzovanie funkčnej zhody (FCAF), ak je dostupný a je to primerané, MUSÍ byť štandardnou implementáciou funkčnej zhody na skúšanie integrity, základných funkcií, protokolov a rozhraní, ktoré sú stanovené príslušnými aktmi Únie, na ktoré odkazuje databáza požiadaviek.

Normatívna požiadavka: Okrem základných testovacích súborov FCAF MUSÍ hranica funkčnej zhody pre Slovensko zahŕňať slovenský národný integračný testovací súbor alebo ekvivalentnú národnú testovaciu základňu, ktorú spravuje príslušný slovenský orgán, na účely povinného skúšania technickej interoperability s národnou infraštruktúrou.

Hodnotiaca činnosť CAB: CAB MUSÍ vykonávať alebo sledovať funkčné integračné testy overujúce integráciu s národnými mechanizmami registrácie alebo validácie spoliehajúcich sa strán, s národným poskytovateľom PID na bezpečné vydávanie a prepojenie PID a s akýmikoľvek bezplatnými validačnými mechanizmami poskytovanými členským štátom.

Normatívna požiadavka: Schéma MUSÍ zostať nezávislá od nástrojov. CAB MÔŽE používať proprietárne, open-source alebo nástroje tretích strán na vykonávanie alebo automatizáciu testovacích špecifikácií, za predpokladu, že vykonané testovacie ciele, očakávané výsledky a sledovateľnosť podávania správ zostanú ekvivalentné s uvedenými testovacími súbormi.

Hodnotiaca činnosť CAB: CAB MUSÍ zdokumentovať výsledky funkčného skúšania pomocou prístupu vyhlásenia o zhode implementácie alebo ekvivalentnej štruktúry podávania správ, ktorá zachováva sledovateľnosť od deklarovanej funkcie po cieľ skúšania, vstup skúšania, očakávaný výsledok, skutočný výsledok, odchýlku a záver.

I.3.4 Závislosť a hranica záruky opätovnej použiteľnosti

Normatívna požiadavka: Ak sa certifikácia opiera o externé komponenty, podslužby, existujúce certifikáty alebo predchádzajúce posudzovanie zhody, tieto prvky MUSIA byť identifikované buď ako komponenty v predmete pôsobnosti, závislosti, predpoklady prevádzkového prostredia, alebo ako prvky mimo predmetu pôsobnosti. Nejednoznačné zaobchádzanie s predmetom pôsobnosti nie je povolené.

Normatívna požiadavka: Informácie o opätovne použiteľnej záruke MÔŽU podporiť záver certifikácie až po tom, čo CAB posúdila ich autentickosť, predmet, platnosť, spôsobilosť vydavateľa, predpoklady, nezhody, obmedzenia integrácie a relevantnosť pre súčasnú slovenskú architektúru.

Hodnotiaca činnosť CAB: CAB MUSÍ klasifikovať opakovane použiteľné informácie o záruke ako prijaté bez ďalších činností, prijaté s kompenzačnými opatreniami, prijaté s ďalším skúšaním CAB alebo zamietnuté. Táto klasifikácia MUSÍ byť zaznamenaná ako vstup do Správy o certifikačnom posúdení.

I.4 Predmet slovenských certifikačných modulov

I.4.1 Modul riešenia EUDIW-SK

Normatívna požiadavka: Riešenie peňaženky MÔŽE byť certifikované ako samostatný modul za predpokladu, že výsledok certifikácie na najvyššej úrovni pokrýva ako riešenie peňaženky, tak aj systém elektronickej identifikácie, v rámci ktorého je poskytované, ak celkový certifikovaný objekt zahŕňa oboje.

Normatívna požiadavka: Ak sa žiada o certifikáciu riešenia peňaženky ako samostatného modulu, cieľ certifikácie MUSÍ zahŕňať minimálne tieto prvky:

- inštanciu peňaženky vo všetkých deklarovaných variantoch a súvisiace softvérové komponenty;
- bezpečnú kryptografickú aplikáciu peňaženky (WSCA), či už poskytovanú priamo, alebo využívanú prostredníctvom externej závislosti;
- hranice alebo závislosti zariadenia Wallet Secure Cryptographic Device (WSCD), vrátane dôkazov o záruke a predpokladov týkajúcich sa prostredia;
- IKT systémy a backendové služby podporujúce jednotky peňaženky, životný cyklus peňaženky a správu peňaženky;
- procesy načítania, poskytovania, správy a aktualizácie inštancie peňaženky, WSCA a súvisiacich backendových komponentov;
- procesy vývoja, zmien, zraniteľnosti, incidentov a riadenia podvodov;
- rozhrania so službami PID, službami validácie, mechanizmami spoliehajúcich sa strán, dôveryhodnými službami a inou národnou infraštruktúrou potrebnou na udržanie vysokého stupňa záruky.

Hodnotiaca činnosť CAB: CAB MUSÍ overiť uvedené hranice modulu. Ak riešenie peňaženky závisí od externých modulov, ako je samostatná služba vydávania PID, externá služba validácie, QTSP, certifikovaný HSM alebo externe certifikované WSCD, CAB MUSÍ vykonať analýzu závislostí a skúšanie rozhraní v rozsahu dostatočnom na potvrdenie, že kompozitné riešenie spĺňa úroveň záruky vysoka.

I.4.2 Modul služby SK-PID

Normatívna požiadavka: Ak sa žiada o certifikáciu služieb na poskytovanie údajov o identifikácii osoby (PID), cieľ certifikácie MUSÍ zahŕňať aspoň systém IKT, službu poskytovania a správy PID, procesy vývoja a riadenia zmien, procesy riadenia zraniteľnosti, incidentov a podvodov a procesy registrácie používateľov a verifikácie identity.

Normatívna požiadavka: Služba PID MUSÍ byť preukázaná v súlade s príslušnými požiadavkami vykonávacieho nariadenia (EÚ) 2015/1502 pre úroveň záruk vysoká, ak sa vydávanie PID používa na podporu peňaženky alebo schémy eID s stupňom záruky „vysoký“.

Hodnotiaca činnosť CAB: CAB MUSÍ vyhodnotiť procesy implementované poskytovateľom PID vo vzťahu k príslušným požiadavkám na registráciu, správu prostriedkov elektronickej identifikácie a organizačné opatrenia. Ak poskytovateľ PID pôsobí v rámci slovenskej kompozitnej architektúry, CAB MUSÍ overiť, či vydávanie PID overuje a vykonáva validáciu osvedčenia peňaženky pred vydaním, alebo používa iný povolený mechanizmus s vysokou úrovňou záruky. CAB MUSÍ prostredníctvom funkčného skúšania overiť, či sa PID vydáva v povinných formátoch požadovaných platnými právnymi predpismi Únie a vnútroštátnymi technickými špecifikáciami.

I.4.3 Modul služby SK-Validácia

Normatívna požiadavka: Ak sa žiada o certifikáciu služieb validácie, cieľ certifikácie MUSÍ zahŕňať systémy IKT a prevádzkové procesy podporujúce validačný mechanizmus, vrátane procesov riadenia vývoja, zmien, zraniteľnosti, incidentov a podvodov.

Normatívna požiadavka: Validačná služba MUSÍ podporovať povinnosti členského štátu v oblasti overovania pravosti a platnosti registrovaných spoliehajúcich sa strán a MUSÍ byť navrhnutá a prevádzkovaná s primeranou odolnosťou pre úroveň záruky vysoká , ak takúto záruku vyžaduje celková architektúra, model dôvery spoliehajúcich sa strán alebo prípad použitia.

Hodnotiaca činnosť CAB: CAB MUSÍ overiť, či členský štát v prípade potreby poskytuje bezplatné mechanizmy validácie a či tieto mechanizmy umožňujú používateľom alebo dôverujúcim stranám, podľa potreby, overiť pravosť a platnosť identity registrovaných dôverujúcich strán. CAB MUSÍ vykonať audit príslušného systému riadenia informačnej bezpečnosti (ISMS) a technických opatrení validačného mechanizmu s cieľom zabezpečiť vysokú dostupnosť a odolnosť voči útočníkom s vysokým útočným potenciálom, zodpovedajúcu deklarovanej kritickosti služby a modelu hrozieb.

I.4.4 Vydavatelia poverení, služby QTSP a iné súvisiace služby

Normatívna požiadavka: Kvalifikovaní alebo nekvalifikovaní vydavatelia osvedčení o elektronických atribútoch, poskytovatelia dôveryhodných služieb, podpisové služby, služby na začlenenie spoliehajúcich sa strán a iné súvisiace služby MUSIA byť zahrnuté do certifikátu EUDIW-SK len vtedy, ak ich žiadateľ výslovne uvádza ako súčasť certifikovaného objektu. V opačnom prípade sa s nimi MUSÍ zaobchádzať ako so závislosťami, predpokladmi prevádzkového prostredia alebo službami mimo predmetu s jasne zaznamenanými rozhraniami a zvyškovými rizikami.

Hodnotiaca činnosť CAB: CAB MUSÍ overiť, či akákoľvek dôvera v status QTSP, posudzovanie zhody dôveryhodných služieb, záruka zdroja atribútov alebo záruka externého vydavateľa podlieha analýze závislostí a nevytvára nepodložené certifikačné tvrdenie pre komponenty mimo predmetu hodnotenia.

I.5 Architektonické profily a modifikátory prípadov použitia

Informatívny text: Aby bola schéma pripravená na budúcnosť a uplatniteľná pre verejných alebo súkromných poskytovateľov peňaženiek, schéma definuje univerzálne teoretické profily WSCD. Každý poskytovateľ, ktorý žiada o certifikáciu, musí vybrať príslušný profil alebo profily, uplatniť príslušné modifikátory prípadov použitia Online a/alebo Proximity a priradiť konkrétnu slovenskú implementáciu k vybranej základnej línii profilu.

Normatívna požiadavka: Pre každú zahrnutú architektúru MUSÍ žiadateľ poskytnúť popis konkrétnej architektúry, bezpečnostné opatrenia spojené s vysokým stupňom záruky, plán hodnotenia, bezpečnostné požiadavky zohľadňujúce register rizík Únie, priradenie opatrení k komponentom a popis účinnosti.

Hodnotiaca činnosť CAB: Pre každý deklarovaný profil MUSÍ CAB overiť, či implementovaná architektúra zodpovedá deklarovanej architektúre a či sú všetky požiadavky profilu prítomné a konzistentné v rámci hodnotiaceho plánu, mapovania rizík, mapovania opatrení na riadenie, závislostí a súboru dôkazov.

Profil	Popis profilu	Minimálny predmet a dôsledky hodnotenia

Profil A – Architektúra vzdialeného WSCD	WSCD je vzdialené zariadenie, napríklad HSM alebo cloudové HSM, ku ktorému sa pristupuje cez sieť. Komponenty v predmete zvyčajne zahŕňajú inštanciu peňaženky, backend poskytovateľa peňaženky, vzdialenú WSCA a vzdialenú WSCD.	CAB overuje dôkazy o záruke WSCD, hranice TOE, platnosť certifikátov, komunikačné kanály medzi inštanciou peňaženky/backendom/WSCA/WSCD, argument o výhradnej kontrole, obmedzenia používania kľúčov a reziduálnu expozíciu. Tvrdenia o nižšej úrovni záruky pre časti WSCA musia byť odôvodnené analýzou rizík a závislostí.
Profil B – Lokálna externá architektúra WSCD	WSCD je externé hardvérové zariadenie, napríklad čipová karta alebo identifikačná karta, pripojené k zariadeniu používateľa prostredníctvom NFC alebo iného kanála s krátkym dosahom.	CAB overuje záruky o zabezpečení externého WSCD, vyvolanie WSCD inštanciou peňaženky, ochranu proti extrakcii alebo kompromitácii prostredníctvom operačného systému zariadenia používateľa, ochranu kanála a predpoklady toku PRX/ONL.
Profil C – Lokálna interná architektúra WSCD	WSCD je integrované priamo do zariadenia používateľa, napríklad ako vstavaný bezpečnostný prvok alebo eSIM. Keďže platformu nemusí poskytovať poskytovateľ peňaženky, sú potrebné prísne predpoklady týkajúce sa platformy.	CAB overuje zdokumentované predpoklady týkajúce sa hardvéru a operačného systému, mechanizmy verifikácie behu, ako je osvedčenie zariadenia, podmienky poskytovania, reziduálna expozícia a kompatibilita s vysokým stupňom záruky.
Profil D – Lokálna natívna architektúra WSCD	WSCD je komponent zabudovaný v zariadení používateľa, ku ktorému sa pristupuje prostredníctvom natívneho rozhrania API operačného systému, napríklad zabezpečenej enklávy operačného systému. Tento profil je vyhradený pre budúci vývoj trhu, keď budú k dispozícii primerané dôkazy o záruke.	Profil D je v súčasnosti predmetom obmedzenej dostupnosti dôkazov o záruke. Žiadateľ, ktorý žiada o certifikáciu podľa profilu D, MUSÍ preukázať, že vybraný WSCD alebo natívne zabezpečené prostredie poskytuje odolnosť voči útočníkom s vysokým útočným potenciálom prostredníctvom formálnych dôkazov o záruke, odôvodnenia rizika a doplňujúcich hodnotiacich činností dohodnutých s CAB. CAB MUSÍ pred vydaním certifikátu zdokumentovať každé rozhodnutie o certifikácii podľa profilu D a jeho odôvodnenie.

I.5.1 Modifikátory prípadov použitia

Normatívna požiadavka: Každý poskytovateľ peňaženky, ktorý žiada o certifikáciu, MUSÍ výslovne uviesť, ktorý architektonický profil alebo profily sa uplatňujú, a MUSÍ preukázať, ako vybraná architektúra funguje v rámci deklarovaných tokov online a/alebo bezkontaktných transakcií v predmete pôsobnosti.

Normatívna požiadavka: V prípade prípadov použitia Online (ONL) MUSÍ žiadateľ identifikovať deklarované toky transakcií ONL a poskytnúť mapovanie rizík špecifické pre architektúru pre tieto toky, vrátane hrozieb spojených so vzdialenou prezentáciou, dostupnosťou backendu, bezpečnosťou protokolu, autentizáciou spoliehajúcej sa strany, súhlasom používateľa a viazaním kanálu.

Normatívna požiadavka: V prípade prípadov použitia typu Proximity (PRX) MUSÍ žiadateľ opísať deklarovanú architektúru PRX, hranice dôvery, predpoklady pripojiteľnosti, použitie NFC, BLE, interakcie založenej na QR alebo ekvivalentnej interakcii na krátku vzdialenosť a použitie komponentov WSCD a WSCA pre tok prezentácie typu Proximity.

Hodnotiaca činnosť CAB: CAB MUSÍ vyhodnotiť mapovanie rizík špecifických pre architektúru pre toky ONL a PRX v rámci metodiky posudzovania rizík typu „challenge-and-review“. Ak sú komponenty WSCD alebo WSCA externé, samostatne certifikované alebo podporované opakovane použiteľnými informáciami o záruke, CAB MUSÍ overiť vhodnosť týchto informácií o záruke, predpokladov prevádzkového prostredia, obmedzení integrácie a kompenzačných opatrení pre deklarovaný tok.

I.5.2 Opis účinnosti

Normatívna požiadavka: Pre vybranú kombináciu architektonických profilov a modifikátorov prípadov použitia MUSÍ žiadateľ poskytnúť popis vysvetľujúci, ako bezpečnostné opatrenia, mapovania, bezpečnostné požiadavky a plán hodnotenia spoločne riešia riziká a hrozby identifikované pre architektúru až do požadovaného stupňa záruky.

Hodnotiaca činnosť CAB: CAB MUSÍ posúdiť súdržnosť argumentu o účinnosti prostredníctvom výberu kritických hrozieb z modifikátorov ONL a PRX a overením, či sú implementované opatrenia zdokumentované a skúšané podľa plánu, vrátane činností posudzovania zraniteľnosti relevantných pre útočníkov s vysokým útočným potenciálom.

I.6 Slovenská národná inštanciácia a podávanie správ o predmete

Normatívna požiadavka: Žiadateľ MUSÍ identifikovať konkrétnu slovenskú implementačnú architektúru, deklarovaný predmet služieb, deklarované moduly, deklarované architektonické profily, deklarované modifikátory prípadov použitia, deklarované verejné a neverejné rozhrania, prevádzkové lokality a všetky relevantné závislosti.

Normatívna požiadavka: Osvedčenie o zhode, verejná certifikačná správa a správa o certifikačnom posúdení MUSIA jasne uvádzať posudzovaný predmet, architektonické hranice, predpoklady týkajúce sa prostredia, závislosti, hodnotené komponenty, hodnotené verzie, hodnotené prípady použitia, vylúčené komponenty, opätovne použiteľné informácie o záruke a obmedzenia predmetu.

Normatívna požiadavka: Ak sa certifikácia vykonáva počas vývoja, pilotnej prevádzky alebo postupného nasadenia, konečné osvedčenie MUSÍ rozlišovať medzi dôkazmi zhromaždenými z pilotných alebo kontrolovaných prostredí a dôkazmi platnými pre certifikovaný objekt v produkčnom prostredí. Demo alebo testovacie komponenty NESMÚ byť automaticky považované za komponenty certifikované pre produkčné prostredie.

Hodnotiaca činnosť CAB: CAB MUSÍ určiť, či implementovaná slovenská architektúra zodpovedá deklarovanému predmetu a či sú súbor dôkazov, analýza závislostí a hodnotiace činnosti dostatočné na podloženie tvrdení uvedených v certifikáte. Akýkoľvek nesúlad medzi deklarovanou a implementovanou architektúrou MUSÍ byť zaznamenaný a vyriešený pred prijatím rozhodnutia o certifikácii.

I.7 Mapa sledovateľnosti pre neskoršie prílohy

Informatívny popis: Príloha I je mapou predmetu. Následné prílohy by mali používať nižšie uvedené prvky ako stabilné referencie pre požiadavky na dôkazy, hodnotiace kritériá, hodnotiace metódy a kroky certifikačného procesu.

Prvok prílohy I	Ako definuje predmet	Mapovanie dôkazov v prílohe IV	Mapovanie kritérií v prílohe X	Mapovanie metód v prílohe XI
Európske základné komponenty a procesy z tabuliek I-1 až I-3	Taxonómia komponentov, predmet prevádzkových procesov a kategórie opakovateľných záruk.	Architektonický balík, referenčné konfigurácie, dôkazy SDLC, záznamy o zmenách, dôkazy o zraniteľnosti a incidentoch, certifikáty komponentov.	Kritériá pre riadenie IKT, kryptografickú infraštruktúru, inštanciu peňaženky, funkčnú zhodu a komplexné hodnotenie.	Audit procesov, inšpekcia architektúry, skúšanie zraniteľnosti, analýza závislostí, preskúmanie účinnosti prevádzky.
Modul riešenia EUDIW-SK	Inštancia peňaženky, závislosť WSCA/WSCD, služba jednotky peňaženky, služba poskytovania a správy, procesy aktualizácie a životného cyklu.	Binárne súbory, SBOM, ICS, dôkazy o bezpečných aktualizáciách, dôkazy o bezpečnosti mobilných zariadení/aplikácií, dôkazy o backende, dôkazy o správe kľúčov.	Kritériá inštancie peňaženky, kryptografické kritériá, funkčná zhoda, riadenie a právna oprávnenosť.	Skúšanie mobilných zariadení/aplikácií, testy protokolov, testy integrácie FCAF/národné testy integrácie, analýza závislostí WSCD/WSCA, penetračné testovanie.
Modul služby SK-PID	Vydávanie PID, overovanie identity, prepojenie schémy eID a správa životného cyklu.	Dátový model PID, politika vydávania PID, dôkazy overenia identity, dôkazy zdrojového registra, dôkazy osvedčenia peňaženky.	Zhoda PID, LoA High overovanie identity, zhoda formátu údajov, kontrolné opatrenia riadenia.	Audit procesov, funkčné skúšanie, skúšanie rozhraní, posudzovanie rizík a vzorkovanie účinnosti prevádzky.
Modul služby SK-Validácia	Validácia spoliehajúcej sa strany, kotvy dôvery, rozhrania registrov a výsledky validácie.	Dokumentácia validácie API, dôkazy o registri spoliehajúcej sa strany, protokoly, dôkazy o dostupnosti, záznamy o incidentoch a zraniteľnostiach.	Funkčné a bezpečnostné kritériá validačnej služby, požiadavky na dostupnosť a integritu.	Funkčná validácia, inšpekcia API, audit ISMS, preskúmanie dostupnosti a procesu riešenia incidentov.
Architektonické profily A-D a modifikátory ONL/PRX	Predpoklady špecifické pre profil, hranice dôvery a vystavenie riziku.	Deklarácia profilu, mapovanie rizík špecifické pre architektúru, predpoklady týkajúce sa zariadení/platforiem, dôkazy o certifikovaných komponentoch.	Bezpečnostné opatrenia špecifické pre profil a argumentácia o účinnosti.	Analýza závislostí, posúdenie zraniteľnosti, funkčné testy špecifické pre profil, odôvodnenie výberu vzorky.
Slovenské zákonné povinnosti podľa zákona č. 272/2016 Z. z.	Spolupráca orgánov, nápravné opatrenia, pozastavenie/zrušenie registrácie dôverujúcej strany, automatizované hlásenie dôverujúcej strany, hlásenie nezákonného/podvodného použitia, aktualizácia prostriedkov overovania dôverujúcej strany.	Postupy, technické rozhrania, protokoly, postupy eskalácie, záznamy o rozhodnutiach a dôkazy o prevádzke.	Správa a riadenie, právna spôsobilosť, riadenie podvodov a kritériá prevádzkových opatrení.	Audit procesov, inšpekcia technických mechanizmov vynútiteľnosti, odber vzoriek protokolov a preskúmanie prevádzkovej účinnosti.
Rozsah certifikátu a správy	Verejný predmet, vylúčenia, predpoklady, závislosti a zostatkové obmedzenia.	Vyhlásenie o predmete, balík verejných informácií, vstupy do správy, matica závislostí.	Výstupy rozhodnutí pre závery modulov a záver celkovej certifikácie.	Preskúmanie certifikačného rozhodnutia, konsolidácia CAR, spúšťače dohľadu a údržby.

I.8 Pravidlá na zachovanie prílohy I počas budúceho vývoja schémy

- **Zachovať základný rámec EÚ:** Európsky katalóg komponentov v tabuľkách I-1 až I-3 by mal zostať prvou štrukturálnou vrstvou, pokiaľ sa schéma EÚ nezmení. Národné doplnenia by sa mali zaznamenávať oddelene, aby bola neskoršia transformácia na schému na úrovni EÚ zvládnuteľná.
- **Vyhnite sa duplicite:** Zoznamy dôkazov patria primárne do prílohy IV, hodnotiace kritériá do prílohy X a hodnotiace postupy do prílohy XI. Príloha I by mala uvádzať predmet, hranice, závislosti, profily a očakávania v oblasti podávania správ.
- **Udržujte tvrdenia o profiloch explicitné:** Certifikát NESMIE naznačovať pokrytie architektonického profilu, variantu peňaženky, operačného systému, toku prípadov použitia, funkcie PID alebo služby validácie, ktoré neboli deklarované, hodnotené a vykazované.
- **Používajte analýzu závislostí namiesto slepého opätovného použitia:** Existujúce certifikáty a audity sú cenné, ale musia byť priradené k slovenskej certifikovanej entite, aby mohli podporiť záver certifikácie.
- **Oddeľte pilotný projekt od produkcie:** Dôkazy z pilotného projektu, demonštrácie alebo kontrolovanej prevádzky môžu podporiť hodnotenie, ale certifikovaný produkčný objekt musí byť výslovne verzionovaný a ohraničený.
- **Udržujte sledovateľnosť:** Každý prvok predmetu v tejto prílohe by mal byť sledovateľný aspoň k jednej položke dôkazu, jednému hodnotiacemu kritériu a jednej hodnotiacej metóde v neskorších prílohách.

PRÍLOHA II – Záruka kontinuity a životný cyklus certifikácie

Národná certifikačná schéma európskej peňaženky digitálnej identity občana (EUDIW-SK)

Informatívny popis – poznámka k návrhu: Táto príloha zachováva životný cyklus uvedený v európskej prílohe II ako hlavný základ: ročné hodnotenie dohľadu, hodnotenie recertifikácie, osobitné hodnotenie, harmonogram dohľadu a parametre významnosti. Je kombinovaná so slovenským modulárnym predmetom z prílohy I, modelom dôkazov v prílohe IV, kritériami v prílohe X, metódami v prílohe XI a očakávaniami týkajúcimi sa spôsobilostí/procesov certifikačných orgánov v prílohe VIII.

II.0 Účel, predmet pôsobnosti a vzťah k ostatným prílohám

Informatívny text: Príloha II definuje, ako certifikovaná služba IKT zostáva v zhode po vydaní certifikátu. Neopakuje kritériá prílohy X ani metódy prílohy XI; definuje, kedy sa tieto kritériá a metódy musia opätovne uplatniť počas životného cyklu certifikátu.

Normatívna požiadavka: Držiteľ certifikátu MUSÍ prevádzkovať certifikovanú službu IKT v súlade s predmetom, predpokladmi, profilmi, modulmi, závislosťami, opatreniami a obmedzeniami uvedenými v certifikáte, certifikačnej správe a správe o certifikačnom posúdení.

Normatívna požiadavka: CAB MUSÍ použiť túto prílohu na plánovanie dohľadu, recertifikácie a osobitných hodnotení pre riešenie EUDIW-SK, službu SK-PID, službu SK-Validácia a akýkoľvek záver o zastrešujúcej certifikácii, ktorý kombinuje tieto moduly.

Normatívna požiadavka: Kontinuita záruky MUSÍ zahŕňať aspoň: poskytovanie certifikovanej služby IKT v čase; zmeny v certifikovanej službe IKT; zmeny v opätovne použiteľných informáciách o záruke; zmeny v prostredí hrozieb; zraniteľnosti a incidenty; a zmeny ovplyvňujúce slovenské zákonné alebo národné integračné povinnosti.

Normatívna požiadavka: Sťažnosti, odvolania, dôsledky nedodržiavania požiadaviek, pozastavenie, zrušenie a odňatie sa riešia v súlade s hlavnou časťou schémy, najmä s oddielmi o sťažnostiach a odvolaniach a kapitolami 5 až 8 o monitorovaní dodržiavania, nezhodách, riadení zraniteľností a zverejňovaní zraniteľností.

Prvok životného cyklu	Účel v EUDIW-SK	Hlavný odkaz na ostatné prílohy
Ročné hodnotenie dohľadu	Potvrdzuje pokračujúcu zhodu a prevádzkovú účinnosť za predchádzajúce obdobie.	Dôkazy podľa prílohy IV, kritériá podľa prílohy X, audit/inšpekcia/skúšanie podľa prílohy XI.
Hodnotenie recertifikácie	Potvrdzuje trvalú zhodu celého certifikovaného predmetu pred uplynutím platnosti certifikátu.	Predmet podľa prílohy I, všetky kritériá podľa prílohy X, kompletný súbor metód podľa prílohy XI.
Špeciálne hodnotenie	Cielené hodnotenie vyvolané podstatnou zmenou, podstatnou zraniteľnosťou, podstatnou nezhodou, pozastavením alebo žiadosťou orgánu.	Pravidlá významnosti podľa prílohy II, osobitné metódy podľa prílohy XI, pravidlá pre rozhodovanie o certifikátoch.
Neustále monitorovanie	Neustále monitorovanie zo strany držiteľa, CAB a príslušných orgánov.	Kapitoly o monitorovaní, riadení zraniteľnosti a zverejňovaní; registre dôkazov podľa prílohy IV.

II.1 Hodnotenia v rámci dohľadu

Normatívna požiadavka: Hodnotenia dohľadu MUSIA zabezpečiť priebežnú platnosť preukázania splnenia požiadaviek schémy. MUSIA zahŕňať: a) poskytovanie certifikovanej služby IKT počas určitého obdobia; b) zmeny v certifikovanej službe IKT; a c) zmeny v prostredí hrozieb.

Normatívna požiadavka: Schéma MUSÍ používať tri typy hodnotenia udržiavania: ročné hodnotenie dohľadu, hodnotenie recertifikácie a osobitné hodnotenie.

Normatívna požiadavka: Účelom ročného hodnotenia dohľadu MUSÍ byť potvrdenie trvalej zhody a účinnosti certifikovanej služby IKT počas vymedzeného obdobia dohľadu, zvyčajne jedného roka.

Činnosť CAB: CAB MUSÍ analyzovať zmeny od posledného hodnotenia, vrátane zmien architektúry, modulov, profilov, tokov ONL/PRX, opatrení, verzií softvéru, konfigurácií, prevádzkových lokalít, závislostí, dodávateľov, opakovane použiteľných informácií o zárukách a slovenských zákonných rozhraní.

Činnosť CAB: CAB MUSÍ posúdiť vhodnosť upravených opatrení, overiť ich existenciu a implementáciu a vyhodnotiť prevádzkovú účinnosť vybraných opatrení počas obdobia dohľadu.

Činnosť CAB: CAB MUSÍ vykonať alebo vyžadovať funkčné, bezpečnostné alebo integračné testy funkcií, komponentov alebo tokov ovplyvnených zmenami, vrátane národných rozhraní PID, validácie, rozhraní životného cyklu spoliehajúcej sa strany a peňaženky, ak je to relevantné.

Normatívna požiadavka: Pri každom ročnom hodnotení dohľadu MUSÍ CAB vyhodnotiť minimálne všetky opatrenia súvisiace s riadením incidentov, riadením zraniteľností, riadením podvodov, vývojom, Riadením zmien, riadením certifikovaných verzií a monitorovaním závislostí.

Normatívna požiadavka: Pri prvom hodnotení dohľadu po počiatočnom vydaní MUSÍ CAB vyhodnotiť prevádzkovú účinnosť všetkých opatrení, ktoré nebolo možné počas počiatočnej certifikácie plne pozorovať, pretože služba ešte nebola v prevádzke.

Normatívna požiadavka: Ročné dozorné činnosti MUSIA byť dostatočné na pokrytie očakávaní v oblasti posudzovania zraniteľnosti podľa článku 5c ods. 4 nariadenia (EÚ) č. 910/2014, pokiaľ nie je samostatný cyklus posudzovania zraniteľnosti výslovne zdokumentovaný a prijatý CAB.

Normatívna požiadavka: Ročné dozorné činnosti MUSIA zohľadňovať povinnosť dvojročného posudzovania zraniteľnosti definovanú v oddiele II.1.4 a musia overiť, či držiteľ certifikátu naďalej dodržiava harmonogram na jej splnenie.

II.1.2 Hodnotenie recertifikácie

Normatívna požiadavka: Účelom hodnotenia recertifikácie MUSÍ byť potvrdenie trvalej zhody a účinnosti služby IKT ako celku a trvalej relevantnosti predmetu certifikácie pred uplynutím platnosti certifikátu.

Normatívna požiadavka: Hodnotenie recertifikácie MUSÍ byť naplánované a vykonané včas, aby bolo možné certifikát obnoviť pred uplynutím jeho platnosti. MUSÍ zahŕňať všetky príslušné hodnotiace kritériá a všetky certifikované moduly, profily, modifikátory prípadov použitia a závislosti.

Činnosť CAB: CAB MUSÍ preskúmať predchádzajúce správy o hodnotení dohľadu, osobitné správy o hodnotení, záznamy o nezhodách, analýzy vplyvu zraniteľností, zmeny závislostí, výsledky testov, incidenty, prípady podvodu a významné zmeny počas certifikačného cyklu.

Normatívna požiadavka: Ak je certifikovaným objektom zastrešujúci certifikačný záver, recertifikácia MUSÍ zahŕňať potvrdenie, že každý modul zostáva v predmete a že žiadna závislosť, predpoklad ani opakovane použiteľný prvok záruky nezneplatňuje záver najvyššej úrovne.

II.1.3 Špeciálne hodnotenie

Normatívna požiadavka: Osobitné hodnotenie SA MUSÍ vykonať, ak je to potrebné na rozhodnutie o pokračovaní, zmene, obmedzení, pozastavení, zrušení pozastavenia, odňatí alebo opätovnom vydaní certifikátu.

Normatívna požiadavka: Osobitné hodnotenie SA MUSÍ vykonať pred úplným obnovením pozastaveného certifikátu.

Normatívna požiadavka: Ak bol certifikát pozastavený z dôvodu potvrdeného narušenia bezpečnosti, ohrozenia alebo podstatnej nezhody a problém nebol včas odstránený, CAB MUSÍ zrušiť alebo stiahnuť certifikát zhody v súlade s príslušnými ustanoveniami vykonávacieho nariadenia Komisie (EÚ) 2024/2981 a tejto schémy.

Normatívna požiadavka: Osobitné hodnotenie MUSÍ byť vyvolané podstatnými zmenami, podstatnými nezhodami, podstatnými zraniteľnosťami, významnými zmenami v informáciách o záruke, ktoré sa dajú opätovne použiť, rozhodnutiami príslušných orgánov alebo udalosťami, ktoré môžu ovplyvniť predmet certifikácie alebo záver o úrovni záruky vysoká.

Činnosť CAB: CAB MUSÍ zamerať osobitné hodnotenie na dotknuté požiadavky, opatrenia, komponenty, rozhrania, moduly, profily, závislosti a prevádzkové procesy, avšak MUSÍ rozšíriť predmet hodnotenia v prípadoch, keď je príčina alebo dopad širší, než bolo pôvodne uvedené.

II.1.4 Dvojročné posúdenie zraniteľnosti

Normatívna požiadavka: Hodnotenie zraniteľnosti certifikovanej služby IKT sa MUSÍ vykonávať najmenej raz za dva roky v súlade s článkom 5c ods. 4 nariadenia (EÚ) č. 910/2014 a príslušnými požiadavkami vykonávacieho nariadenia Komisie (EÚ) 2024/2981. Toto posúdenie MUSÍ zahŕňať inštanciu peňaženky, WSCA, závislosti WSCD, backendové komponenty, rozhrania, závislosti a prevádzkové predpoklady relevantné pre predmet certifikácie.

Normatívna požiadavka: Dvojročné posúdenie zraniteľnosti MÔŽE byť začlenené do ročného dohľadu, recertifikácie alebo osobitného hodnotenia za predpokladu, že tento cyklus zabezpečuje, že aspoň raz za dva roky sa zdokumentuje úplné posúdenie zraniteľnosti a že CAB zaznamená predmet, metódy, výsledky, zostatkové zraniteľnosti a stav nápravy.

II.2 Harmonogram dohľadu a výstupy rozhodnutí

Normatívna požiadavka: Každý rok sa MUSÍ vykonať aspoň jedno ročné hodnotenie dohľadu.

Normatívna požiadavka: Hodnotenie recertifikácie SA MUSÍ vykonať pred dátumom vypršania platnosti certifikátu a v dostatočnom predstihu, aby sa zabezpečil neprerušený certifikačný cyklus.

Normatívna požiadavka: Osobitné hodnotenie sa MUSÍ vykonať na základe rozhodnutia certifikačného orgánu alebo ak to vyžaduje vlastník schémy, NCCA, príslušný orgán, žiadosť držiteľa certifikátu, podstatná zmena, podstatná nezhoda, podstatná zraniteľnosť alebo pozastavenie certifikátu.

Normatívna požiadavka: Po každom hodnotení dohľadu, recertifikácii alebo osobitnom hodnotení sa MUSÍ uskutočniť preskúmanie a rozhodnutie o certifikácii.

Výsledok hodnotenia	Význam	Vplyv na certifikát
Pokračovanie bez zmien	Žiadna podstatná skutočnosť nemá vplyv na predmet certifikácie.	Certifikát zostáva platný v pôvodnom znení.
Pokračovanie s požadovanými nápravnými opatreniami	Nepodstatné problémy sa akceptujú s podmienkou ich vyriešenia v stanovenom termíne.	Certifikát zostáva platný; následné opatrenia sa skontrolujú pri najbližšom hodnotení alebo skôr, ak je to potrebné.
Zmena certifikátu	Certifikovaný predmet, obmedzenia, závislosti alebo usmernenia musia byť aktualizované bez predĺženia dátumu ukončenia platnosti.	Certifikát zostáva platný s dodatkom a aktualizovanými informáciami vo verejnej správe/certifikačnej správe.

Výsledok hodnotenia	Význam	Vplyv na certifikát
Pozastavenie	Závažný problém môže byť odstránený, ale záruka je dočasne ovplyvnená alebo spolupráca je nedostatočná.	Certifikát je pozastavený, kým špeciálne hodnotenie nepotvrdí obnovenie platnosti.
Zrušenie	Nezhodu alebo zraniteľnosť nie je možné odstrániť alebo certifikát už nezodpovedá certifikovanej službe IKT.	Certifikát sa odníma.
Zrušenie a nový certifikát	Recertifikácia podporuje obnovený predmet a dobu platnosti.	Starý certifikát je zrušený; nový certifikát je vydaný s novým dátumom ukončenia, ktorý neprekračuje zákonný maximálny limit.

Informatívny popis: Európsky základ rozlišuje medzi podstatnými udalosťami a bežnými udalosťami. Slovenská schéma uplatňuje toto rozlíšenie na moduly, profily, národnú integráciu a opakovateľnú záruku.

Normatívna požiadavka: Držiteľ certifikátu MUSÍ udržiavať zdokumentované procesy na určovanie významnosti nezhôd, zmien, zraniteľností, incidentov, podvodných udalostí a zmien závislostí.

Normatívna požiadavka: Podstatná udalosť MUSÍ byť oznámená CAB bez čakania na ročné hodnotenie dohľadu. CAB MUSÍ preskúmať posúdenie podstatnosti a určiť, či je potrebné osobitné hodnotenie alebo zmena certifikátu.

Normatívna požiadavka: Nepodstatné udalosti MÔŽU byť riešené v rámci procesu držiteľa certifikátu za predpokladu, že CAB vyhodnotí účinnosť tohto procesu počas ročného dohľadu.

Normatívna požiadavka: Ak CAB zistí, že držiteľ certifikátu opakovane nesprávne klasifikuje významné udalosti ako nevýznamné, CAB MÔŽE vyžadovať dočasné oznamovanie všetkých udalostí v príslušnej kategórii procesov, kým sa nepreukáže účinnosť procesu.

II.3.1 Významnosť nezhôd

Normatívna požiadavka: Nezhoda SA POVAŽUJE za **významnú**, ak spôsobuje neúčinnosť opatrenia alebo kontroly použitej na splnenie požiadavky, spochybňuje predpoklad závislosti alebo spôsobuje, že certifikát, certifikačná správa alebo verejné informácie nesprávne predstavujú certifikovanú službu.

Normatívna požiadavka: Opakované nepodstatné nezhody MÔŽU nadobudnúť podstatný charakter, ak ich opakovaním dôjde k neúčinnosti opatrenia alebo procesu.

II.3.2 Závažnosť zmien

Normatívna požiadavka: Zmena SA POVAŽUJE za **podstatnú**, ak môže viesť k podstatnej nezhode, ovplyvňuje bezpečnostné funkcie, ovplyvňuje externé alebo interné rozhrania, mení organizáciu alebo architektúru, na ktorej je založená služba IKT, mení kritické komponenty, ako sú WSCD alebo WSCA, alebo mení predmet certifikácie, profily alebo modifikátory prípadov použitia.

Oblasť zmeny	Príklady podstatnej zmeny	Požiadavka na zaobchádzanie
Hranica modulu prílohy I	Pridanie/odstránenie riešenia EUDIW-SK, služby SK-PID, služby SK-Validácia alebo zastrešujúceho predmetu.	Oznámiť CAB; pravdepodobne bude potrebné osobitné hodnotenie alebo recertifikácia.
Profil architektúry	Zmena medzi vzdialeným WSCD, lokálnym externým WSCD, lokálnym interným WSCD alebo lokálnym natívnym WSCD; nové hranice WSCA/WSCD.	Informujte CAB; je potrebná aktualizácia rizík a skúšania špecifických pre profil.
Tok ONL/PRX	Nový tok online alebo proximity transakcií, zmenený protokol, zmenený model interakcie spoliehajúcej sa strany.	Informujte CAB; preskúmanie funkčného a rizikového skúšania.

Oblasť zmeny	Príklady podstatnej zmeny	Požiadavka na zaobchádzanie
Inštancia peňaženky	Nová platforma, distribučný kanál, variantu operačného systému, hlavná verzia, zmena lokálnej autentifikácie alebo zmena bezpečného úložiska.	Informovať CAB; zdôvodnenie odberu vzoriek a aktualizácia posúdenia zraniteľnosti.
PID a viazanie identity	Zmena poskytovateľa PID, zdrojového registra, overovania identity, osvedčenia peňaženky alebo formátu údajov PID.	Upozorniť CAB; preskúmanie záruky pre PID a eID.
Mechanizmy validácie a dôveryhodných strán	Zmena registra dôveryhodnej strany, API validácie, dôveryhodných kotiev, podpory aktualizácie certifikátov alebo automatizovaného hlásenia.	Upozorniť CAB; skúšanie národnej integrácie a preskúmanie zákonných povinností.
Kryptografická infraštruktúra	Zmena algoritmov, kľúčov, HSM, WSCD, WSCA, modelu správy kľúčov alebo certifikovanej kryptografickej komponenty.	Upozorniť CAB; analýza závislostí a kryptografické hodnotenie.
Opätovne použiteľná záruka	Pozastavenie, zrušenie, uplynutie platnosti, obmedzenie predmetu alebo nepriaznivé zistenie v certifikáte alebo audite, na ktorý sa spoliehate.	Upozorniť CAB; diferenciálna analýza závislostí.
Prevádzka a dodávatelia	Nový kritický dodávateľ, miesto hostingu, prevádzkový proces, proces riešenia incidentov alebo proces riešenia zraniteľností.	Informujte CAB, ak to môže ovplyvniť záruku alebo predmet.

Normatívna požiadavka: Držiteľ certifikátu MUSÍ určiť významnosť vplyvu zraniteľnosti v kontexte certifikovaného predmetu, modelu hrozieb, ovplyvnených komponentov, využiteľnosti, vystavenia, predpokladov závislosti, kompenzačných opatrení a vplyvu na používateľov.

Normatívna požiadavka: Zraniteľnosť SA MUSÍ považovať za významnú, ak môže ovplyvniť kritické aktíva peňaženky, autentizáciu používateľa, vydávanie PID, životný cyklus jednotky peňaženky, validáciu spoliehajúcej sa strany, kryptografické operácie, kontrolu certifikovanej verzie, dôvernosť alebo integritu osobných údajov alebo schopnosť udržať úroveň záruky vysoká v.

Normatívna požiadavka: Zraniteľnosť v opätovne použitej komponente MUSÍ byť posúdená vzhľadom na integráciu, použitie a predpoklady v slovenskej architektúre. Kritická zraniteľnosť môže byť nepodstatná len vtedy, ak CAB súhlasí s tým, že nie je zneužiteľná v certifikovanej konfigurácii alebo je včas úplne zmiernená.

II.4 Povinnosti v oblasti nepretržitého monitorovania

Normatívna požiadavka: Držiteľ certifikátu MUSÍ nepretržite monitorovať zraniteľnosti, incidenty, indikátory podvodov, zmeny, stav závislostí, stav certifikátov, správy o zabezpečení, bezpečnostné upozornenia, zmeny v prostredí hrozieb a národné integračné povinnosti relevantné pre predmet certifikácie.

Normatívna požiadavka: Držiteľ certifikátu MUSÍ zaviesť, udržiavať a uplatňovať politiku riadenia zraniteľností, ktorá spĺňa požiadavky stanovené v prílohe I k nariadeniu (EÚ) 2024/2847 (zákon o kybernetickej odolnosti), ak sa to vzťahuje na certifikovanú službu IKT alebo jej komponenty.

Normatívna požiadavka: CAB MUSÍ monitorovať informácie, ktoré majú vplyv na certifikáty, ktoré vydala, vrátane sťažností, informácií o zraniteľnosti, informácií príslušných orgánov, zmien v opätovne použiteľnej záruke a informácií poskytnutých držiteľom certifikátu.

Normatívna požiadavka: Ak je certifikát alebo správa o záruke, na ktoré sa spolieha, aktualizované, pozastavené, zrušené alebo nahradené, CAB MUSÍ vykonať analýzu diferenciálnej závislosti a zaznamenať výsledok ako súčasť údržby certifikátu.

Normatívna požiadavka: Ak sa aktualizujú registre rizík Únie, dokumenty o najnovšom stave techniky, národné technické referenčné rámce alebo slovenské integračné požiadavky, držiteľ certifikátu MUSÍ posúdiť vplyv na certifikovaný predmet a v prípade, že je to podstatné, poskytnúť toto posúdenie CAB.

II.5 Dôkazy o údržbe a podávanie správ

Normatívna požiadavka: Pri každom hodnotení údržby MUSÍ držiteľ certifikátu poskytnúť súbor dôkazov o údržbe, ktorý obsahuje register zmien, register zraniteľností, register incidentov a podvodov, stav závislostí, stav informácií o záruke, dôkazy o prevádzkovej účinnosti opatrení, výsledky testov, stav nápravných opatrení a aktualizáciu obmedzení predmetu.

Normatívna požiadavka: CAB MUSÍ zaznamenať predmet, kritériá, metódy, vzorky, testy, zistenia, nezhody, rozhodnutia o závislosti a konečné odporúčanie každého hodnotenia údržby v správe vhodnej pre správu o certifikačnom posúdení a certifikačné preskúmanie.

Normatívna požiadavka: Verejná certifikačná správa MUSÍ byť aktualizovaná v prípadoch, keď zmeny v údržbe ovplyvňujú predmet, obmedzenia, usmernenia, certifikované verzie, stav platnosti, zmeny certifikátu alebo informácie požadované v prílohe III.

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

PRÍLOHA III – Zoznam verejne dostupných informácií

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny popis – poznámka k návrhu: Táto príloha zachováva európsky návrh prílohy III ako základnú štruktúru a rozširuje ju len tam, kde je to potrebné, aby odzrkadľovala slovenský modulárny predmet, architektonické profily, modifikátory prípadov použitia ONL/PRX, transparentnosť stavu certifikátov a logiku národnej integrácie.

III.0 Účel a výklad

Informatívny text: Príloha III definuje balík verejnej transparentnosti, ktorý musí držiteľ certifikátu EUDIW-SK sprístupniť. Pomáha používateľom, dôverujúcim stranám, orgánom a zainteresovaným stranám pochopiť, čo bolo certifikované, v akom predmete a s akými obmedzeniami, a ako sa rieši bezpečnostná podpora a hlásenie zraniteľností.

Normatívna požiadavka: Držiteľ certifikátu EUDIW-SK MUSÍ sprístupniť informácie uvedené v tejto prílohe verejnosti v elektronickej forme, a to jasným, komplexným a ľahko dostupným spôsobom.

Normatívna požiadavka: Verejné informácie MUSIA zostať dostupné a v prípade potreby aktualizované aspoň do uplynutia platnosti, odňatia alebo nahradenia certifikátu EUDIW-SK.

Normatívna požiadavka: Verejné informácie NESMÚ prezradiť citlivé bezpečnostné údaje, osobné údaje, dôverné zistenia z hodnotenia, podrobnosti o zraniteľnostiach, ktoré je možné zneužiť, obchodné tajomstvá ani informácie, ktoré by mohli ohroziť bezpečnosť certifikovanej služby IKT.

Normatívna požiadavka: Ak sú informácie z bezpečnostných dôvodov redigované alebo zhrnuté, držiteľ MUSÍ zabezpečiť, aby verejná verzia zostala presná a nevytvárala zavádzajúce tvrdenia týkajúce sa certifikovaného predmetu.

III.1 Európske základné verejné informácie o kybernetickej bezpečnosti

Normatívna požiadavka: Pre každú certifikovanú službu IKT MUSÍ držiteľ sprístupniť verejnosti usmernenia a odporúčania, ktoré pomáhajú koncovým používateľom, spoliehajúcim sa stranám alebo príslušným prevádzkovateľom pri bezpečnej konfigurácii, inštalácii, nasadení, prevádzke, údržbe a vyradení certifikovanej služby IKT a jej komponentov, ak je to vhodné.

Normatívna požiadavka: Držiteľ MUSÍ zverejniť všetky obmedzenia týkajúce sa používania certifikovanej služby IKT, vrátane obmedzení funkčných, technických, týkajúcich sa stupňa záruky, zariadení, platforiem, profilov, nasadenia, jurisdikcie alebo životného cyklu, ktoré sú relevantné pre bezpečné používanie.

Normatívna požiadavka: Držiteľ MUSÍ zverejniť obdobie, počas ktorého sa poskytuje bezpečnostná podpora, vrátane obdobia, počas ktorého sa budú poskytovať aktualizácie týkajúce sa kybernetickej bezpečnosti, riešenie zraniteľností a bezpečnostné odporúčania.

Normatívna požiadavka: Držiteľ MUSÍ zverejniť kontaktné informácie a akceptované metódy prijímania informácií o zraniteľnostiach od koncových používateľov, dôverujúcich strán, výskumníkov v oblasti bezpečnosti, orgánov posudzovania zhody a príslušných orgánov.

Normatívna požiadavka: Držiteľ MUSÍ zverejniť odkaz na online repozitáre, v ktorých sú uvedené verejne zverejnené zraniteľnosti súvisiace s certifikovanou službou IKT alebo riešením peňaženky, a na príslušné bezpečnostné upozornenia.

Normatívna požiadavka: Ak certifikovaná služba IKT zahŕňa softvérové komponenty poskytované používateľom na prevádzku na ich vlastných zariadeniach, držiteľ MUSÍ zverejniť podrobné pokyny alebo odkazy týkajúce sa bezpečného prvotného uvedenia do prevádzky, bezpečného používania počas celej životnosti komponentu, aktualizácií týkajúcich sa bezpečnosti, vplyvu zmien na bezpečnosť údajov, bezpečného vyradenia z prevádzky a odporúčaní v prípade straty, krádeže, kompromitácie alebo výmeny zariadenia používateľa.

Normatívna požiadavka: Ak sa na komponent alebo inštanciu peňaženky vzťahuje nariadenie (EÚ) 2024/2847 alebo iná povinnosť zverejňovať informácie o bezpečnosti výrobku, držiteľ MUSÍ zverejniť príslušnú internetovú adresu vyhlásenia o zhode EÚ alebo rovnocenné verejné informácie o bezpečnosti výrobku, ak je to relevantné.

Normatívna požiadavka: Verejné informácie MUSIA identifikovať názov certifikovanej služby IKT, prípadne obchodný názov, certifikovanú verziu, držiteľa certifikátu, identifikátor certifikátu, certifikačný orgán, prípadne zodpovedný vnútroštátny orgán, dátum vydania, dobu platnosti, stav certifikátu a odkaz na certifikát alebo záznam v registri certifikátov.

Normatívna požiadavka: Verejné informácie MUSIA identifikovať typ certifikovanej služby IKT a modul alebo moduly, na ktoré sa vzťahujú, s použitím terminológie prílohy I: Riešenie EUDIW-SK, Služba SK-PID, Služba SK-Validácia, záver o zastrešujúcej certifikácii alebo jasne vymedzená podmnožina.

Normatívna požiadavka: V prípade modulu EUDIW-SK Solution musia verejné informácie uvádzať varianty inštancií peňaženky, na ktoré sa certifikát vzťahuje, architektonický profil alebo profily, na ktoré sa vzťahuje, a či sa vzťahujú modifikátory prípadov použitia online a/alebo v blízkosti.

Normatívna požiadavka: Verejné informácie MUSIA identifikovať obmedzenia predmetu certifikácie, vylúčené varianty, vylúčené funkcie, postupne zavádzané alebo odložené funkcie, nepodporované prípady použitia a necertifikované závislosti spôsobom zrozumiteľným pre používateľov a dôverujúce strany.

Normatívna požiadavka: Verejné informácie MUSIA na vysokej úrovni uvádzať akékoľvek predpoklady týkajúce sa zariadení používateľov, platforiem, prevádzkového prostredia alebo závislostí, ktoré ovplyvňujú bezpečné používanie certifikovanej služby.

Normatívna požiadavka: Ak je pre verejný predmet relevantná závislosť od externých certifikovaných komponentov, služieb QTSP, národnej infraštruktúry, služieb PID, služieb validácie alebo mechanizmov spoliehajúcich sa strán, držiteľ MUSÍ opísať túto závislosť na vysokej úrovni bez zverejnenia citlivých podrobností.

III.3 Informácie špecifické pre riešenie peňaženky

Normatívna požiadavka: Ak certifikovaná služba IKT zahŕňa riešenie peňaženky, držiteľ MUSÍ zverejniť politiku, v ktorej sa špecifikujú podmienky a časový rámec pre zrušenie, pozastavenie alebo neplatnosť osvedčení jednotiek peňaženky, ak je to relevantné podľa práva Únie a certifikovanej architektúry.

Normatívna požiadavka: Držiteľ MUSÍ zverejniť usmernenia o bezpečnom používaní týkajúce sa aktivácie peňaženky, jej poskytovania, overovania, schvaľovania transakcií, predkladania dôveryhodným stranám, aktualizácie, obnovy, zrušenia, pozastavenia a vyradenia z prevádzky, ak sa na tieto funkcie vzťahuje certifikát.

Normatívna požiadavka: Držiteľ MUSÍ zverejniť informácie, ktoré používateľom umožnia pochopiť, ktoré certifikované funkcie vyžadujú dostupnosť siete, ktoré funkcie sa môžu používať v blízkosti a ktoré funkcie závisia od backendových služieb alebo externej infraštruktúry.

Normatívna požiadavka: Držiteľ MUSÍ zverejniť usmernenia pre používateľov, v ktorých vysvetlí, ako rozpoznať certifikované verzie, ako sa vyhnúť zavádzajúcim alebo napodobňujúcim aplikáciám peňaženky a ako reagovať na podozrenie z kompromitácie, nezákonného alebo podvodného používania peňaženky.

Normatívna požiadavka: Ak je zdrojový kód alebo zoznam softvérových komponentov zverejnený v rámci programu otvoreného zdrojového kódu, transparentnosti alebo riadenia zraniteľností, držiteľ MUSÍ identifikovať verejné umiestnenie a predmet zverejnených informácií.

III.4 Verejné informácie o službe PID a službe validácie

Normatívna požiadavka: Ak certifikát zahŕňa službu SK-PID, verejné informácie MUSIA na vysokej úrovni opisovať certifikovanú službu PID, vrátane zodpovedného poskytovateľa, certifikovaného predmetu, podporovaných funkcií vydávania alebo životného cyklu, podporovaných formátov, ak sú verejné, obmedzení a usmernenia pre používateľov týkajúcich sa bezpečného používania PID.

Normatívna požiadavka: Ak sa certifikát vzťahuje na službu SK-Validation, verejné informácie MUSIA na vysokej úrovni opisovať certifikovaný validačný mechanizmus, vrátane účelu služby, podporovaných validačných funkcií, účelu validácie spoliehajúcej sa strany, očakávaní týkajúcich sa dostupnosti alebo podpory, obmedzení a kontaktných miest.

Normatívna požiadavka: Verejné informácie o službách PID a validácii NESMÚ zverejňovať citlivé podrobnosti o implementácii, materiály týkajúce sa dôveryhodných kotiev ani prevádzkové informácie, ktoré by mohli ohroziť bezpečnosť služby.

Normatívna požiadavka: Držiteľ MUSÍ udržiavať balík verejných informácií s kontrolou verzií a MUSÍ ho bez zbytočného odkladu aktualizovať po vydaní certifikátu, zmene certifikátu, pozastavení certifikátu, zrušení certifikátu, podstatnej zmene predmetu, zverejnení podstatnej zraniteľnosti, zmene obdobia podpory alebo zmene kontaktnej osoby pre hlásenie zraniteľností.

Normatívna požiadavka: Verejné informácie MUSIA byť dostupné aspoň v slovenčine a v jazyku, ktorý je ľahko prístupný cezhraničným používateľom a zainteresovaným stranám. V prípade potreby MUSÍ byť k dispozícii anglická verzia na podporu cezhraničného uznávania a transparentnosti.

Informatívny text: Požiadavka na anglickú verziu je rozšírením vnútroštátnej transparentnosti v Slovenskej republike, ktorého cieľom je podporiť cezhraničné porozumenie, a nemení minimálne požiadavky na verejné informácie uvedené v vykonávacom nariadení Komisie (EÚ) 2024/2981.

Normatívna požiadavka: Verejné informácie MUSIA byť v súlade s certifikátom, certifikačnou správou, záznamom v registri certifikátov, obsahom certifikátu podľa prílohy V, certifikačnou správou podľa prílohy VI a akýmikoľvek povolenými informáciami o značke dôveryhodnosti EUDI Wallet. Tento národný systém nezavádza samostatnú slovenskú značku alebo označenie zhody.

III.6 Kontrolný zoznam verejných informácií

Č.	Položka verejných informácií	Vzťahuje sa na	Účel zverejnenia
III.1	Usmernenia pre bezpečnú konfiguráciu, inštaláciu, nasadenie, prevádzku, údržbu a vyradenie z prevádzky	Všetky príslušné moduly	Bezpečné používanie a transparentnosť
III.1	Obmedzenia používania certifikovanej služby IKT	Všetky moduly	Vyhnite sa zavádzajúcim tvrdeniam o certifikácii
III.1	Doba poskytovania bezpečnostnej podpory a informácie o aktualizáciách v oblasti kybernetickej bezpečnosti	Všetky moduly	Transparentnosť životného cyklu a podpory
III.1	Kontakt na hlásenie zraniteľností a akceptované metódy	Všetky moduly	Koordinované zverejňovanie zraniteľností
III.1	Verejne zverejnené zraniteľnosti a upozornenia	Všetky moduly	Neustála transparentnosť v oblasti zraniteľností
III.2	Názov certifikovanej služby, verzia, identifikátor certifikátu, stav a platnosť	Všetky moduly	Identifikácia certifikátu
III.2	Certifikovaný modul, architektonický profil a pokrytie ONL/PRX	Všetky moduly, najmä riešenie EUDIW-SK	Transparentnosť predmetu v súlade s prílohou I
III.2	Vylúčené funkcie, obmedzenia a predpoklady	Všetky moduly	Hranica dôvery medzi používateľom a spoliehajúcou sa stranou
III.3	Politika zrušenia alebo neplatnosti osvedčenia peňaženky	Riešenie EUDIW-SK	Transparentnosť životného cyklu peňaženky
III.3	Usmernenie pre prípad straty, krádeže, ohrozenia, obnovy a vyradenia z prevádzky	Riešenie EUDIW-SK	Bezpečnosť koncového používateľa
III.4	Informácie o predmete služieb PID a služieb validácie	Služba SK-PID, služba SK-Validácia	Pochopenie národných služieb zo strany verejnosti
III.5	Správa publikácií a história aktualizácií	Všetky moduly	Súlad medzi osvedčením, správou a informáciami pre verejnosť

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny popis – poznámka k vypracovaniu: Táto príloha vychádza z európskeho návrhu prílohy IV, podľa ktorého musí žiadateľ poskytnúť verejné informácie, informácie o organizácii a architektúre, informácie o certifikačnom pláne a posúdenie rizík. Národná verzia rozširuje tento základ o balík prevádzkových dôkazov v súlade s prílohou I, slovenským modulárnym predmetom, architektonickými profilmi, modifikátormi prípadov použitia ONL/PRX, opätovne použiteľnými informáciami o záruke a slovenskými zákonnými povinnosťami.

IV.0 Preambula, účel a prierezové pravidlá

Informatívny text: Príloha IV je bránou k dôkazom v rámci schémy. Nedefinuje hodnotiace kritériá ani hodnotiace metódy. Definuje informácie, ktoré musí žiadateľ poskytnúť, aby CAB mohla uplatniť prílohu X a prílohu XI na predmet definovaný v prílohe I.

Normatívna požiadavka: Žiadateľ o certifikáciu v rámci schémy EUDIW-SK MUSÍ poskytnúť alebo inak zabezpečiť CAB všetky informácie potrebné na činnosti posudzovania zhody.

Normatívna požiadavka: Informácie MUSIA byť dostupné pri začatí hodnotenia a podľa potreby počas celého hodnotenia. CAB MÔŽE požiadať o akékoľvek dodatočné informácie, prístup, technické artefakty, vysvetlenia, rozhovory alebo demonštrácie potrebné na dosiahnutie záveru bez námietok.

Normatívna požiadavka: Ak niektoré základné komponenty stále prechádzajú certifikáciou, na začiatku hodnotenia MÔŽU byť poskytnuté návrhy dokumentov, ale konečné dokumenty MUSIA byť poskytnuté pred konečným rozhodnutím CAB o posudzovaní zhody.

Normatívna požiadavka: Na zaručenie reprodukovateľnosti MUSIA byť všetky interné dokumenty, technická dokumentácia, testovacie artefakty a záznamy predložené žiadateľom jednoznačne identifikované s uvedením vlastníka, dátumu vydania, čísla verzie, predmetu a klasifikácie dôvernosti.

Normatívna požiadavka: Žiadateľ MUSÍ štruktúrovať podanie tak, aby CAB mohol vysledovať požiadavky k opatreniam, opatrenia k zložkám a procesom a zložky a procesy ku konkrétnym dôkazom.

Tabuľka IV-1 – Európska základná úroveň a rozšírenie dôkazov v Slovenskej republike

Trieda informácií európskej základnej úrovne	Slovenské rozšírenie v tejto prílohe	Použitie v ďalších prílohách
Požiadavky na verejné informácie na konci certifikácie	Balík verejne dostupných informácií, webová stránka držiteľa certifikátu, usmernenia pre používateľov, obmedzenia používania, doba poskytovania bezpečnostnej podpory a informácie o hlásení zraniteľností	Prílohy III, V, VI a uverejňovanie certifikátov
Organizácia a architektúra služby IKT	Právna úloha, predmet modulu, architektúra komponentov, rozhrania, priestory, závislosti, predpoklady a prevádzkové procesy	Predmet prílohy I, kritériá prílohy X, preskúmanie návrhu a analýza závislostí podľa prílohy XI
Certifikačný plán	Existujúce a plánované certifikáty komponentov, informácie o záruke, bezpečnostné ciele, ETR, SoA, usmernenia a integračné dokumenty	Prijateľnosť podľa prílohy IX, analýza závislostí podľa prílohy XI, správa o zložení podľa prílohy VII
Posúdenie rizík priradené k registru rizík Únie	Posúdenie rizík špecifické pre implementáciu, plán ošetrenia rizika, priradenie k opatreniam, priradenie ku komponentom a odôvodnenie zvyškových rizík	Hodnotiace kritériá podľa prílohy X, posúdenie rizík a preskúmanie podľa prílohy XI

IV.1 Žiadateľ, certifikovaný objekt a organizačný kontext

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť identifikáciu žiadateľa a navrhovaného držiteľa osvedčenia.

Normatívna požiadavka: Žiadateľ MUSÍ určiť konkrétny modul alebo moduly, ktoré sú predmetom certifikácie, pričom použije názvy modulov a postupy certifikácie definované v prílohe I: Riešenie EUDIW-SK, Služba SK-PID, Služba SK-Validácia a zdieľané alebo externé závislosti.

Normatívna požiadavka: Žiadateľ MUSÍ uviesť, či sa certifikácia požaduje pre samostatný modul, súbor modulov alebo pre zastrešujúci certifikačný záver pokrývajúci riešenie peňaženky a schému eID, v rámci ktorej sa poskytuje.

Normatívna požiadavka: Žiadateľ MUSÍ identifikovať právnu úlohu a zákonný základ uplatniteľný na každý modul podľa práva Únie, slovenského práva a schémy EUDIW-SK.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť opis úloh prevádzkovateľa, subdodávateľa, dodávateľa a tretích strán zapojených do poskytovania, údržby alebo prevádzky hodnotenej služby IKT.

Normatívna požiadavka: V prípade modulu Riešenie EUDIW-SK žiadateľ MUSÍ predložiť dôkazy preukazujúce, že poskytovateľ riešenia peňaženky je kvalifikovaným poskytovateľom dôveryhodných služieb alebo uzavrel platnú zmluvu s kvalifikovaným poskytovateľom dôveryhodných služieb, ak to vyžaduje slovenské právo.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť formálne vyhlásenie o predmete, ktoré zodpovedá prílohe I. Vyhlásenie MUSÍ identifikovať certifikovaný modul, deklarovaný architektonický profil alebo profily, modifikátory prípadov použitia ONL a/alebo PRX, zahrnuté varianty, vylúčené varianty, závislosti, predpoklady prevádzkového prostredia a obmedzenia verejného predmetu.

Tabuľka IV-2 – Vyhlásenie o predmete v súlade s prílohou I

Predmet rozsahu v prílohe I	Požiadavky na informácie v prílohe IV	Dôvod zaradenia
Riešenie EUDIW-SK	Varianty inštancií peňaženky, hranica WSCA/WSCD, služba jednotky peňaženky, služba poskytovania a správy, proces načítania a aktualizácie, backendové služby a rozhrania	Definuje hranice certifikátu peňaženky a zabezpečuje, aby certifikát neskrýval riziká špecifické pre profil alebo variantu
Služba SK-PID	Služba poskytovania a správy PID, proces overovania identity, proces registrácie, osvedčenie peňaženky alebo ekvivalentné overenie s vysokou úrovňou záruky, formáty údajov a rozhrania zdrojového registra	Umožňuje posúdenie vydávania PID na stupni záruky High a jeho prepojenie s jednotkou peňaženky
Služba SK-Validácia	Validačný mechanizmus, validácia spoliehajúcej sa strany, rozhrania registrov spoliehajúcich sa strán, požiadavky na dostupnosť, kotvy dôvery a prevádzkové procesy	Umožňuje hodnotenie povinností v oblasti validácie členského štátu a kritickosti služby
Architektonické profily A–D	Vzdialený WSCD, lokálny externý WSCD, lokálny interný WSCD alebo lokálny natívny WSCD, spolu s predpokladmi a dôkazmi pre hranice WSCD/WSCA	Podporuje mapovanie rizík špecifické pre profil, kryptografickú záruku a posúdenie zraniteľnosti
Modifikátory ONL/PRX	Online a proximity transakčné toky, protokoly, hranice dôvery a offline/online závislosti	Podporuje výber testov, overovanie rizík, vzorkovanie a funkčnú zhodu
Zdieľané a externé závislosti	QTSP, certifikované HSM/WSCD, ISO/IEC 27001, ETSI, EUCC/Common Criteria, FCAF alebo národná záruka na zabezpečenie kybernetickej bezpečnosti	Podporuje analýzu závislostí a prípustnosti podľa prílohy IX a prílohy XI

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť informácie o architektúre opisujúce každú zložku hodnotenej služby IKT, vrátane základných bezpečnostných vlastností, externých závislostí, rozhraní, hraníc dôveryhodnosti a zodpovedností zložiek.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť základné konfigurácie softvéru a nastavenia pre všetky moduly v predmete pôsobnosti, vrátane identifikátorov verzií, identifikátorov zostavení, parametrov nasadenia a konfiguračných možností relevantných pre bezpečnosť.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť dokumentáciu prevádzkových procesov podporujúcich poskytovanie služby, vrátane zapojenia používateľov, registrácie, správy prostriedkov elektronickej identifikácie, poskytovania peňaženiek, správy peňaženiek, životného cyklu PID, prevádzky služby validácie, riadenia zmien, správy zraniteľností, správy incidentov a správy podvodov, ak je to relevantné.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť dokumentáciu o opatreniach zavedených na zabezpečenie používania aktuálne certifikovanej verzie hodnotenej služby IKT.

Normatívna požiadavka: V prípade modulu riešenia EUDIW-SK žiadateľ MUSÍ predložiť dokumentáciu o funkčných požiadavkách a mechanizmoch bezpečnej aktualizácie týkajúcich sa každej softvérovej komponenty, vrátane inštancie peňaženky a WSCA, ak je to relevantné.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť dôkaz o funkčnej zhode s príslušnými funkčnými a funkčno-bezpečnostnými požiadavkami peňaženky EUDI, ak je to relevantné pre deklarovaný modul, architektonický profil, modifikátor prípadu použitia ONL/PRX a predmet slovenskej národnej integrácie. Ak sa uplatňuje **Rámec posudzovania zhody funkčnej peňaženky európskej digitálnej identity (FCAF), verzia 0.1**, žiadateľ MUSÍ predložiť príslušné dôkazy založené na FCAF, vrátane výsledkov testov, vyplnených špecifikácií testov alebo testovacích kníh, záznamov testovacích údajov, mapovaní sledovateľnosti, vyhlásenia o zhode implementácie, záznamov o odchýlkach a odôvodnených vyhlásení o neaplikovateľnosti.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť kompletné mapovanie interných a externých rozhraní, tokov údajov a hraníc dôveryhodnosti, vrátane rozhraní s PID, validáciou, spoliehajúcou sa stranou, QTSP, WSCA, WSCD a komponentmi národnej infraštruktúry.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť zoznam prevádzkových miest a priestorov, v ktorých sú umiestnené backendové služby, vrátane cloudových regiónov, dátových centier a poskytovateľov spravovaných služieb, ak je to relevantné.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť opis všetkých predpokladov týkajúcich sa prevádzkového prostredia. Pre každý predpoklad, ktorý nie je podložený osvedčením o zhode, MUSÍ žiadateľ opísať mechanizmus

používaný na vynútenie alebo overenie predpokladu, napríklad kontroly v čase behu, osvedčenie zariadenia, vynútenie politiky, monitorovanie alebo kompenzačné opatrenia.

IV.3 Bezpečnostné opatrenia, úroveň záruky a priradenie ku komponentom

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť opis každej implementovanej bezpečnostnej kontroly a jej požadovaného stupňa záruky na základe príslušných požiadaviek Únie a schémy, vrátane vykonávacieho nariadenia (EÚ) 2015/1502 pre úroveň záruky vysoká, ak je to relevantné.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť mapovanie, ktoré ukazuje, ako sú opatrenia na riadenie implementované v rámci komponentov, procesov, organizačných opatrení a závislostí.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť odôvodnenie, v ktorom vysvetlí, prečo je pre každé opatrenie požadovaná daná úroveň záruky a ako sú splnené príslušné bezpečnostné aspekty.

Normatívna požiadavka: Pre každý vybraný architektonický profil a modifikátor ONL/PRX žiadateľ MUSÍ poskytnúť opis účinnosti, v ktorom vysvetlí, ako implementované opatrenia spoločne riešia hrozby a riziká pre architektúru až do požadovaného stupňa záruky.

Normatívna požiadavka: Ak sú opatrenia implementované externými komponentmi alebo pod službami, žiadateľ MUSÍ identifikovať príslušné opakovane použiteľné informácie o záruke a reziduálne opatrenia implementované žiadateľom.

IV.4 Certifikačný plán, model závislostí a opakovane použiteľné informácie o záruke

Normatívna požiadavka: Žiadateľ MUSÍ predložiť úplný zoznam existujúcich certifikátov zhody a ďalších informácií o zárukách, ktoré sa majú použiť ako dôkaz.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť certifikačný plán, v ktorom identifikuje komponenty plánované na samostatnú certifikáciu a ich predpokladané časové harmonogramy.

Normatívna požiadavka: Pre každú informáciu o záruke, ktorú je možné opätovne použiť, žiadateľ MUSÍ uviesť totožnosť a spôsobilosť vydavateľa, dobu platnosti, príslušný rámec alebo normu, hodnotený predmet, predpoklady, nezhody a priradenie k požiadavkám schémy.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť bezpečnostné ciele, technické hodnotiace správy, vyhlásenia o použiteľnosti, certifikačné správy, prepojovacie listy, správy o dohľade alebo rovnocenné dokumenty o predmete certifikácie pre certifikované komponenty a certifikované služby.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť súvisiace usmernenia, integračné dokumenty, predpoklady a obmedzenia prevádzkového prostredia potrebné na overenie, že integrácia bola vykonaná správne.

Normatívna požiadavka: Ak sa opätovne používajú dôkazy z hodnotení QTSP, národných auditov kybernetickej bezpečnosti, certifikátov EUCC/Common Criteria, ISO/IEC 27001, auditov ETSI, FCAF alebo iných posudzovaní zhody, žiadateľ MUSÍ vysvetliť zamýšľané opätovné použitie a navrhované zostávajúce činnosti CAB.

IV.5 Posúdenie rizík, plán hodnotenia a odôvodnenie rozsahu

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť posúdenie rizík špecifické pre implementáciu, v ktorom podrobne opíše riziká a hrozby v oblasti kybernetickej bezpečnosti pre hodnotenú službu IKT.

Normatívna požiadavka: Žiadateľ použije externý technický referenčný dokument „Wallet-Related Service Provider Security Requirements, Version 0.5.614, March 2026“[1] , založený na norme EN 319 401, ako podporný zdroj na prípravu mapovania opatrení a odôvodnenia pokrytia rizík, ak je to relevantné pre predmet certifikácie. Žiadateľ nie je povinný reprodukovať celý citovaný dokument v balíku certifikačných dôkazov. Namiesto toho žiadateľ určí, ktoré požiadavky, mapovania rizík a skupiny požiadaviek z externého referenčného dokumentu sa vzťahujú na deklarovaný modul, architektonický profil, modifikátor prípadu použitia ONL/PRX a predmet integrácie podľa slovenských národných predpisov. Neaplikovateľnosť sa odôvodní v posúdení rizík alebo v mapovaní dôkazov.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť formálne mapovanie implementovaných opatrení na riziká a hrozby v oblasti kybernetickej bezpečnosti identifikované v registri rizík Únie uvedenom v prílohe I k nariadeniu (EÚ) 2024/2981.

[1] alebo posledná dostupná verzia

Normatívna požiadavka: Žiadateľ MUSÍ odôvodniť každé riziko alebo hrozbu označené ako neuplatniteľné a MUSÍ vysvetliť, prečo záver o neuplatniteľnosti vyplýva z deklarovanej architektúry, profilu, modifikátora prípadu použitia alebo hranice modulu.

Normatívna požiadavka: Žiadateľ MUSÍ identifikovať riziká špecifické pre implementáciu, ktoré nie sú výslovne uvedené v registri rizík Únie, najmä riziká vyplývajúce zo smerovania Remote WSCD, predpokladov týkajúcich sa mobilných zariadení, integrácie národných PID, dostupnosti služby validácie, registrácie spoliehajúcej sa strany alebo slovenských zákonných procesov.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť navrhovaný plán hodnotenia a validácie špecifický pre danú implementáciu. Plán MUSÍ identifikovať audity, inšpekcie, skúšanie, analýzu závislostí, testovanie funkčnej zhody, posúdenie zraniteľnosti, penetračné testovanie a vzorkovacie činnosti navrhované pre certifikovaný predmet.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť odôvodnenie preukazujúce vhodnosť navrhovaného plánu hodnotenia na pokrytie všetkých príslušných opatrení, rizík, modulov, profilov, modifikátorov prípadov použitia a závislostí.

IV.6 Dôkazy o implementácii, testovacie artefakty a zoznam komponentov

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť prístup k potrebným testovacím prostrediam, reprezentatívnym zariadeniam, rozhraniam API, testovacím povereniam, testovacím údajom a technickej podpore potrebnej na hodnotenie.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť dôkazy získané priamo počas testov, pilotných projektov alebo kontrolovanej prevádzky na preukázanie prevádzkovej účinnosti implementovaných opatrení, ak ešte nie sú k dispozícii historické dôkazy z prevádzky.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť vyčerpávajúci zoznam komponentov tretích strán používaných pri implementácii hodnotenej služby IKT, v ktorom podrobne uvedie názov komponentu, verziu, dodávateľa, úlohu v službe, stav v rámci predmetu alebo závislosť a predchádzajúci stav posudzovania zhody.

Normatívna požiadavka: Ak hodnotená služba IKT zahŕňa softvérové komponenty alebo nasaditeľné artefakty, žiadateľ MUSÍ poskytnúť binárne súbory aplikácií, zostavenia, balíky verzií a zoznam softvérových komponentov.

Normatívna požiadavka: V prípade softvérových komponentov aplikácie riešenia peňaženky žiadateľ MUSÍ predložiť dôkaz o licencovaní open source v súlade s článkom 5a ods. 3 nariadenia (EÚ) č. 910/2014, ak sa toto ustanovenie uplatňuje, vrátane umiestnenia repozitára, informácií o licencii, predmete zverejnenia a akýchkoľvek odôvodnených výnimiek.

Normatívna požiadavka: Ak sa funkčná zhoda posudzuje pomocou FCAF, súboru slovenských národných integračných testov alebo iného určeného rámca, žiadateľ MUSÍ poskytnúť vyplnené vyhlásenie o zhode, vyhlásenie o zhode implementácie alebo ekvivalentný vstupný artefakt špecifický pre daný rámec.

Normatívna požiadavka: Ak je to relevantné, žiadateľ MUSÍ predložiť dokumentáciu o architektonickom preskúmaní súladu so zásadami ochrany súkromia už v štádiu návrhu, vrátane dôkazov o selektívnom zverejňovaní, neprepojiteľnosti, súhlase používateľa, minimalizácii údajov a obmedzeniach logovania transakcií.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť dôkazy o skúškach vývojárov, artefakty interného posúdenia zraniteľnosti, artefakty penetračných testov, záznamy o nápravných opatreniach a záznamy o známych zraniteľnostiach.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť politiku riadenia zraniteľností a súvisiace postupy, ktoré preukazujú, ako držiteľ osvedčenia spĺňa požiadavky stanovené v prílohe I k nariadeniu (EÚ) 2024/2847 (zákon o kybernetickej odolnosti), ak sa to vzťahuje na certifikovanú službu IKT alebo jej komponenty.

Normatívna požiadavka: Žiadateľ MUSÍ poskytnúť podrobnosti o zdrojovom kóde alebo dôkazy o preskúmaní zdrojového kódu, ak je to potrebné na posúdenie zraniteľnosti na základe kritickosti komponentov a vystavenia riziku.

IV.7 Balík verejne dostupných informácií

Normatívna požiadavka: Pre všetky moduly žiadateľ MUSÍ predložiť balík verejných informácií, vrátane odkazu na webovú stránku držiteľa certifikátu, ktorá obsahuje informácie, ktoré musia byť podľa certifikačnej schémy verejne dostupné.

Normatívna požiadavka: Balík verejných informácií MUSÍ obsahovať, ak je to relevantné, názov a verziu certifikovanej služby, identitu držiteľa certifikátu, predmet certifikátu, obmedzenia používania, predpoklady viditeľné pre používateľov, usmernenie pre používateľov, obdobie bezpečnostnej podpory, kontaktné informácie, metódy hlásenia zraniteľností a odkazy na verejné repozitáre alebo odporúčania.

Normatívna požiadavka: V prípade modulu EUDIW-SK Solution žiadateľ MUSÍ poskytnúť informácie špecifické pre peňaženku určené na zverejnenie, vrátane obmedzení používania riešenia peňaženky, usmernení na bezpečnú konfiguráciu, usmernení na inštaláciu a údržbu, obdobia podpory kybernetickej bezpečnosti, akceptovaných spôsobov prijímania informácií o zraniteľnostiach a odkazov na verejne zverejnené zraniteľnosti alebo upozornenia.

Normatívna požiadavka: Ak by verejné informácie odhalili citlivé bezpečnostné informácie, žiadateľ MUSÍ poskytnúť verejnú verziu a dôvernú verziu s odôvodnením redigovania.

IV.8 Dôkazy o slovenskej zákonnej a národnej integrácii

Informatívny popis: Táto časť transformuje slovenské národné rozšírenie z prílohy I na povinnosti týkajúce sa dôkazov. Nevytvára nový predmet certifikácie; zabezpečuje, aby boli zákonné schopnosti a národné integračné mechanizmy, ktoré ovplyvňujú certifikovaný predmet, zdokumentované a kontrolovateľné.

Normatívna požiadavka: Ak je to relevantné, žiadateľ MUSÍ poskytnúť zdokumentované postupy a technické dôkazy, ktoré preukazujú, ako sa informácie potrebné na monitorovanie dodržiavania (predpisov/zhody) poskytujú orgánu na požiadanie.

Normatívna požiadavka: Ak je to relevantné, žiadateľ MUSÍ poskytnúť dôkazy, ktoré preukazujú, ako je možné prijímať, sledovať, implementovať a preukazovať nápravné opatrenia uložené orgánom.

Normatívna požiadavka: Ak je to relevantné, žiadateľ MUSÍ poskytnúť postupy a technické mechanizmy na pozastavenie alebo zrušenie registrácie spoliehajúcej sa strany na základe rozhodnutia orgánu.

Normatívna požiadavka: Ak je to relevantné, žiadateľ MUSÍ predložiť dôkazy o automatizovanom oznamovaní informácií o spoliehajúcich sa stranách Ministerstvu vnútra počas procesu registrácie.

Normatívna požiadavka: Ak je to relevantné, žiadateľ MUSÍ poskytnúť postupy, postupy eskalácie a Logovanie na bezodkladné hlásenie podozrenia z nezákonného alebo podvodného používania európskej peňaženky orgánu.

Normatívna požiadavka: Ak je to relevantné, žiadateľ MUSÍ predložiť dôkaz, že dôveryhodné strany môžu bezodkladne aktualizovať certifikáty a prostriedky vzájomnej autentifikácie s európskou peňaženkou.

Normatívna požiadavka: Žiadateľ MUSÍ predložiť dôkazy o národnej integrácii pre národného poskytovateľa PID, národné mechanizmy validácie dôveryhodných strán a bezplatné mechanizmy validácie, ak sú súčasťou certifikovaného predmetu alebo povinných závislostí.

Informatívny popis: Nasledujúca matica je operačný nástroj odvodený z vyššie uvedených normatívnych požiadaviek. Slúži na podporu prípravy žiadateľa a plánovania zo strany CAB. Neobmedzuje schopnosť CAB požadovať dodatočné dôkazy.

Tabuľka IV-3 – Kontrolný zoznam podkladov žiadateľa / matica dôkazov

Č.	Požiadavka na dokument / informáciu	Platí pre	Stav	Očakávaný formát / príklad	Klasifikácia
IV.1	Identifikácia žiadateľa a držiteľa osvedčenia	Všetky moduly	Povinné	Formálne vyhlásenie obsahujúce právnu identitu, kontaktné miesto a zamýšľaného držiteľa osvedčenia	Verejné/Dôverné
IV.1	Vyhlásenie o predmete priradené k modulom a profilom uvedeným v prílohe I	Všetky moduly	Povinné	Matica predmetu pôsobnosti prílohy I zahŕňajúca riešenie EUDIW-SK, službu SK-PID, službu SK-Validácia, závislosti a modifikátory ONL/PRX	Verejné/Dôverné
IV.1	Právna úloha a zákonný základ	Všetky moduly	Povinné	Stručné právne odôvodnenie zahŕňajúce eIDAS, slovenské právo a úlohu špecifickú pre daný modul	Verejné/Dôverné
IV.1	Mapovanie úloh prevádzkovateľa, subdodávateľa a tretej strany	Všetky moduly	Povinné	Matica zodpovedností, zmluvy, mapy služieb, model RACI a delegovania	Dôvernosť
IV.1	Stav QTSP alebo dôkaz o zmluve QTSP	Riešenie EUDIW-SK	Povinné, ak to vyžaduje slovenské právo	Certifikát QTSP, dôkaz o zaradení do zoznamu dôveryhodných subjektov alebo platná zmluva s QTSP	Dôvernosť
IV.2	Návrhy architektúry a model závislostí	Všetky moduly	Povinné	Súčasná produkčná architektúra, katalóg komponentov, model nasadenia a mapa závislostí	Dôvernosť
IV.2	Mapovanie rozhrania, toku dát a hraníc dôveryhodnosti	Všetky moduly	Povinné	DFD, zoznam API, diagram hraníc dôveryhodnosti, diagramy integračných sekvencií	Dôvernosť
IV.2	Základné konfigurácie a nastavenia softvéru	Všetky moduly	Povinné	Základná konfigurácia, základné bezpečnostné nastavenia, parametre nasadenia, identifikátory verzií	Dôvernosť

Č.	Požiadavka na dokument / informáciu	Platí pre	Stav	Očakávaný formát / príklad	Klasifikácia
IV.2	Prevádzkové lokality a priestory	Všetky moduly so službami na pozadí	Povinné	Zoznam zariadení, umiestnenia hostingu, dôkazy o regióne cloudu, prevádzková zodpovednosť	Dôvernosť
IV.2	Prevádzkové procesy	Všetky moduly	Povinné tam, kde sa proces uplatňuje	Zavádzanie nových zamestnancov, registrácia, správa EIM, prideľovanie oprávnení, aktualizácia, incidenty, zraniteľnosti, zmeny a podvody – štandardné operačné postupy	Dôvernosť
IV.2	Predpoklady týkajúce sa prostredia a mechanizmy vynútiteľnosti	Všetky moduly	Povinné	Register predpokladov, kontroly počas prevádzky, osvedčenie zariadenia, kompenzačné opatrenia	Dôvernosť
IV.3	Bezpečnostné opatrenia a mapovanie stupňa záruky	Všetky moduly	Povinné	Vyhlásenie o uplatniteľnosti alebo ekvivalentný katalóg kontrolných opatrení priradený k CIR 2015/1502 a kritériám schémy	Dôvernosť
IV.3	Priradenie opatrení k zložkám	Všetky moduly	Povinné	Matica sledovateľnosti spájajúca opatrenia, zložky, procesy a dôkazy	Dôvernosť
IV.3	Popis účinnosti	Všetky moduly	Povinné	Argument týkajúci sa účinnosti, ktorý vysvetľuje, ako opatrenia zmierňujú riziká na úrovni záruky vysoká	Dôvernosť
IV.4	Existujúce certifikáty a informácie o záruke	Všetky moduly	Povinné v prípade opätovného použitia	EUCC, Spoločné kritériá, ISO/IEC 27001, ETSI, QTSP, národný audit kybernetickej bezpečnosti, FCAF a ďalší zoznam dôkazov	Verejné/Dôverné
IV.4	Bezpečnostné ciele, ETR, SoA a dokumenty o predmete	Certifikované komponenty a opätovne použité služby	Podmienené	Cieľ bezpečnosti, technická hodnotiaca správa, vyhlásenie o použiteľnosti, prepojovacie listy, listy o dohľade	Dôvernosť
IV.4	Usmernenie pre integráciu a predpoklady z certifikovaných komponentov	Všetky moduly, ktoré sa spoliehajú na komponenty	Povinné, ak je to relevantné	Usmernenia, predpoklady prevádzkového prostredia, obmedzenia integrácie a potreby týkajúce sa zostatkových dôkazov	Dôvernosť
IV.5	Posúdenie rizík špecifických pre implementáciu	Všetky moduly	Povinné	Register rizík, správa o posúdení rizík a plán ošetrenia rizika	Dôvernosť
IV.5	Prepojenie s registrom rizík Únie	Všetky moduly	Povinné	Matica pokrytia hrozieb a rizík vrátane odôvodnení neaplikovateľnosti	Dôvernosť
IV.5	Navrhovaný plán hodnotenia a validácie	Všetky moduly	Povinné	Plán hodnotenia opisujúci audit, inšpekciu, skúšanie, analýzu závislostí, odber vzoriek a opätovné použitie dôkazov	Dôvernosť
IV.6	Testovacie prostredia, zariadenia a rozhrania API	Všetky moduly	Povinné v prípadoch, kde sa uplatňuje skúšanie	Prístup k sandboxu, reprezentatívne zariadenia, testovacie prihlasovacie údaje, koncové body API a testovacie údaje	Dôvernosť
IV.6	Dôkazy o prevádzkovej účinnosti	Všetky moduly	Povinné	Pilotné protokoly, auditové stopy, protokoly transakcií, vzorové záznamy, záznamy o zmenách a incidentoch	Dôvernosť
IV.6	Zoznam komponentov tretích strán	Všetky moduly	Povinné	Register majetku dodávateľa, úloha komponentu, verzia, stav v predmete pôsobnosti, stav zhody	Dôvernosť
IV.6	Binárne súbory aplikácií, zostavenia a SBOM	Softvérové moduly	Povinné v prípade existencie softvéru	Binárne súbory, zostavenia, balíky verzií, SBOM v CycloneDX/SPDX alebo ekvivalente	Dôvernosť
IV.6	Vyhlásenie o zhode a artefakty funkčných testov	Moduly podliehajúce skúšaniu funkčnosti	Podmienečné	ICS, vstupy FCAF, záznamy o národných integračných testoch, testovacie protokoly	Dôvernosť
IV.6	Preskúmanie architektúry z hľadiska ochrany súkromia už v štádiu návrhu	Všetky moduly spracúvajúce osobné údaje	Podmienečné	DPIA, preskúmanie ochrany súkromia, selektívne zverejňovanie a dôkazy o neodvysledovateľnosti	Dôvernosť
IV.6	Dôkazy z testov vývojárov a interné artefakty zraniteľnosti	Všetky moduly	Povinné	Interné protokoly o skúšaní, správy o skenovaní, správy o penetračných testoch, záznamy o nápravných opatreniach	Dôvernosť
IV.6	Prístup k zdrojovému kódu alebo dôkazy o preskúmaní zdrojového kódu	Kľúčové softvérové komponenty	Podmienečné	Prístup k úložisku, správa o preskúmaní zdrojového kódu, dôkazy SAST/DAST	Dôvernosť
IV.7	Všeobecný balík transparentnosti a odkaz na webovú stránku	Všetky moduly	Povinné	Verejná webová stránka s informáciami o držiteľovi certifikátu, obmedzeniami predmetu, usmerneniami pre používateľov, dobou platnosti podpory a kontaktom pre hlásenie zraniteľností	Verejné
IV.7	Verejné informácie v prílohe V týkajúce sa peňaženky	Riešenie EUDIW-SK	Povinné	Obmedzenia používania, usmernenia pre bezpečnú konfiguráciu, doba poskytovania bezpečnostnej podpory, spôsob hlásenia zraniteľností, verejné upozornenia	Verejné
IV.8	Dôkaz o splnení zákonných povinností v Slovenskej republike	Príslušné slovenské úlohy	Povinné, ak je to relevantné	Postupy a rozhrania pre žiadosti orgánov, nápravné opatrenia, pozastavenie/zrušenie registrácie dôverujúcej strany, podávanie správ a podporu aktualizácie certifikátov	Dôverné/Verejné podľa potreby
IV.8	Dôkazy o národnej integrácii	Riešenie EUDIW-SK, služba SK-PID, služba SK-Validácia	Povinné, ak je to relevantné	Integrácia s národným poskytovateľom PID, registrom dôveryhodných strán/mechanizmami validácie a bezplatnými mechanizmami validácie	Dôvernosť

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

PRÍLOHA V – Obsah certifikátu EUDIW-SK

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny popis – poznámka k vypracovaniu: Táto príloha používa európsky návrh prílohy V ako hlavný základ a dopĺňa polia špecifické pre Slovensko, potrebné na modulárnu certifikáciu, architektonické profily, modifikátory prípadov použitia ONL/PRX, zmeny certifikátov, vnútroštátne orgány a balík verejnej transparentnosti.

V.0 Účel a výklad

Informatívny text: Príloha V definuje minimálny obsah certifikátu EUDIW-SK. Certifikát je verejným formálnym potvrdením certifikačného rozhodnutia. Podrobné verejné vysvetlenie patrí do certifikačnej správy podľa prílohy VI a podrobné informácie o hodnotení patria do správy o certifikačnom posúdení alebo do technickej dokumentácie o hodnotení podľa prílohy VII.

Normatívna požiadavka: Certifikát EUDIW-SK MUSÍ jasne identifikovať certifikovanú službu IKT, držiteľa certifikátu, certifikačný orgán, certifikovaný predmet, príslušná schéma, úroveň záruky, dobu platnosti a umiestnenie verejných informácií.

Normatívna požiadavka: Certifikát NESMIE naznačovať certifikáciu funkcií, modulov, architektonických profilov, prípadov použitia, variantov, závislostí alebo poskytovateľov služieb, ktoré nie sú výslovne zahrnuté v predmete certifikátu.

V.1 Jedinečná identifikácia certifikátu

Normatívna požiadavka: Certifikát MUSÍ obsahovať jedinečný identifikátor certifikátu pridelený certifikačným orgánom, ktorý certifikát vydáva.

Normatívna požiadavka: Identifikátor MUSÍ byť dostatočný na odlíšenie certifikátu od všetkých ostatných certifikátov vydaných v rámci schémy a MAL BY obsahovať alebo byť sledovateľný k názvu schémy, referencii akreditácie alebo autorizácie certifikačného orgánu, roku vydania a poradovému číslu certifikátu.

Normatívna požiadavka: Certifikát MUSÍ obsahovať jedinečný odkaz na príslušnú slovenskú národnú certifikačnú schému EUDI Wallet a na príslušnú verziu schémy.

V.2 Informácie o certifikovanej službe IKT a držiteľovi certifikátu

Normatívna požiadavka: Certifikát MUSÍ obsahovať názov certifikovanej služby IKT, prípadne akýkoľvek obchodný názov, a presnú certifikovanú verziu, vydanie, zostavenie alebo konfiguračnú základňu.

Normatívna požiadavka: Certifikát MUSÍ uvádzať typ služby IKT s použitím kategórií definovaných v jadre schémy a v prílohe I, vrátane informácie, či certifikát pokrýva riešenie peňaženky a schému eID spoločne, modul riešenia peňaženky, modul služby PID, modul validačnej služby alebo iný jasne vymedzený predmet povolený schémou.

Normatívna požiadavka: Certifikát MUSÍ identifikovať držiteľa certifikátu podľa mena, adresy a kontaktných informácií.

Normatívna požiadavka: Certifikát MUSÍ obsahovať odkaz na webovú stránku držiteľa certifikátu, ktorá obsahuje informácie, ktoré musia byť verejne dostupné podľa prílohy III.

Normatívna požiadavka: V prípade potreby MUSÍ certifikát identifikovať vlastníka certifikačnej schémy, vydávajúci členský štát, zodpovedný vnútroštátny orgán alebo dozorné rozhranie platné pre slovenský certifikačný systém.

V.3 Certifikovaný predmet, moduly, profily a obmedzenia

Normatívna požiadavka: Certifikát MUSÍ uvádzať certifikovaný modul alebo moduly s použitím terminológie prílohy I: Riešenie EUDIW-SK, Služba SK-PID, Služba SK-Validácia, záver o zastrešujúcej certifikácii alebo jasne vymedzená podmnožina modulov.

Normatívna požiadavka: V prípade modulu EUDIW-SK Solution certifikát MUSÍ identifikovať varianty inštancií peňaženky, na ktoré sa vzťahuje, architektonický profil alebo profily, na ktoré sa vzťahuje, a či sa vzťahujú modifikátory prípadov použitia online a/alebo v blízkosti.

Normatívna požiadavka: Certifikát MUSÍ identifikovať hlavné komponenty v predmete pôsobnosti a na vysokej úrovni akékoľvek kritické závislosti alebo opakovane použiteľné informácie o záruke, na ktorých sa certifikát zakladá.

Normatívna požiadavka: Certifikát MUSÍ identifikovať obmedzenia predmetu, vylúčené funkcie, vylúčené varianty, postupne zavádzané alebo odložené funkcie, predpoklady verejného prevádzkového prostredia a obmedzenia používania.

Normatívna požiadavka: Ak sa certifikát mení a dopĺňa, certifikát alebo priložený dodatok MUSÍ jasne identifikovať zmenený predmet, dátum zmeny a doplnenia, dôvod zmeny a doplnenia a vplyv na platnosť certifikátu.

V.4 Informácie o hodnotení a certifikácii

Normatívna požiadavka: Certifikát MUSÍ identifikovať vlastníka schémy podľa mena.

Normatívna požiadavka: Certifikát MUSÍ obsahovať odkazy na nariadenie (EÚ) č. 910/2014 a vykonávacie nariadenie Komisie (EÚ) 2024/2981.

Normatívna požiadavka: Certifikát MUSÍ uvádzať certifikačný orgán, ktorý certifikát vydal, vrátane jeho názvu, adresy a kontaktných údajov.

Normatívna požiadavka: Certifikát MUSÍ identifikovať, ak je to relevantné, subdodávateľov alebo laboratóriá, ktoré sa podieľali na hodnotení, na úrovni primeranej pre zverejnenie.

Normatívna požiadavka: Certifikát MUSÍ identifikovať zodpovedný národný certifikačný orgán pre kybernetickú bezpečnosť alebo ekvivalentný slovenský orgán zodpovedný za riadenie certifikácie na stupni záruky „vysoký“, ak je to relevantné.

Normatívna požiadavka: Certifikát MUSÍ odkazovať na certifikačnú správu podľa prílohy VI a na príslušnú správu o posúdení certifikácie alebo technickú správu o hodnotení zloženia podľa prílohy VII.

Normatívna požiadavka: Certifikát MUSÍ obsahovať odkaz na hlavné normy, technické špecifikácie, vykonávacie akty a prílohy schémy použité na hodnotenie, vrátane ich verzií, ak je to relevantné.

Normatívna požiadavka: Certifikát MUSÍ uvádzať dátum prvého vydania, dátum aktuálneho vydania, začiatok a koniec hodnotiaceho obdobia, ak je to primerané, dobu platnosti, dátum uplynutia platnosti, stav certifikátu a termín alebo predpokladaný čas nasledujúceho hodnotenia dohľadu.

V.5 Úroveň záruky, označenie a jazyk

Normatívna požiadavka: Certifikát MUSÍ uvádzať, že je vydaný na úroveň záruky vysoká v rámci príslušného rámca certifikácie kybernetickej bezpečnosti, a MUSÍ identifikovať akékoľvek samostatné vyhlásenie o stupni záruky podľa nariadenia eIDAS len vtedy, ak predmet certifikácie a hodnotenie takúto záruku podporujú.

Normatívna požiadavka: Ak je s certifikátom spojená značka alebo označenie, certifikát MUSÍ obsahovať alebo odkazovať na pravidlá týkajúce sa značiek a označení uvedené v prílohe XII.

Normatívna požiadavka: Certifikát MUSÍ byť poskytnutý v úradnom jazyku Európskej únie. Pre slovenský národný systém MUSÍ byť k dispozícii národná verzia a na podporu cezhraničného používania MUSÍ byť k dispozícii anglický preklad, pokiaľ vlastník schémy nestanoví iný rovnocenný mechanizmus zverejňovania.

V.6 Matica obsahu osvedčenia

Normatívna požiadavka: Matica obsahu osvedčenia MUSÍ obsahovať meno vlastníka schémy a odkazy na nariadenie (EÚ) č. 910/2014 a vykonávacie nariadenie Komisie (EÚ) 2024/2981 ako povinné polia osvedčenia.

Pole certifikátu	Minimálny obsah	Dôvod / odkaz na iné prílohy
Jedinečný identifikátor	Odkaz na schému, odkaz na certifikačný orgán, rok a číslo certifikátu alebo ekvivalentný jedinečný identifikátor	Sledovateľnosť certifikátu a označenie podľa prílohy XII
Certifikovaná služba IKT	Názov, typ, certifikovaná verzia, základná verzia/súbor/konfigurácia	Presnosť predmetu podľa prílohy I
Držiteľ certifikátu	Názov, adresa, kontaktné údaje a URL s verejnými informáciami	Uverejnenie v prílohe III
Certifikované moduly	Riešenie EUDIW-SK, služba SK-PID, služba SK-Validácia, zastrešujúci modul alebo povolená podmnožina	Predmet pôsobnosti prílohy I
Profily a toky	Profily A–D, modifikátory ONL/PRX, varianty inštancií peňaženiek, ak je to relevantné	Hodnotenie zohľadňujúce profily podľa príloh I, X a XI
Obmedzenia a predpoklady	Verejné obmedzenia, vylúčené funkcie, prevádzkové predpoklady a obmedzenia používania	Prílohy III a VI – transparentnosť
Závislosti	Kľúčové závislosti na vysokej úrovni a referencie o opätovne použiteľnej záruke	Analýza závislostí podľa prílohy IX
Certifikačný orgán a orgány	Certifikačný orgán vydávajúci certifikát, prípadne subdodávatelia, zodpovedný orgán	Prílohy VIII, XIII a základný rámec schémy
Správy	Odkaz na certifikačnú správu podľa prílohy VI a CAR/ETR podľa prílohy VII	Sledovateľnosť certifikačného rozhodnutia
Normy a verzia schému	Platná verzia schémy a hlavné normy/technické špecifikácie	Prílohy X a XI
Dátumy a stav	Prvé vydanie, aktuálne vydanie, platnosť, uplynutie platnosti, stav a najbližší termín dozoru	Životný cyklus prílohy II
Značka alebo štítok	Odkaz na značku/označenie alebo informácia, že značka dôveryhodnosti peňaženky sa riadi osobitne	Príloha XII

PRÍLOHA VI – Obsah certifikačnej správy

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny popis – poznámka k vypracovaniu: Príloha VI EÚ sa môže použiť ako hlavný základ, nie je však postačujúca ako surová kópia pre slovenskú schému, pretože slovenská príloha I zavádza modulárny predmet, architektonické profily, modifikátory ONL/PRX, národnú zákonnú integráciu a explicitné klasifikácie závislostí. Táto príloha preto zachováva štruktúru EÚ a začleňuje slovenskú logiku podávania správ.

VI.0 Účel, stav a logika zverejňovania

Informatívny popis: Certifikačná správa je verejná alebo verejne zdieľateľná správa, ktorá sprevádza certifikát. Vysvetľuje certifikovanú službu IKT, jej predmet, obmedzenia, bezpečnostný model a výsledok hodnotenia bez zverejnenia citlivých podrobností, ktoré patria do správy o posúdení certifikácie alebo technickej správy o hodnotení.

Normatívna požiadavka: Pre každý certifikát EUDIW-SK certifikačný orgán VYHOTOVÍ certifikačnú správu na základe technickej správy o hodnotení, správy o posúdení certifikácie a preskúmania rozhodnutia o certifikácii.

Normatívna požiadavka: Certifikačná správa MUSÍ obsahovať všetky verejne dostupné a zdieľateľné informácie relevantné pre používateľov, dôverujúce strany, príslušné orgány a zainteresované strany. Citlivé technické podrobnosti MÔŽU byť uvedené v dôverných správach namiesto toho, aby boli zverejnené.

Normatívna požiadavka: Správa o certifikácii MUSÍ byť v súlade s certifikátom, vyhlásením o predmete v prílohe I, súborom dôkazov v prílohe IV, rozhodnutiami o závislosti v prílohe IX, kritériami v prílohe X a metódami v prílohe XI.

VI.1 Požadované časti certifikačnej správy

Normatívna požiadavka: Správa o certifikácii MUSÍ obsahovať aspoň tieto časti: súhrn; identifikáciu certifikovanej služby IKT; opis certifikovanej služby IKT; informácie o verejnej bezpečnosti; súhrn hodnotenia a plánu hodnotenia; súhrn preskúmania a rozhodnutia o certifikácii; súhrn obmedzení, predpokladov a závislostí; informácie o údržbe a dohľade; a bibliografiu.

Časť	Minimálny obsah	Slovenský dodatok
Zhrnutie	Identifikátor certifikátu, držiteľ certifikátu, certifikovaná služba IKT, úroveňzáruky a záver.	Uveďte, či certifikát zahŕňa riešenie EUDIW-SK, službu SK-PID, službu SK-Validácia alebo zastrešujúcu certifikáciu.
Identifikácia služby IKT	Názov, verzia, držiteľ certifikátu, kontakt, predmet certifikátu a platnosť certifikátu.	Identifikujte moduly, profily A–D, toky ONL/PRX, certifikované verzie a obmedzenia predmetu.
Popis služby IKT	Architektúra, komponenty, zásady, opatrenia, predpoklady a verejné informácie.	Použite taxonómiu modulov/profilov z prílohy I a rozlišujte priamy predmet, závislosti a vylúčenia.
Informácie o verejnej bezpečnosti	Požiadavky na informácie podľa prílohy III a verejné usmernenia.	Zahrňte obmedzenia pre používateľov, dobu podpory, hlásenie zraniteľností a obmedzenia národnej integrácie, ak je to relevantné.
Zhrnutie hodnotenia	Hodnotiace činnosti, plán, metódy, odber vzoriek, testy a výsledky na vysokej úrovni.	Zhrňte kritériá prílohy X a metódy prílohy XI podľa modulov a profilov bez citlivých podrobností.
Preskúmanie a rozhodnutie	Rozhodnutie o certifikácii, dosiahnutý úroveň záruky, platnosť a jedinečný identifikátor.	Uveďte odôvodnenie rozhodnutia pre všeobecné závery a klasifikácie závislosti.

Časť	Minimálny obsah	Slovenský dodatok
Informácie o udržiavaní	Termín dohľadu a povinnosti týkajúce sa údržby.	Určenie termínu nasledujúceho ročného dohľadu, termínu recertifikácie a povinností oznamovania významných udalostí.
Bibliografia	Hodnotiace kritériá, normy, správy a dokumentácia vývojára.	Uveďte dokumenty podľa verzie/dátumu a odkazujte na triedy dôkazov v prílohe IV bez zverejnenia dôverného obsahu.

VI.2 Súhrn

Normatívna požiadavka: Súhrn MUSÍ obsahovať stručný opis výsledku certifikácie, vrátane identifikátora certifikátu, držiteľa certifikátu, certifikovanej služby IKT, stupňa záruky, doby platnosti certifikátu, certifikačného orgánu a informácie o tom, či išlo o počiatočnú certifikáciu, certifikáciu na základe dohľadu, zmenenú certifikáciu, špeciálnu certifikáciu alebo recertifikáciu.

Normatívna požiadavka: Súhrn MUSÍ uvádzať, či je záver certifikácie samostatný alebo zložený a či sa opiera o opakovane použiteľné informácie o zárukách.

VI.3 Identifikácia služby IKT

Normatívna požiadavka: Certifikačná správa MUSÍ identifikovať certifikovanú službu IKT s dostatočnou presnosťou, aby sa predišlo nejednoznačnosti. MUSÍ obsahovať názov, obchodné alebo úradné označenie, verziu, vydanie, identifikátory zostavenia alebo konfigurácie, držiteľa certifikátu a webovú stránku, na ktorej sú k dispozícii verejné informácie.

Normatívna požiadavka: Správa MUSÍ identifikovať certifikovaný modul alebo moduly: riešenie EUDIW-SK, službu SK-PID, službu SK-Validácia, zdieľané závislosti alebo zastrešujúci certifikačný záver pokrývajúci riešenie peňaženky a schému eID, v rámci ktorej sa poskytuje.

Normatívna požiadavka: Ak certifikovaný predmet zahŕňa riešenie peňaženky, správa MUSÍ identifikovať deklarované varianty inštancií peňaženky, podporované platformy, architektonické profily A–D, modifikátory prípadov použitia ONL a/alebo PRX a hlavné rodiny protokolov alebo formátov údajov, na ktoré sa certifikácia vzťahuje.

Normatívna požiadavka: Správa MUSÍ identifikovať funkcie zahrnuté v predmete certifikácie a funkcie výslovne vylúčené z predmetu certifikácie, vrátane pilotných, demo, testovacích, budúcich alebo odložených funkcií, ak je to relevantné.

VI.4 Opis certifikovanej služby IKT

Normatívna požiadavka: Správa MUSÍ opísať architektúru a komponenty služby IKT, vrátane požadovaného hardvéru, softvéru, procesov, podslužieb IKT a závislostí na úrovni vhodnej pre verejné pochopenie a budúce opätovné použitie.

Normatívna požiadavka: Správa MUSÍ opisovať bezpečnostné politiky relevantné pre používateľov a spoliehajúce sa strany a MÔŽE odkazovať na balík verejných informácií požadovaný v prílohe III.

Normatívna požiadavka: Správa MUSÍ opisovať rámec opatrení na vysokej úrovni, vrátane toho, ako sa opatrenia vzťahujú na hlavné riziká, moduly, profily a závislosti, bez zverejnenia citlivých podrobností o implementácii.

Normatívna požiadavka: Správa MUSÍ uvádzať predpoklady prevádzkového prostredia a verejné obmedzenia, ktoré sú relevantné pre súladné a bezpečné používanie certifikovanej služby IKT.

Normatívna požiadavka: Správa MUSÍ uvádzať zoznam komponentov alebo podslužieb, ktoré boli hodnotené pred hodnotením EUDIW-SK, vrátane verzie, odkazu na informácie o záruke, dátumu, platnosti a súhrnu predmetu, ak je možné takéto informácie zverejniť.

Normatívna požiadavka: Správa MUSÍ obsahovať alebo odkazovať na úplný súbor informácií, ktoré sa majú zverejniť podľa prílohy III, vrátane usmernení na bezpečné používanie, obmedzení používania, obdobia bezpečnostnej podpory, kontaktných údajov na hlásenie zraniteľností a odkazov na verejné repozitáre zraniteľností alebo upozornenia.

Normatívna požiadavka: Ak certifikovaná služba IKT zahŕňa riešenie peňaženky, správa MUSÍ obsahovať alebo odkazovať na usmernenia pre používateľov špecifické pre peňaženku týkajúce sa inštalácie, aktivácie, aktualizácie, zrušenia, pozastavenia, obnovenia, straty alebo krádeže zariadenia, bezpečného vyradenia z prevádzky a obmedzenia predmetu služby.

VI.6 Zhrnutie hodnotenia a plán hodnotenia

Normatívna požiadavka: Správa MUSÍ obsahovať zhrnutie hodnotenia a jeho výsledkov, vrátane plánu hodnotenia, hodnotiacich činností, vybraných metód, odôvodnenia výberu vzorky, funkčného skúšania, posúdenia zraniteľnosti, analýzy závislostí a posúdenia prevádzkovej účinnosti.

Normatívna požiadavka: Správa MUSÍ na súhrnnej úrovni vysvetliť, ako hodnotenie pokrylo kritériá uvedené v prílohe X a metódy uvedené v prílohe XI pre každý modul, profil, modifikátor prípadu použitia a závislosť v predmete pôsobnosti.

Normatívna požiadavka: V prípade hodnotenia údržby správa MUSÍ obsahovať zhrnutie nezhôd, významných udalostí, zmien certifikátu a významných zmien od predchádzajúceho hodnotenia v rozsahu primeranom na zverejnenie.

VI.7 Súhrn posúdenia a rozhodnutia o certifikácii

Normatívna požiadavka: Správa o certifikácii MUSÍ obsahovať potvrdenie dosiahnutého stupňa záruky a dátum vydania, dobu platnosti a jedinečný identifikátor certifikátu.

Normatívna požiadavka: Správa MUSÍ uvádzať, či certifikačný orgán ukončil hodnotenie a preskúmanie bez námietok a či niektoré nepodstatné nezhody podliehajú následnému sledovaniu.

Normatívna požiadavka: Ak sa certifikácia opiera o opätovne použiteľné informácie o záruke, správa MUSÍ zhrnúť kategórie spoľahlivosti bez zverejnenia dôverných údajov, pričom sa použijú typy výsledkov uvedené v prílohe IX: prijaté, prijaté s kompenzačnými opatreniami, prijaté s dodatočným skúšaním CAB alebo zamietnuté.

VI.8 Bibliografia a reprodukovateľnosť

Normatívna požiadavka: Časť bibliografia MUSÍ obsahovať odkazy na všetky dokumenty použité pri zostavovaní certifikačnej správy, vrátane hodnotiacich kritérií, dokumentov o najnovšom stave techniky, špecifikácií, technických hodnotiacich správ, správ o zložení, technických noriem a dokumentácie vývojára použitej pri hodnotiacich činnostiach.

Normatívna požiadavka: Na zaručenie reprodukovateľnosti MUSÍ byť každý dokument, na ktorý sa v certifikačnej správe odkazuje, jednoznačne identifikovaný názvom, vlastníkom alebo vydavateľom, verziou, dátumom a, ak je to primerané, klasifikáciou dôvernosti.

Normatívna požiadavka: Ak dokument nemožno zverejniť, certifikačná správa MUSÍ tento dokument dostatočne identifikovať, aby príslušné orgány a budúci hodnotitelia mohli požiadať o dôverný zdroj alebo ho vyhľadať prostredníctvom certifikačného orgánu alebo držiteľa certifikátu.

VI.9 Kontrolný zoznam certifikačnej správy

Č.	Položka certifikačnej správy	Povinný obsah
VI.2	Zhrnutie	Výsledok certifikácie, úroveň záruky, platnosť, certifikačný orgán a držiteľ certifikátu.
VI.3	Identifikácia služby IKT	Názov, verzia, modul, profil, toky ONL/PRX, zahrnuté/vylúčené funkcie.

Č.	Položka certifikačnej správy	Povinný obsah
VI.4	Popis služby	Architektúra, komponenty, bezpečnostný model, závislosti, predpoklady a obmedzenia.
VI.5	Verejné informácie	Príloha III – verejný balík, usmernenie pre používateľov, doba podpory a hlásenie zraniteľností.
VI.6	Zhrnutie hodnotenia	Hodnotiace činnosti, metódy, odber vzoriek, funkčné testy, posúdenie zraniteľnosti a analýza závislostí.
VI.7	Zhrnutie rozhodnutia	Dosiahnutý úroveň záruky, odôvodnenie rozhodnutia, stav nezhody a zhrnutie spoľahlivosti.
VI.8	Bibliografia	Všetky dokumenty identifikované podľa verzie/dátumu a statusu verejný/dôverný.

PRÍLOHA VII – Obsah technickej hodnotiacej správy o zložení a certifikačnej hodnotiacej správy

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny popis – poznámka k vypracovaniu: Príloha VII EÚ nemôže slúžiť ako vzor pre slovenský systém, pretože slovenský systém využíva modulárny predmet podľa prílohy I, hodnotenie zohľadňujúce profil, explicitné klasifikácie závislostí a integráciu do vnútroštátnych právnych predpisov. Táto príloha zachováva obsah technickej hodnotiacej správy EÚ o zložení a prispôsobuje ho štruktúre slovenskej hodnotiacej správy o certifikácii, ktorá je vhodná na použitie NCCA, dozornými orgánmi a pre budúce komplexné hodnotenie.

VII.0 Účel, dôvernosť a použitie

Informatívny text: Táto príloha definuje balík dôverných technických správ, ktorý podporuje rozhodnutie o certifikácii a budúce zloženie. Obsahuje viac podrobností ako verejná certifikačná správa podľa prílohy VI.

Normatívna požiadavka: Pre každý certifikát EUDIW-SK certifikačný orgán VYHOTOVÍ správu o posúdení certifikácie alebo technickú správu o hodnotení zloženia, ktorá podporuje rozhodnutie o certifikácii a umožňuje budúce opätovné použitie príslušnými orgánmi a CAB vykonávajúcimi kompozitné hodnotenia.

Normatívna požiadavka: Správa MUSÍ byť chránená ako dôverná, ak obsahuje citlivé bezpečnostné informácie, obchodné tajomstvá, osobné údaje, podrobnosti o zraniteľnosti, informácie o zdrojovom kóde, podrobnú architektúru alebo informácie o útokoch.

Normatívna požiadavka: Správa MUSÍ byť dostatočne úplná, aby príslušný orgán alebo budúci CAB mohol pochopiť certifikovaný predmet, dôkazy, kritériá, metódy, rozhodnutia o závislostiach, zistenia a odôvodnenie záveru certifikácie.

VII.1 Identifikačné a administratívne informácie

Normatívna požiadavka: Správa MUSÍ obsahovať odkaz na certifikát, s ktorým súvisí, a na certifikovanú službu IKT, vrátane aspoň jej názvu, verzie, vydania a konfigurácie, ako je uvedené v certifikáte a certifikačnej správe.

Normatívna požiadavka: Správa MUSÍ uvádzať držiteľa certifikátu, žiadateľa, ak je iný, registračné informácie, ak sú relevantné, poštovú a elektronickú adresu, ako aj príslušné informácie o dcérskych spoločnostiach, dodávateľoch a subdodávateľoch, ktorí vyrábajú, poskytujú alebo prevádzkujú komponenty v predmete certifikácie v mene držiteľa certifikátu.

Normatívna požiadavka: Správa MUSÍ uvádzať certifikačný orgán, referenčné číslo akreditácie, prípadne stav autorizácie alebo oznámenia a totožnosť zodpovednej osoby alebo osôb oprávnených prijať certifikačné rozhodnutie.

Normatívna požiadavka: Správa MUSÍ obsahovať zoznam mien a funkcií fyzických osôb zapojených certifikačným orgánom a subdodávateľmi do vykonávania posudzovania zhody, s výhradou platných pravidiel dôvernosti a ochrany údajov.

VII.2 Podrobný predmet a architektúra

Normatívna požiadavka: Správa MUSÍ obsahovať podrobný opis certifikovaného predmetu, vrátane každého produktu IKT, procesu IKT, služby IKT, spravovanej služby, organizačného procesu a závislosti, na ktoré sa posudzovanie vzťahuje.

Normatívna požiadavka: Správa MUSÍ priradiť certifikovaný predmet k prílohe I, vrátane riešenia EUDIW-SK, služby SK-PID, služby SK-Validácia, zdieľaných/externých závislostí, architektonických profilov A–D a modifikátorov prípadov použitia ONL/PRX.

Normatívna požiadavka: Správa MUSÍ obsahovať alebo odkazovať na architektonické diagramy, identifikátory verzií, diagramy toku údajov, diagramy hraníc dôveryhodnosti, model závislostí, dôkazy o mieste prevádzky a konfiguračné základné línie použité ako základ pre hodnotenie.

Normatívna požiadavka: Správa MUSÍ identifikovať všetky vylúčenia, obmedzenia, predpoklady, odložené funkcie, pilotné/testovacie/demonštračné komponenty a obmedzenia predmetu.

VII.3 Súbor dôkazov a register dokumentácie

Normatívna požiadavka: Správa MUSÍ obsahovať úplný zoznam verejných a interných dokumentov, ktoré boli súčasťou predmetu posudzovania zhody, s názvom, vlastníkom alebo vydavateľom, verziou, dátumom, klasifikáciou dôvernosti a umiestnením zdroja alebo identifikátorom registra dôkazov.

Normatívna požiadavka: Register dokumentácie MUSÍ obsahovať aspoň: podmienky alebo používateľské dohody; posúdenie rizík a mapovanie registra rizík Únie; interné prevádzkové dokumenty; uvádzané normy; informácie o WSCD/WSCA a HSM; dôveryhodné systémy alebo výrobky používané držiteľom certifikátu; certifikáty a správy o záruke; správy o skúškach; dôkazy o preskúmaní zdrojového kódu; a dôkazy o národnej integrácii.

Normatívna požiadavka: Správa MUSÍ uvádzať, či každý dôkaz prešiel inšpekciou, skúšaním, odobratý ako vzorka, použitý na základe analýzy závislosti, zamietnutý alebo použitý iba ako kontextová informácia.

VII.4 Mapovanie kontrolného rámca a kritérií

Normatívna požiadavka: Správa MUSÍ obsahovať opis kontrolného rámca držiteľa certifikátu a priradenie každého príslušného kritéria prílohy X ku opatreniam, zložkám, procesom, dôkazom a hodnotiacim činnostiam, ktoré podporujú zhodu.

Normatívna požiadavka: Pre každú požiadavku prílohy X, ktorá sa neuplatňuje, správa MUSÍ zaznamenať odôvodnenie neuplatnenia a prepojiť ho s certifikovaným predmetom, hranicou modulu, profilom, modifikátorom prípadu použitia alebo analýzou závislostí.

Normatívna požiadavka: Pre každú uplatniteľnú požiadavku MUSÍ správa identifikovať opatrenia prispievajúce k jej splneniu a odkazy na informácie o zárukách kvality zo zložiek, služieb alebo procesov hodnotených inde.

VII.5 Hodnotiace činnosti a výsledky

Normatívna požiadavka: Správa MUSÍ opisovať vykonané hodnotiace činnosti, odôvodnenie ich výberu a použitú metodiku, vrátane auditu, inšpekcie, funkčného skúšania, národného integračného skúšania, posúdenia zraniteľnosti, penetračného skúšania, analýzy závislostí, preskúmania rizík, preskúmania zdrojového kódu a metodiky odberu vzoriek, ak je to relevantné.

Normatívna požiadavka: Pre každú hodnotiacu činnosť MUSÍ správa obsahovať: povahu činnosti; časový rámec alebo obdobie, na ktoré sa vzťahuje; rozsah činnosti; odôvodnenie výberu vzoriek, ak sa použili; relevantnosť vo vzťahu k požiadavkám a opatreniam; súhrnný popis; výsledok; odchýlky; zistenia; a odôvodnenie, ak je to potrebné.

Normatívna požiadavka: Správa MUSÍ rozlišovať medzi činnosťami vykonávanými priamo CAB, činnosťami vykonávanými subdodávateľmi, činnosťami pozorovanými CAB, činnosťami opätovne vykonanými CAB a činnosťami prijatými prostredníctvom opakovane použiteľných informácií o záruke.

VII.6 Analýza závislostí a záznam o zložení

Normatívna požiadavka: Správa MUSÍ obsahovať záznam analýzy závislosti požadovaný v prílohe IX pre každý certifikát, správu z auditu, správu o skúškach, výsledok posudzovania zhody, položku záruky dodávateľa alebo iné opätovne použiteľné informácie o záruke, na ktoré sa spolieha.

Normatívna požiadavka: Pre každé rozhodnutie o spoliehaní sa správa MUSÍ zaznamenať zdroj záruky, vydavateľa, základ spôsobilosti, predmet, platnosť, predpoklady, zistenia, relevantnosť pre slovenskú architektúru, zostatkové nedostatky, výsledok spoliehania sa a následnú činnosť.

Normatívna požiadavka: Správa MUSÍ obsahovať záver o zloženom osvedčení, v ktorom sa vysvetľuje, ako moduly, závislosti, predpoklady, kompenzačné opatrenia a zostávajúce činnosti podporujú konečný záver o záruke pre predmet osvedčenia.

Príloha IX Výsledok posúdenia spoľahlivosti	**Ako podávať správy v prílohe VII**	**Dôsledok rozhodnutia**
Prijaté	Pokrytie kritérií dokumentu a splnené predpoklady.	Môže podporiť kladný záver pre kritériá, na ktoré sa vzťahuje.
Prijaté s kompenzačnými opatreniami	Nedostatok v dokumente, kompenzačné opatrenia, dôkazy z testov/auditu a zvyškové riziko.	Kladný záver je možný len v prípade, ak sú opatrenia účinné.
Prijaté s dodatočným skúšaním CAB	Zaznamenať zostávajúce činnosti a výsledky.	Kladný záver je možný len vtedy, ak zostatkové činnosti prejdú.
Zamietnuté	Zdokumentujte dôvod zamietnutia a alternatívny dôkaz alebo vylúčenie z predmetu.	Pozitívny záver nie je možné podporiť, pokiaľ nie je nahradený priamym hodnotením.

VII.7 Nezhody, nápravné opatrenia a zraniteľné miesta

Normatívna požiadavka: Správa MUSÍ obsahovať vyhlásenie, v ktorom sa v prípade potreby uvádza, že v čase rozhodnutia o certifikácii neexistujú žiadne podstatné nezhody.

Normatívna požiadavka: Pre každú zistenú nezhodu MUSÍ správa obsahovať klasifikáciu, dotknutú požiadavku, dotknutú zložku alebo proces, príčinu, ak je známa, plán nápravných opatrení, časový harmonogram, zodpovednú stranu a plánovanú činnosť verifikácie CAB.

Normatívna požiadavka: Pre každú podstatnú nezhodu, ktorá bola odstránená pred rozhodnutím, správa MUSÍ obsahovať dátum dokončenia nápravných opatrení a hodnotiacu činnosť, ktorú CAB použila na overenie účinnosti nápravy.

Normatívna požiadavka: Správa MUSÍ obsahovať zhrnutie analýz vplyvu závažných zraniteľností a rozhodnutí o nápravných opatreniach relevantných pre rozhodnutie o certifikácii, bez zbytočného zverejňovania podrobností o zneužití mimo autorizovaného distribučného reťazca.

VII.8 Preskúmanie, rozhodnutie o certifikácii a dohľad

Normatívna požiadavka: Správa MUSÍ obsahovať zhrnutie preskúmania a certifikačného rozhodnutia, vrátane odôvodnenia vysvetľujúceho, ako služba IKT ako celok spĺňa úroveň záruky vysoká podľa zákona o kybernetickej bezpečnosti a, ak je to relevantné, ako prostriedky eID, komponenty schémy eID alebo služba PID spĺňajú požiadavky na úroveň záruky vysoká podľa eIDAS.

Normatívna požiadavka: Správa MUSÍ pre každú fázu posudzovania zhody uvádzať obdobie, na ktoré sa vzťahuje, a čas, ktorý certifikačný orgán strávil v osobodňoch, vrátane auditu dokumentácie, posudzovania implementácie, inšpekcie na mieste, posudzovania na diaľku, skúšania a preskúmania.

Normatívna požiadavka: Správa MUSÍ uvádzať termín nasledujúceho hodnotenia dohľadu a akékoľvek povinné následné opatrenia, osobitné hodnotenie, zmenu certifikátu alebo požiadavku na plánovanie recertifikácie.

Normatívna požiadavka: Správa MUSÍ obsahovať výslovné vyhlásenie, že certifikačné dokumenty, vrátane tejto správy, sú určené na použitie národným orgánom pre certifikáciu kybernetickej bezpečnosti a inými príslušnými orgánmi, ak to povoľuje zákon a schéma.

Ref.	Blok správy	Minimálny obsah
VII.1	Administratívna identifikácia	Certifikát, služba, držiteľ, žiadateľ, CAB, akreditácia, tím a subdodávatelia.
VII.2	Podrobný predmet	Moduly, profily, toky ONL/PRX, architektúra, vylúčenia a predpoklady.
VII.3	Register dôkazov	Všetky dokumenty, záznamy, testy, certifikáty, audítorské správy a identifikátory dôkazov.
VII.4	Kontrolný rámec	Kritériá prílohy X, uplatniteľnosť, opatrenia, zložky, dôkazy a priradenia.
VII.5	Hodnotiace činnosti	Audit, inšpekcia, skúšanie, analýza závislostí, preskúmanie rizík, odber vzoriek a výsledky.
VII.6	Záznam o zložení	Rozhodnutia o závislostiach, zostávajúce činnosti, kompenzačné opatrenia a súhrnný záver.
VII.7	Zistenia a zraniteľnosti	Nezhody, nápravné opatrenia, podstatné slabé miesta a verifikácia.
VII.8	Rozhodnutie a údržba	Odôvodnenie záruky, rozhodnutie, človekodni, ďalší dohľad a vyhlásenie o používaní oprávnenia.

Slovenská národná certifikačná schéma EUDI Wallet

PRÍLOHA VIII – Požiadavky na orgány posudzovania zhody

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny text – poznámka k vypracovaniu: Príloha VIII EÚ vychádza z kandidátskej schémy EÚ 0.4.614 a je zosúladená s prílohou I SK, prílohou IV SK, prílohou X SK a prílohou XI SK.

VIII.0 Účel, úloha a logika vypracovania

Informatívny text: Táto príloha definuje požiadavky, ktoré musia spĺňať orgány posudzovania zhody, certifikačné orgány, subdodávateľské orgány a technickí experti podieľajúci sa na posudzovaní zhody v rámci schémy EUDIW-SK. Vychádza z európskeho návrhu prílohy VIII ako hlavného základu a rozširuje ho len tam, kde je to potrebné na to, aby bola národná modulárna architektúra, súbor dôkazov, hodnotiace kritériá a hodnotiace metódy funkčné.

Normatívna požiadavka: Táto príloha SA MUSÍ vykladať spolu s prílohou I, prílohou IV, prílohou X a prílohou XI. Príloha I definuje predmet pôsobnosti, moduly, profily a modifikátory prípadov použitia. Príloha IV definuje súbor dôkazov. Príloha X definuje hodnotiace kritériá. Príloha XI definuje metódy a postupy. Príloha VIII definuje požiadavky na spôsobilosť, akreditáciu, autorizáciu, proces a subdodávky, ktoré umožňujú orgánom posudzovania záruky uplatňovať tieto prílohy na vysokej úrovni záruky.

Normatívna požiadavka: Požiadavky v tejto prílohe dopĺňajú, ale nenahrádzajú normy EN ISO/IEC 17065, ETSI EN 319 403-1 a žiadne povinné požiadavky uložené nariadením (EÚ) 2019/881, nariadením (EÚ) č. 910/2014, vykonávacím nariadením Komisie (EÚ) 2024/2981 a príslušnými slovenskými právnymi predpismi.

Normatívna požiadavka: Ak CAB vykonáva len časť hodnotiacich činností alebo sa spolieha na subdodávateľov, technických expertov, laboratóriá alebo predchádzajúce informácie o záruke, CAB vydávajúca certifikát ZOSTÁVA zodpovedná za celkové posudzovanie zhody, rozhodnutie o certifikácii, dostatočnosť dôkazov a konzistentnosť predmetu certifikátu.

Úroveň	Funkcia prílohy VIII	Prepojenie s ostatnými prílohami EUDIW-SK
Akreditácia a autorizácia	Definuje formálnu oprávnenosť CAB a hranice oprávnenia pre úrove§ záruky vysoká.	Na vymedzenie predmetu akreditácie a oprávnenia sa používajú kategórie predmetu z prílohy I a metódy z prílohy XI.
spôsobilosť	Definuje vedomosti, zručnosti a skúsenosti požiadavky na tím CAB a na osoby s rozhodovacou právomocou.	Zahŕňa kritériá prílohy X, metódy prílohy XI, analýzu závislostí a integráciu slovenských právnych predpisov.
Požiadavky na proces	Rozširuje proces auditu podľa normy ETSI EN 319 403-1 o inšpekciu, hodnotenie návrhu, posúdenie rizík, skúšanie a posúdenie zraniteľnosti.	Implementuje postupné hodnotenie životného cyklu podľa prílohy XI a preskúmanie dôkazov podľa prílohy IV.
Subdodávateľstvo a opätovné použitie dôkazov	Definuje, ako je možné využiť externé skúšanie, inšpekciu, audity a opätovne použiteľné záruky bez oslabenia záveru certifikácie.	Podporuje logiku závislostí podľa prílohy IX, dôkazy o záruke podľa prílohy IV a klasifikáciu zostatkových činností podľa prílohy XI.
Podávanie správ a kontinuita	Definuje požiadavky na výstupy CAB, sledovateľnosť, uchovávanie, dôvernosť a ukončenie.	Podporuje logiku prílohy V, prílohy VI, prílohy VII a údržby certifikátov.

VIII.1 Referenčný rámec a úplnosť európskych referencií

Informatívny text: Kandidátska schéma európskeho systému uvádza súbor nariadení, noriem a technických špecifikácií, ktoré tvoria referenčný rámec pre certifikáciu EUDIW. Slovenské prílohy nemusia opakovať každý dokument v každej prílohe, ale CAB musí mať spôsobilosť rozpoznať, kedy je každý odkaz relevantný a ako ovplyvňuje predmet, dôkazy, hodnotiace kritériá, hodnotiace metódy, subdodávky a certifikačné rozhodnutia.

Normatívna požiadavka: CAB MUSÍ viesť register uplatniteľnosti referencií pre každé hodnotenie. Register MUSÍ identifikovať, ktoré právne akty, normy, technické špecifikácie, dokumenty o najnovšom stave techniky a národné požiadavky sa vzťahujú na deklarovaný modul, architektonický profil, modifikátor prípadu použitia ONL/PRX, závislosť a hodnotiacu činnosť.

Normatívna požiadavka: Ak sa referenčný dokument z európskej kandidátskej schémy priamo nepoužíva v certifikovanom predmete, CAB MUSÍ zaznamenať odôvodnenie neplatnosti. Ak sa referenčný dokument používa iba prostredníctvom certifikátu o zložke

Odkaz z návrhu EÚ / súvisiacej základnej normy EÚ	Relevancia CAB v EUDIW-SK	Kde sa používa alebo by sa mala používať v slovenských prílohách
Nariadenie (EÚ) 2019/881 – Zákon o kybernetickej bezpečnosti	Celkový rámec certifikácie kybernetickej bezpečnosti, úroveň záruky vysoký, akreditácia/autorizácia CAB, logika monitorovania a vzájomného hodnotenia.	Základná schéma, príloha VIII, príloha XI, podávanie správ a údržba.
Vykonávacie nariadenie Komisie (EÚ) 2024/482 – EUCC	Opätovne použiteľné záruky pre WSCD, HSM, WSCA alebo iné bezpečnostne kritické komponenty certifikované podľa Spoločných kritérií/EUCC.	Závislosti podľa prílohy I, dôkazy o záruke podľa prílohy IV, kryptografické kritériá podľa prílohy X, analýza závislostí podľa prílohy XI.
Nariadenie (EÚ) č. 910/2014 – eIDAS	Právny predmet certifikácie, peňaženka EUDI, schéma eID, úroveň záruky, rozhranie dohľadu a kontext dôveryhodnej služby.	Predmet pôsobnosti prílohy I, právny balík/balík dôkazov podľa prílohy IV, kritériá PID/validácie podľa prílohy X, spôsobilosť podľa prílohy VIII.
Nariadenie (EÚ) 2024/1183 – Rámec európskej digitálnej identity	Zmena a doplnenie, ktorým sa zriaďuje rámec peňaženky EUDI a kontext certifikácie podľa článku 5a/5c.	Základná schéma a právomoci podľa prílohy VIII; relevantné pre predmet pôsobnosti a tvrdenia v certifikátoch.
Vykonávacie nariadenie Komisie (EÚ) 2024/2981 – Certifikácia peňaženky EUDI	Primárny vykonávací akt pre certifikáciu peňaženky, register rizík, informácie o záruke, hodnotiace činnosti a očakávania CAB.	Balík rizík a dôkazov podľa prílohy IV, kritériá podľa prílohy X, metódy podľa prílohy XI, spôsobilosť podľa prílohy VIII.
Vykonávacie nariadenie Komisie (EÚ) 2024/2979 – integrita a základné funkcie	Funkčná a integritná základná úroveň pre funkčnosť peňaženky.	Príloha X funkčná zhoda, príloha XI funkčné skúšanie, príloha VIII spôsobilosť v oblasti funkčného skúšania.
Vykonávacie nariadenie Komisie (EÚ) 2024/2977 – PID a elektronické osvedčenia atribútov	Funkčná a formátová základná úroveň pre PID a toky osvedčení, ak je to relevantné.	Príloha X – kritériá PID a osvedčovania, príloha XI – funkčné skúšanie, príloha VIII – spôsobilosť v oblasti PID/eID.
Vykonávacie nariadenie Komisie (EÚ) 2024/2982 – protokoly a rozhrania	Základné požiadavky na protokoly a rozhrania pre diaľkové a bezkontaktné toky.	Príloha X interoperabilita, príloha XI skúšanie FCAF/národnej integrácie, príloha VIII spôsobilosť v oblasti protokolov.
Vykonávacie nariadenie Komisie (EÚ) 2025/2162 – akreditácia CAB QTSP	Odkaz na logiku akreditácie a podávanie správ v prípadoch, keď sa opätovne využívajú hodnotenia QTSP alebo výstupy QTSP CAB.	Príloha IV opätovne použiteľná záruka, príloha VIII spôsobilosť v oblasti akreditácie, príloha XI analýza závislostí.
Smernica (EÚ) 2022/2555 – NIS2	Riadenie kybernetickej bezpečnosti, kontext riadenia incidentov a rizík relevantný pre prevádzkovateľov podobných dôveryhodných službám.	Príloha I Systémy/procesy IKT, príloha X Riadenie služieb, príloha VIII Spôsobilosť v oblasti riadenia kybernetickej bezpečnosti.
Vykonávacie nariadenie Komisie (EÚ) 2024/2690 – technické a metodické požiadavky NIS2	Referenčný rámec pre prevádzkovú bezpečnosť, riadenie incidentov a rizík odzrkadlený v norme ETSI EN 319 401 a riadenie služieb.	Príloha I Systémy/procesy IKT, príloha IV Prevádzkové dôkazy, príloha X Kritériá riadenia.
Nariadenie (EÚ) 2024/2847 – Zákon o kybernetickej odolnosti	Relevantné pre softvérové produkty uvádzané na trh a pre zásady týkajúce sa zraniteľnosti/SBOM/aktualizácií používané v rámci schémy.	Príloha IV dôkazy o SBOM/zraniteľnosti, príloha X kritériá inštancií peňaženiek, príloha VIII spôsobilosť v oblasti bezpečného vývoja.
EN ISO/IEC 17065:2012	Základné požiadavky na orgány pre akreditáciu a certifikáciu pre výrobky, procesy a služby.	Príloha VIII akreditácia, nestrannosť, subdodávateľstvo, certifikačné rozhodnutie a sťažnosti/odvolania.
ISO/IEC DIS 17067	Logika certifikačnej schémy a odôvodnenie typu schémy pre komplexné certifikačné systémy.	Základná logika schémy a pochopenie fungovania schémy podľa prílohy VIII.
EN ISO/IEC 17021-1:2015	Referenčné kritériá spôsobilostí pre subdodávateľské služby v oblasti auditu systémov manažérstva alebo opätovné použitie auditov ISMS.	Príloha VIII – Vhodnosť subdodávateľov a spôsobilosť auditu ISMS.
EN ISO/IEC 17025:2017	Spôsobilosť skúšania laboratórie, ak CAB vykonáva alebo zadáva funkčné/bezpečnostné skúšky subdodávateľom.	Príloha VIII – spôsobilosť v oblasti skúšania a zadávanie prác subdodávateľom; Príloha XI – skúšobné metódy.
EN ISO/IEC 17029:2019	Spôsobilosť v oblasti validácie/verifikácie v prípadoch, keď sa využívajú validizačné alebo verifikačné orgány.	Príloha VIII subdodávateľské služby a opätovné použitie záruk.
ISO/IEC 17000:2020	Slovník posudzovania zhody a všeobecné zásady.	Príloha VIII – konzistentnosť terminológie a interpretácia schémy.
ETSI EN 319 401 v3.2.1	Správa podobná službám zameraným na budovanie dôvery, prevádzková bezpečnosť a základné zásady pre služby IKT v rámci EUDIW.	Príloha I Predmet procesu IKT, príloha X kritériá riadenia, príloha VIII technická spôsobilosť.
ETSI EN 319 403-1 v2.3.1	Základný proces CAB/auditu na posudzovanie zhody dôveryhodných služieb.	Príloha VIII základné požiadavky na proces a príloha XI metodika auditu.
ISO/IEC 15408:2022	Hodnotiace kritériá spoločných kritérií pre komponenty kritické z hľadiska bezpečnosti a logiku profilu ochrany.	Závislosti WSCD/WSCA podľa prílohy I, kryptografické kritériá podľa prílohy X, pojmy zraniteľnosti podľa prílohy XI.
ISO/IEC 18045:2022	Metodika hodnotenia podľa spoločných kritérií, vrátane ETR a pojmov hodnotenia zraniteľnosti.	Metódy uvedené v prílohe XI a spôsobilosť uvedená v prílohe VIII na interpretáciu hodnotení komponentov.
CEN TS 18072:2022	Analýza závislostí, hodnotenie služieb/podslužieb a pojmy týkajúce sa prevádzkovej účinnosti.	Analýza závislostí podľa prílohy IX/prílohy XI a procesná spôsobilosť podľa prílohy VIII.
EN 17640:2022 – FiTCEM	Metodika hodnotenia kybernetickej bezpečnosti v pevne stanovenom čase pre produkty IKT, najmä hodnotenie inštancií peňaženiek.	Kritériá inštancií peňaženiek podľa prílohy X, skúšanie inštancií peňaženiek podľa prílohy XI, technická spôsobilosť podľa prílohy VIII.
FCAF	Certifikačný orgán MUSÍ preskúmať dôkazy o funkčnej zhode, vrátane dôkazov vypracovaných v rámci **rámca pre posudzovanie zhody európskej digitálnej peňaženky (FCAF), verzia 0.1**, ak je to relevantné.	Príloha XI – Skúšanie inštancií peňaženiek
Požiadavky na bezpečnosť[2]	Certifikačný orgán preskúma dôkazy o zhode s bezpečnostnými požiadavkami, pokrytie rizík a odôvodnenie	Príloha X – kritériá inštancie peňaženky,
Akékoľvek ďalšie relevantné referencie v súlade s ďalším vývojom a posúdením CAB	CAB by mala v čase certifikácie využiť akékoľvek ďalšie použiteľné zdroje	

[2] ENISA, *Bezpečnostné požiadavky na poskytovateľov služieb súvisiacich s peňaženkami, verzia 0.5.614, marec 2026, na základe normy EN 319 401 alebo najnovšej verzie*.

VIII.2 Akreditácia, autorizácia a predmet povolených činností

VIII.2.1 Účel

Táto časť definuje logiku akreditácie, autorizácie a povolených činností pre orgány zúčastňujúce sa na posudzovaní zhody v rámci slovenskej národnej certifikačnej schémy peňaženiek EUDI (EUDIW-SK).

Účelom tejto časti je zachovať praktický a stabilný predmet akreditácie pri zachovaní vysokého stupňa záruky. Štruktúra modulov definovaná v prílohe I sa používa na organizáciu certifikovaného objektu, plánovanie hodnotenia, mapovanie dôkazov a podávanie správ. Nesmie sa to vykladať tak, že sa vyžaduje samostatný akreditačný proces alebo opakovaný akreditačný proces pre každý modul, profil, modifikátor prípadu použitia alebo technickú variantu.

VIII.2.2 Slovenské právne obmedzenie pre úroveň záruky vysoká

Normatívna požiadavka: Podľa slovenského právneho rámca sa certifikácia EUDIW-SK na úroveň záruky vysoká vykonáva iba v rámci právnych obmedzení platných pre certifikáciu kybernetickej bezpečnosti. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti určuje Národný bezpečnostný úrad (NBÚ) ako národný certifikačný orgán pre kybernetickú bezpečnosť a ako orgán posudzovania zhody v systéme certifikácie kybernetickej bezpečnosti. Ten istý zákon v § 5a ods. 3 stanovuje, že certifikáciu kybernetickej bezpečnosti na úrovniach záruky Základná, Významná alebo Vysoká môže vykonávať iba osoba s akreditáciou a že osobou s akreditáciou pre certifikáciu kybernetickej bezpečnosti na úrovni záruky Vysoká môže byť iba Úrad.

Normatívna požiadavka: Na účely tejto certifikačnej schémy je orgánom vydávajúcim certifikáty pre certifikáciu kybernetickej bezpečnosti EUDIW-SK na stupni záruky „Vysoká“ preto NBÚ konajúci vo svojej zákonne povolené úlohe ako akreditovaná osoba pre certifikáciu kybernetickej bezpečnosti s vysokým stupňom záruky, pokiaľ nedôjde k zmene príslušných slovenských právnych predpisov.

Vysvetlenie: Slovenská národná služba pre akreditáciu (SNAS, v pracovných diskusiách niekedy označovaná ako slovenský akreditačný orgán) zostáva národným orgánom pre akreditáciu. Vyššie uvedené právne vyhlásenie sa vzťahuje na NBÚ ako orgán, ktorý môže byť akreditovanou osobou pre úroveň záruky vysoká podľa zákona č. 69/2018 Z. z.; nemalo by sa vykladať ako prenesenie úlohy rozhodovania o certifikácii na akreditačný orgán.

Kontextový odkaz: Zákon č. 272/2016 Z. z. o dôveryhodných službách stanovuje slovenský národný kontext pre európsku peňaženku digitálnej identity, vrátane podmienok pre poskytovateľa európskej peňaženky a predkladania certifikátu európskej peňaženky orgánu. Logiku akreditácie a autorizácie v tejto časti je preto potrebné vykladať spolu s logikou poskytovateľa peňaženky a dohľadu podľa zákona č. 272/2016 Z. z., najmä § 1 a § 10.

VIII.2.3 Predmet akreditácie a úroveň podrobnosti

Normatívna požiadavka: Predmet akreditácie pre orgán vydávajúci certifikáty sa stanoví na úrovni certifikačnej schémy EUDIW-SK ako celku. Nesmie sa rozdeľovať na samostatné predmety akreditácie pre každý modul, komponent, architektonický profil, modifikátor prípadu použitia, hodnotiacu činnosť alebo variant implementácie uvedený v prílohe I.

Normatívna požiadavka: Predmet akreditácie musí byť dostatočne široký, aby pokrýval certifikáciu slovenského riešenia EUDIW a modulov definovaných v prílohe I, vrátane modulu riešenia EUDIW-SK, modulu služby SK-PID, modulu validácie SK-Validation, zdieľaných auditovateľných procesov a akéhokoľvek zastrešujúceho certifikačného záveru založeného na týchto moduloch.

Normatívna požiadavka: Predmet akreditácie musí tiež umožňovať orgánu vydávajúcemu certifikáty využívať opakovane použiteľné informácie o záruke a externé technické výstupy za predpokladu, že orgán vydávajúci certifikáty zostáva zodpovedný za rozhodnutie o certifikácii a vykonáva analýzu závislostí, prípustnosti a zostatkových činností požadovanú certifikačnou schémou.

Tabuľka VIII.2-1 – Základná položka predmetu akreditácie pre EUDIW-SK

Skupina výrobkov	Položka	Názov produktu	Certifikačná schéma	Zákony, normy
Produkty IKT / Služby IKT	Slovenské riešenie EUDIW	Slovenské národné riešenie európskych digitálnych identifikačných peňaženiek (EUDIW-SK)	Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK	Vykonávacie nariadenie Komisie (EÚ) 2024/2981 z 28. novembra 2024, ktorým sa stanovujú pravidlá na uplatňovanie nariadenia (EÚ) č. 910/2014, pokiaľ ide o certifikáciu európskych digitálnych identitných peňaženiek; nariadenie (EÚ)

				2019/881; zákon č. 69/2018 Z. z.; zákon č. 272/2016 Z. z.

Informatívna poznámka: Znenie v tabuľke predmetu akreditácie je zámerne prispôsobené štruktúre predmetu akreditácie v Slovenskej republike. Dodatočné znenie „služby IKT“ a odkazy na vnútroštátne právne predpisy sú zahrnuté s cieľom vyhnúť sa nejednoznačnosti, pretože európska kandidátska schéma považuje certifikovateľné objekty za služby IKT a pretože obmedzenie na vysokú záruku vyplýva z vnútroštátnych právnych predpisov v oblasti kybernetickej bezpečnosti.

VIII.2.4 Vzťah medzi akreditáciou, autorizáciou a povolenými činnosťami

Normatívna požiadavka: Akreditácia potvrdzuje spôsobilosť a zhodu orgánu vydávajúceho certifikáty vykonávať certifikáciu v rámci schémy EUDIW-SK v rámci definovaného predmetu akreditácie. Autorizácia potvrdzuje, ak je to relevantné, že orgán môže vykonávať činnosti posudzovania zhody EUDIW na stupni záruky „Vysoká“ pod riadením vnútroštátneho certifikačného orgánu pre kybernetickú bezpečnosť.

Normatívna požiadavka: Povolené činnosti v rámci akreditovaného a autorizovaného predmetu EUDIW-SK musia zahŕňať, podľa toho, čo sa vzťahuje na certifikovaný modul alebo zložený objekt:

- potvrdenie predmetu certifikácie, hraníc modulu, predpokladov a závislostí;
- preskúmanie súboru dôkazov žiadateľa a plánu hodnotenia;
- hodnotenie návrhu a preskúmanie ošetrenia rizika špecifického pre danú architektúru;
- analýzu závislostí a prijateľnosti z hľadiska záruky opakovane použiteľných informácií o záruke;
- určenie zostávajúcich hodnotiacich činností potrebných pre modul alebo zložené riešenie;
- preskúmanie alebo vykonanie audítorských, inšpekčných a skúšobných činností požadovaných v prílohe XI;
- preskúmanie dôkazov o posúdení zraniteľnosti a penetračnom skúšaní, vrátane zostatkových zistení;
- preskúmanie dôkazov o funkčnej zhode, vrátane výstupov z FCAF alebo národných integračných testov, ak je to relevantné;
- preskúmanie výsledkov hodnotenia a rozhodnutia o certifikácii;
- činnosti v oblasti dohľadu, údržby, pozastavenia, odňatia a aktualizácie certifikátu.

Normatívna požiadavka: Orgán vydávajúci certifikáty nemusí vykonávať všetky technické činnosti vlastnými zamestnancami. Môže využívať kompetentné interné alebo externé zdroje, akreditované laboratóriá, odborných subdodávateľov, predchádzajúce certifikáty a opätovne použiteľné informácie o záruke, za predpokladu, že orgán vydávajúci certifikáty si ponechá zodpovednosť za certifikačné rozhodnutie a zdokumentuje vhodnosť a obmedzenia všetkých takýchto vstupov.

VIII.2.5 Modulárne hodnotenia a posudzovanie svedkov

Normatívna požiadavka: Modulárna štruktúra EUDIW-SK sa použije na plánovanie certifikácie a podávanie správ, nie na zbytočnú fragmentáciu akreditácie. Certifikácia jedného modulu alebo prvý skutočný alebo pilotný certifikačný prípad pozorovaný akreditačným orgánom postačí na preukázanie praktického uplatňovania schémy, ak prípad s prítomnosťou svedka pokrýva základnú logiku schémy.

Normatívna požiadavka: Reprezentatívne prvé hodnotenie za prítomnosti svedka by malo zahŕňať minimálne:

- definíciu a potvrdenie predmetu podľa prílohy I;
- posúdenie súboru dôkazov žiadateľa podľa prílohy IV;
- preskúmanie rizík a priradenie opatrení k rizikám a komponentom;
- analýzu závislostí a klasifikáciu prijateľnosti opakovane použiteľných informácií o záruke;
- plánovanie hodnotenia podľa prílohy XI;
- preskúmanie výsledkov, nezhôd a zostávajúcich činností;
- preskúmanie certifikácie a logika rozhodovania;
- príprava výstupov v podobe certifikátu, certifikačnej správy a správy o posúdení certifikácie.

Normatívna požiadavka: Po úspešnej akreditácii na základe prvého modulu alebo certifikačného prípadu, pri ktorom bol prítomný svedok, sa certifikácia ďalších modulov podľa prílohy I spravidla vykonáva v rámci toho istého akreditovaného predmetu EUDIW-SK prostredníctvom dohľadu, preskúmania spôsobilosti, preskúmania technickej dokumentácie alebo cieleného svedectva, a nie prostredníctvom opakovanej akreditácie pre každý modul.

Normatívna požiadavka: Nový proces úplnej akreditácie sa nevyžaduje len preto, že nasledujúce hodnotenie sa týka iného modulu prílohy I, architektonického profilu, modifikátora prípadu použitia ONL/PRX, varianty implementácie, poskytovateľa technológie, závislosti komponentov alebo scenára opätovného použitia dôkazov, za predpokladu, že činnosť zostáva v rámci schémy EUDIW-SK a orgán vydávajúci certifikát má zdokumentovaný prístup k požadovanej spôsobilosti.

VIII.2.6 Využívanie externých expertov, laboratórií a opätovne použiteľnej záruky

Normatívna požiadavka: Orgán vydávajúci certifikáty sa môže spoliehať na externých odborníkov, laboratóriá, technické skúšanie vykonávané subdodávateľmi, certifikáty vydané v rámci iných schém, správy o posudzovaní zhody a iné informácie o záruke, ak takéto využitie povoľuje schéma a príslušné opatrenia pre akreditáciu a autorizáciu.

Na základe analýzy závislosti a posúdenia vhodnosti možno použiť nasledujúce vstupy:

- EUCC, Spoločné kritériá, FIPS alebo rovnocenné dôkazy pre komponenty kritické z hľadiska bezpečnosti, ako sú WSCD, HSM alebo príslušné kryptografické komponenty;
- správy o posudzovaní zhody kvalifikovaných dôveryhodných služieb a dôkazy o štatúte QTSP;
- ISO/IEC 27001, ETSI EN 319 401 alebo iné akreditované dôkazy o systéme manažérstva alebo záruke služieb;
- dôkazy o funkčnej zhode, vrátane FCAF, vyhlásení o zhode implementácie, národných integračných testov alebo iných uznávaných výstupov z testov;
- správy o penetračnom skúšaní, posúdení zraniteľnosti, revízii kódu a testovaní mobilnej bezpečnosti;
- odborné správy, preskúmania architektúry a technické stanoviská, pri ktorých sa riadi spôsobilosť, nestrannosť a dôvernosť.

Normatívna požiadavka: Opätovné použitie externých výsledkov nesmie byť automatické. Orgán vydávajúci certifikát určí, či je každý vstup prijatý bez zvyškovej činnosti, prijatý s kompenzačnými opatreniami, prijatý so zvyškovou činnosťou CAB alebo zamietnutý. Rozhodnutie a odôvodnenie sa zaznamenajú do hodnotiacej dokumentácie a správy o certifikačnom posúdení.

VIII.2.7 Činnosti povolené po prvom hodnotení za prítomnosti svedka

Normatívna požiadavka: Akonáhle bol prvý prípad certifikácie EUDIW-SK alebo modul posúdený pod dohľadom akreditačného orgánu a akreditácia bola udelená alebo potvrdená, orgán vydávajúci certifikáty môže vykonávať certifikačné činnosti pre ďalšie moduly EUDIW-SK v rámci rovnakého predmetu akreditácie, za predpokladu, že:

- činnosť zostane v rámci certifikačnej schémy EUDIW-SK;
- modul je jedným z modulov definovaných v prílohe I alebo zdokumentovaným vývojom týchto modulov;
- uplatňujú sa rovnaké základné logické postupy a metódy hodnotenia uvedené v prílohe XI;
- orgán vydávajúci certifikáty má zdokumentovaný prístup k potrebnej spôsobilosti pre daný modul;
- akákoľvek nová technická činnosť je pokrytá existujúcou spôsobilosťou alebo sa vykonáva prostredníctvom kompetentných externých zdrojov;
- orgán vydávajúci certifikát zostáva zodpovedný za rozhodnutie o certifikácii;
- je dodržané zákonné obmedzenie pre úroveň záruky vysoká podľa zákona č. 69/2018 Z. z.

Hodnotiaca činnosť CAB: Počas dohľadu môže akreditačný orgán preskúmať dodatočné hodnotenia modulov, certifikačné spisy, záznamy o spôsobilostiach, opatrenia na riadenie externých zdrojov a rozhodnutia o analýze závislostí. Takýto dohľad sa nesmie interpretovať ako požiadavka na opakovanie akreditácie pre každý dodatočný modul.

VIII.2.8 Kedy je potrebné dodatočné posúdenie alebo aktualizácia akreditácie

Normatívna požiadavka: Aktualizácia predmetu akreditácie, dodatočné hodnotenie svedka alebo dodatočné preskúmanie technickej spôsobilosti sa zvážia v prípade, ak je nová činnosť podstatne mimo predtým posudzovaného predmetu EUDIW-SK alebo profilu spôsobilosti.

Takéto dodatočné posúdenie by sa malo zvážiť najmä v prípadoch, keď:

- orgán vydávajúci certifikáty má v úmysle certifikovať objekt mimo schémy EUDIW-SK;
- schéma je zmenená a doplnená spôsobom, ktorý podstatne mení certifikačný proces, metódy hodnotenia alebo kritériá rozhodovania o certifikácii;
- orgán vydávajúci certifikáty má v úmysle priamo vykonávať technickú činnosť, ktorá bola predtým outsourcovaná alebo akceptovaná ako opätovne použiteľná informácia o záruke;
- činnosť vyžaduje spôsobilosť v oblasti skúšania podľa normy ISO/IEC 17025 alebo rovnocennú laboratórnu spôsobilosť, ktorá nebola predtým zahrnutá v modeli akreditácie alebo subdodávateľského modelu;
- nová architektúra zavádza podstatne odlišnú technológiu alebo model rizika, ktorý vyžaduje spôsobilosť, ktorá nebola predtým preukázaná;
- príslušný európsky alebo slovenský právny rámec mení úlohu orgánu vydávajúceho certifikáty alebo podmienky certifikácie s vysokou úrovňou záruky;
- dohľad zistí systematické nesprávne uplatňovanie schémy EUDIW-SK, analýzu závislostí, plánovanie hodnotenia alebo logiku rozhodovania o certifikácii.

Normatívna požiadavka: Zmena modulu, architektonického profilu, verzie implementácie, dodávateľa komponentov, technickej závislosti alebo modifikátora prípadu použitia sama o sebe nevyžaduje nový proces akreditácie, ak táto zmena zostáva v rámci schémy EUDIW-SK a je riadne riadená prostredníctvom opatrení na riadenie spôsobilostí, plánovania hodnotenia, analýzy závislostí, dohľadu a postupov údržby certifikátov.

VIII.3 Nezávislosť, nestrannosť, dôvernosť a ochrana informácií

Normatívna požiadavka: Certifikačný orgán, jeho zamestnanci, osoby s rozhodovacou právomocou, subdodávatelia a technickí experti MUSIA byť nezávislí od žiadateľa, poskytovateľa peňaženky, poskytovateľa PID, poskytovateľa služieb validácie, subdodávateľa alebo poskytovateľa komponentov, ktorých dôkazy alebo implementáciu posudzujú.

Normatívna požiadavka: CAB NESMIE poskytovať poradenské, projektové, vývojové, implementačné, prevádzkové, údržbárske ani nápravné služby pre certifikovanú službu IKT, ak by takéto služby ohrozili nestrannosť alebo vytvorili hrozbu vlastného posudzovania.

Normatívna požiadavka: CAB MUSÍ zaviesť postupy na identifikáciu, dokumentáciu, preskúmanie a zmiernenie konfliktov záujmov pred prijatím hodnotenia a počas celého životného cyklu certifikácie.

Normatívna požiadavka: CAB MUSÍ chrániť dôverné informácie, obchodné tajomstvá, zdrojový kód, kryptografické informácie, informácie o zraniteľnosti, osobné údaje, bezpečnostnú architektúru, audítorské dôkazy a iné citlivé informácie pomocou technických a organizačných opatrení primeraných stupňu záruky vysoká.

Normatívna požiadavka: Ak CAB pristupuje k zdrojovému kódu, kryptografickej konfigurácii, podrobnostiam o zneužití zraniteľností alebo produkčným protokolom, CAB MUSÍ pred sprístupnením informácií definovať pravidlá bezpečného prístupu, ukladania, prenosu, riadenia prístupov hodnotiteľov, uchovávania a likvidácie.

Normatívna požiadavka: CAB MUSÍ zabezpečiť, aby subdodávatelia a externí experti boli viazaní povinnosťami týkajúcimi sa dôvernosti, nezávislosti a ochrany informácií, ktoré sú rovnocenné s povinnosťami uloženými CAB.

VIII.4 Požiadavky na spôsobilosť personálu CAB

Informatívny text: Európsky návrh prílohy VIII vyžaduje, aby personál určujúci zhodu technických komponentov mal formálnu kvalifikáciu alebo odborné trénovanie alebo rozsiahle skúsenosti, najmenej štyri roky praktických skúseností na pracovisku súvisiacich s vývojom softvéru a najmenej dva roky v oblasti identifikačných služieb alebo iných citlivých služieb. Národná príloha zachováva toto ako minimum a dopĺňa spôsobilosť v oblasti modulov potrebnú pre slovenskú národnú architektúru a zákonnú integráciu.

Normatívna požiadavka: Zamestnanci zodpovední za posudzovanie zhody technických komponentov, softvérových komponentov, peňaženkových služieb, služieb PID, validácie alebo integračných mechanizmov MUSIA spĺňať nasledujúce minimálne požiadavky: formálnu akademickú kvalifikáciu, odborné trénovanie alebo rozsiahle skúsenosti preukazujúce schopnosť posudzovať vlastnosti softvéru a služieb prostredníctvom preskúmania návrhu a implementácie; a najmenej štyri roky praxe na plný úväzok v oblasti vývoja softvéru, bezpečnostného inžinierstva, hodnotenia bezpečnosti, identifikačných služieb, dôveryhodných služieb, posudzovania zhody alebo inej relevantnej oblasti, z ktorých sa najmenej dva roky týkajú identifikačných služieb, dôveryhodných služieb, služieb IKT citlivých z hľadiska kybernetickej bezpečnosti alebo digitálnych služieb s vysokou zárukou zabezpečenia.

Normatívna požiadavka: CAB MUSÍ viesť maticu spôsobilostí pre hodnotiaci tím. Matica MUSÍ priradiť každý modul prílohy I, architektonický profil, modifikátor prípadu použitia, skupinu kritérií prílohy X a metódu prílohy XI k menovaným zamestnancom, subdodávateľom alebo technickým expertom s dokumentovanou spôsobilosťou.

Normatívna požiadavka: CAB MUSÍ zabezpečiť, aby osoby s rozhodovacou právomocou v oblasti certifikácie mali spôsobilosť na úrovni záruky „vysoká“, chápali obmedzenia opakovateľnej záruky a boli nezávislé od hodnotiacich činností v rozsahu požadovanom normou EN ISO/IEC 17065.

Oblasť spôsobilostí	Požiadavky na vedomosti a zručnosti	Používa sa na
Právny rámec a rámec schému	eIDAS, nariadenie (EÚ) 2024/1183, CIR (EÚ) 2024/2981, CSA, platné slovenské právo, slovenský zákon č. 272/2016 Z. z., ak je to relevantné, dôkazy podľa slovenského zákona o kybernetickej bezpečnosti, ak sa opätovne používajú.	Rozhodnutia o predmete pôsobnosti, oprávnenosť certifikátu, posúdenie zákonnej integrácie a posúdenie právnej úlohy.
Architektúra a moduly EUDIW	Riešenie EUDIW-SK, služba SK-PID, služba SK-Validácia, zastrešujúca certifikácia, závislosti a externé predpoklady.	Verifikácia hraníc modulov, kompozitné hodnotenie a konsolidácia CAR.
WSCD/WSCA a kryptografia	Vzdialený HSM/cloudový HSM, externé čipové karty, bezpečnostné prvky, natívna bezpečnosť platformy, integrácia WSCA/WSCD, výhradné opatrenie, PKI, životný cyklus kľúčov, podpisy a pečate.	Kryptografické kritériá prílohy X a metódy zraniteľnosti/závislosti prílohy XI.
Spoločné kritériá a záruka produktov	EUCC, ISO/IEC 15408, ISO/IEC 18045, bezpečnostné ciele, ETR, usmernenia, koncepcie AVA_VAN, profily ochrany, dôkazy FIPS, ak sú navrhnuté.	Hodnotenie záruky komponentov a rozhodnutia o zvyškových aktivitách.
Inštancia peňaženky a bezpečnosť mobilných zariadení/aplikácií	Bezpečnosť mobilných aplikácií, varianty pre web/desktop, ak je to relevantné, OWASP MASVS/ASVS, bezpečné ukladanie, lokálna autentifikácia, ochrana proti neoprávneným zásahom, integrita aktualizácií, SAST/DAST a penetračné testovanie.	Hodnotenie inštancie peňaženky, odber vzoriek a posúdenie zraniteľnosti.
PID, registrácia a overovanie identity	CIR 2015/1502 úroveň záruky vysoká, overovanie identity, správa prostriedkov eID, viazanie PID, autoritatívne zdroje, osvedčenie jednotky peňaženky a záznamy o životnom cykle.	Hodnotenie služby SK-PID a schému eID.
Validácia a služby spoliehajúcej sa strany	Validácia dôveryhodnej strany, kotvy dôvery, validačné API, dostupnosť, kontrola certifikátov/stavu, pozastavenie/zrušenie registrácie a národné validačné mechanizmy.	Hodnotenie služby SK-Validácia a integrácia do slovenského právneho poriadku.
Prevádzková bezpečnosť a ISMS	Dôkazy podľa noriem ETSI EN 319 401, ISO/IEC 27001, koncepcie NIS2/CIR 2024/2690, riadenie dodávateľov, procesy týkajúce sa incidentov, zraniteľnosti, zmien, kontinuity a podvodov.	Audit a hodnotenie prevádzkovej účinnosti.
Funkčná zhoda a interoperabilita	FCAF, funkcie odvodené z ARF, OpenID4VP, ISO/IEC 18013-5, SD-JWT VC, mdoc, súbor testov slovenskej národnej integrácie, toky ONL/PRX.	Skúšanie funkčnej zhody a národné integračné testy.
Analýza závislostí a opätovné použitie dôkazov	CEN TS 18072, certifikáty komponentov, správy QTSP, výsledky FCAF, certifikáty ISO/IEC, slovenské audity kybernetickej bezpečnosti, mostové listy a správy o dohľade.	Prijatie, kompenzačné opatrenia, zvyškové skúšanie CAB alebo rozhodnutia o zamietnutí.
Hodnotenie rizík a riadenie zraniteľností	Register rizík Únie, posúdenie rizík špecifických pre implementáciu, potenciál útoku, význam zraniteľnosti, CVD, SBOM, bezpečná aktualizácia a náprava.	Riziková výzva, preskúmanie vplyvu zraniteľností a údržba.
Postup posudzovania zhody	EN ISO/IEC 17065, ETSI EN 319 403-1, audítorské pohovory, odber vzoriek dôkazov, inšpekcia, vypracovanie správ, klasifikácia nezhôd a preskúmanie certifikácie.	Vykonávanie hodnotenia, dokumentácia a podpora pri rozhodovaní o certifikácii.

VIII.5 Spôsobilosťy špecifické pre danú úlohu a zloženie tímu

Normatívna požiadavka: Certifikačný orgán MUSÍ vymenovať hodnotiaci tím, ktorého zloženie zodpovedá predmetu certifikácie. Jedna osoba MÔŽE zastávať viacero úloh len vtedy, ak to umožňujú jej spôsobilosť, nestrannosť a pracovné zaťaženie a ak táto kombinácia úloh nespôsobuje konflikt so nezávislosťou pri posudzovaní alebo pri rozhodovaní o certifikácii.

Normatívna požiadavka: Pri každom hodnotení MUSÍ CAB zdokumentovať zloženie tímu, rozdelenie úloh, dôkazy o spôsobilosti, subdodávateľské činnosti a zodpovednosti za posudzovanie pred začatím hlavného hodnotenia.

Úloha	Požiadavka na zameranie spôsobilostí	Osobitná nezávislosť alebo očakávania týkajúce sa výstupov
Osoba s rozhodovacou právomocou v oblasti certifikácie	Spôsobilosť rozhodovať podľa normy EN ISO/IEC 17065, úroveň záruky vysoká, interpretácia schémy, posudzovanie nezhody a zvyškového rizika.	Nemôže sa spoliehať výlučne na závery hodnotiteľa bez nezávislého preskúmania dostatočnosti a predmetu.
Hlavný hodnotiteľ / hlavný audítor	ETSI EN 319 403-1, proces EN ISO/IEC 17065, plánovanie dôkazov podľa prílohy IV, postupné hodnotenie podľa prílohy XI.	Koordinuje hodnotenie v prvej a druhej fáze a zabezpečuje sledovateľnosť.
Technický inšpektor / hodnotiteľ návrhu	Preskúmanie architektúry, návrh komponentov, bezpečný vývoj, implementácia peňaženky a backendu, mapovanie profilov.	Vykonáva inšpekčné činnosti nad rámec bežného auditu.
Špecialista na analýzu závislostí	CEN TS 18072, dôkazy EUCC/CC, dôkazy QTSP, správy ISMS, prepojovacie listy, zostávajúce činnosti.	Klasifikuje opakovateľné záruky a identifikuje nedostatky.
Odborník na kryptografiu / WSCD / WSCA	HSM/WSCD, WSCA, životný cyklus kľúčov, argumenty týkajúce sa výhradnej kontroly, kryptografické mechanizmy a najnovšie usmernenia.	Hodnotí kryptografickú infraštruktúru a predpoklady špecifické pre daný profil.
Špecialista na bezpečnosť peňaženiek	Bezpečnosť mobilných/webových aplikácií, SAST/DAST, OWASP, bezpečné ukladanie, ochrana proti neoprávneným zásahom, bezpečnosť aktualizácií a kontrola zdrojového kódu.	Podporuje posúdenie zraniteľnosti inštancií peňaženiek.
Tester funkčnej zhody / protokolov	FCAF, národné testovacie sady, OpenID4VP, ISO/IEC 18013-5, SD-JWT VC, mdoc a toky protokolov ONL/PRX.	Vykonáva alebo dohliada na funkčné a interoperabilné skúšanie.
Špecialista na PID/eID a validáciu	úroveň záruky vysoká, overovanie identity, vydávanie PID, validačné mechanizmy, registrácia dôveryhodných strán a integrácia so Slovenskom.	Posudzuje kritériá PID a služieb validácie.
Vedúci posudzovania zraniteľnosti / penetračných testov	Potenciál útoku, penetračné skúšanie, význam zraniteľností, validácia nápravných opatrení, obmedzenia zneužitia a podávanie správ.	Vykonáva alebo dohliada na posúdenie zraniteľnosti.
Recenzent / prevádzkovateľ kvality správ	Požiadavky schémy, úplnosť správy, dostatočnosť dôkazov, konzistentnosť nezhôd a kontrola dôvernosti.	Preskúma vstupy ETR/CAR/CR a konečnú konzistentnosť.

VIII.6 Dodatočné požiadavky na proces hodnotenia EUDIW

Normatívna požiadavka: CAB MUSÍ vykonávať postupy vybavovania sťažností a odvolaní v súlade s hlavnou časťou schémy. Sťažnosti alebo odvolania, ktoré môžu ovplyvniť spôsobilosť CAB, nestrannosť, platnosť certifikátu, pozastavenie, odňatie alebo verejné informácie, MUSIA byť eskalované na NBÚ / vlastníka schémy v súlade s postupmi schémy.

Informatívny popis: Európsky návrh vyžaduje, aby bol proces auditu podľa normy ETSI EN 319 403-1 doplnený o inšpekciu, hodnotenie návrhu, preskúmanie posúdenia rizík, funkčné skúšanie, posúdenie zraniteľnosti a penetračné skúšanie. Slovenská verzia zosúlaďuje tieto procesné požiadavky s prílohou XI.

Normatívna požiadavka: CAB MUSÍ uplatňovať proces hodnotenia v niekoľkých fázach, pozostávajúci z prípravy, prijateľnosti a plánovania v prvej fáze, hlavného hodnotenia, preskúmania a rozhodnutia o certifikácii v druhej fáze a činností údržby alebo dohľadu.

Normatívna požiadavka: V prvej fáze MUSÍ CAB preskúmať súbor dôkazov podľa prílohy IV, potvrdiť úplnosť predmetu v súlade s prílohou I, preskúmať tvrdenie o návrhu, spochybniť posúdenie rizík, posúdiť model závislostí, identifikovať chýbajúce dôkazy, predbežne klasifikovať opätovne použiteľné informácie o záruke a definovať plán hodnotenia pre druhú fázu.

Normatívna požiadavka: Výstup prvej fázy MUSÍ obsahovať plán hodnotenia, v ktorom sú identifikované činnosti auditu, inšpekcie, skúšanie, odber vzoriek, analýza závislostí, preskúmanie rizík, posúdenie zraniteľnosti, skúšanie funkčnej zhody a podávanie správ pre každý modul, profil, modifikátor prípadu použitia a závislosť v predmete pôsobnosti.

Normatívna požiadavka: Počas druhej fázy MUSÍ CAB potvrdiť správnosť popisov, vhodnosť návrhu a opatrenia na riadenie, prevádzkovú účinnosť procesov, primeranosť opätovne použiteľnej záruky, výsledky testov funkčnej zhody, dostatočnosť posúdenia zraniteľnosti a implementáciu požadovaných slovenských zákonných a národných integračných schopností.

Normatívna požiadavka: Ak certifikovaný predmet zahŕňa implementáciu alebo prevádzku služieb peňaženky na IT infraštruktúre poskytovateľa, CAB MUSÍ posudzovanie návrhu a implementácie považovať za inšpekciu, pri ktorej je na určenie zhody potrebný odborný úsudok a technické hodnotenie.

Normatívna požiadavka: CAB NESMIE používať prístup založený výlučne na audite, ak príloha X alebo príloha XI vyžaduje inšpekciu, technické skúšanie, preskúmanie zdrojového kódu, posúdenie zraniteľnosti, penetračné testovanie, skúšanie funkčnej zhody alebo verifikáciu mechanizmov vynútiteľnosti počas behu.

Normatívna požiadavka: Ak skúšanie zhody vykonáva priamo CAB, CAB MUSÍ mať primeranú spôsobilosť v oblasti skúšania a, ak je to relevantné, akreditáciu alebo opatrenia na riadenie subdodávok v súlade s normou EN ISO/IEC 17025. Ak skúšanie zhody vykonáva iný orgán, CAB MUSÍ na výslednú správu o skúšaní, certifikát alebo vyhlásenie o zhode uplatniť analýzu závislosti.

Normatívna požiadavka: CAB MUSÍ odôvodniť akýkoľvek výber vzoriek použitý počas auditu, inšpekcie alebo skúšania. Výber vzoriek SA NESMIE použiť na vyhnutie sa hodnoteniu podstatne odlišných architektúr, kryptografických smerovacích ciest, variantov inštancií peňaženiek, mechanizmov autentifikácie, hraníc dôveryhodnosti alebo národných integračných tokov.

Fáza	Minimálna činnosť CAB	Požadovaný výstup
Prípravné rozhranie	Vyjasniť balík dôkazov, dôvernosť, model prístupu, prístup k testovaciemu prostrediu a očakávané použitie opakovateľnej záruky.	Vyhlásenie o pripravenosti na hodnotenie alebo zoznam požiadaviek na dôkazy.
Prvá fáza – prijateľnosť a plánovanie	Skontrolujte predmet, architektúru, tvrdenie o návrhu, posúdenie rizík, model závislostí, tvrdenie o zhode a navrhovaný plán hodnotenia.	Schválený plán hodnotenia, zoznam zostávajúcich dôkazov a predbežný plán analýzy závislostí.
Druhá fáza – hlavné hodnotenie	Vykonávať audity, inšpekcie, skúšanie, analýzu závislostí, posudzovanie prevádzkovej účinnosti, funkčné skúšanie a posúdenie zraniteľnosti.	Zistenia, nezhody, výsledky testov, závery o dostatočnosti dôkazov a rozhodnutia o zvyškovom riziku.
Preskúmanie a rozhodnutie	Nezávislé preskúmanie výsledkov hodnotenia, predmetu, nezhôd, dostatočnosti dôkazov a tvrdení v certifikáte.	Rozhodnutie o certifikácii, certifikát, certifikačná správa, CAR a vstupy do zloženia, ak je to relevantné.
Údržba a dohľad	Preskúmanie zmien, vplyvu zraniteľnosti, prostredia hrozieb, prevádzky procesov a platnosti záruky opätovného použitia.	Potvrdenie, zmena, osobitné hodnotenie, pozastavenie, zrušenie alebo odporúčanie na recertifikáciu.

VIII.7 Subdodávateľské služby a využívanie výsledkov externého hodnotenia

Normatívna požiadavka: CAB MÔŽE subdodávať hodnotiace činnosti alebo využívať externých technických expertov, ak táto činnosť spadá do rámca akreditácie a autorizačného modelu CAB a ak subdodávanie povoľujú príslušné požiadavky schémy, akreditácie a právne predpisy.

Normatívna požiadavka: CAB MUSÍ niesť plnú zodpovednosť za subdodávateľské činnosti, závery hodnotenia, dostatočnosť dôkazov, preskúmanie certifikácie a rozhodnutie o certifikácii.

Normatívna požiadavka: Predtým, ako sa CAB spolieha na subdodávateľské činnosti, MUSÍ overiť spôsobilosť, nestrannosť, opatrenia na ochranu dôvernosti a vhodnosť subdodávateľa pre konkrétnu činnosť. Verifikácia MUSÍ byť zdokumentovaná.

Normatívna požiadavka: Ak subdodávatelia vykonávajú skúšobné, inšpekčné, audítorské alebo validačné/verifikačné činnosti, CAB MUSÍ posúdiť ich vhodnosť vo vzťahu k príslušnej norme posudzovania zhody, ak je to relevantné: EN ISO/IEC 17025 pre skúšanie, EN ISO/IEC 17020 pre inšpekciu, EN ISO/IEC 17021-1 pre audit systému manažérstva a EN ISO/IEC 17029 pre validáciu alebo verifikáciu.

Normatívna požiadavka: CAB MUSÍ na požiadanie alebo ak to vyžaduje schéma informovať žiadateľa a príslušný orgán schémy o tom, ktoré hodnotiace činnosti sú zadávané subdodávateľom, ktorý subdodávateľ ich vykonáva a aká spôsobilosť alebo akreditácia podporuje ich použitie.

Normatívna požiadavka: Subdodávateľská správa NESMIE byť prijatá mechanicky. CAB MUSÍ posúdiť, či predmet správy, testovaná verzia, prostredie, predpoklady, metódy, zistenia, nevyriešené otázky a obmedzenia sú vhodné pre slovenský certifikovaný predmet.

Normatívna požiadavka: Subdodávateľské služby NESMÚ byť využívané na obídenie požiadavky na spôsobilosť CAB porozumieť hodnoteným technológiám, interpretovať subdodávateľské výsledky, identifikovať zostatkové nedostatky a prijať obhajiteľné certifikačné rozhodnutie.

VIII.8 Výstupy CAB, podávanie správ a sledovateľnosť

Normatívna požiadavka: CAB MUSÍ zachovať sledovateľnosť od každého prvku predmetu v prílohe I k dôkazom v prílohe IV, kritériám v prílohe X, metódam v prílohe XI, hodnotiacej činnosti, zisteniam, nezhodám, zvyškovému riziku a záveru certifikácie.

Normatívna požiadavka: CAB MUSÍ pre každú hodnotiacu činnosť zdokumentovať jej povahu, načasovanie, rozsah, odôvodnenie výberu vzoriek, relevantnosť vo vzťahu k požiadavkám a opatreniam, súhrnný popis, výsledok a akékoľvek odôvodnenie potrebné na podporu certifikačného rozhodnutia.

Normatívna požiadavka: CAB MUSÍ zabezpečiť, aby certifikát, certifikačná správa a správa o certifikačnom posúdení konzistentne uvádzali certifikovaný modul, architektonický profil, modifikátory prípadov použitia ONL/PRX, verziu, závislosti, predpoklady, vylúčené funkcie, zostatkové činnosti, termín dohľadu a obmedzenia použitia.

Normatívna požiadavka: Ak sa CAB spolieha na opakovane použiteľné informácie o záruke, správa MUSÍ uvádzať klasifikáciu prípustnosti, predmet spoliehania sa, zostávajúce činnosti CAB, kompenzačné opatrenia a akékoľvek obmedzenia prenesené do certifikátu alebo certifikačnej správy.

Normatívna požiadavka: CAB MUSÍ zaznamenať výslovný záver o tom, či certifikovaná služba IKT ako celok spĺňa úroveň záruky vysoká pre deklarovaný predmet. Záver NESMIE presiahnuť úroveň záruky podložený vyhodnotenými dôkazmi a závislosťami.

Normatívna požiadavka: Ak sa zistia podstatné nezhody, CAB NESMIE odporučiť vydanie certifikátu, kým sa neoveria nápravné opatrenia, pokiaľ schéma výslovne neumožňuje kontrolované certifikačné rozhodnutie s dokumentovanými obmedzeniami, plánom nápravných opatrení a schválením orgánom. V prípade počiatočnej certifikácie NESMÚ nevyriešené nezhody týkajúce sa existencie alebo vhodnosti požadovaných opatrení brániť vydaniu certifikátu.

VIII.9 Uchovávanie, ochrana, ukončenie a prenos záznamov CAB

Normatívna požiadavka: Držiteľ certifikátu MUSÍ uchovávať vzorky hardvérových komponentov, ktoré boli zahrnuté do predmetu certifikácie, najmenej päť rokov po uplynutí platnosti, stiahnutí alebo zrušení príslušného certifikátu a MUSÍ ich na požiadanie sprístupniť CAB, NBÚ alebo príslušnému orgánu v súlade s článkom 19 ods. 2 písm. b) vykonávacieho nariadenia Komisie (EÚ) 2024/2981.

Normatívna požiadavka: CAB MUSÍ viesť bezpečný systém záznamov obsahujúci všetky dokumenty vyhotovené v súvislosti s každým hodnotením a certifikáciou, ktoré vykonáva, vrátane plánov hodnotenia, registrov dôkazov, korešpondencie, ktorá tvorí súčasť záznamu o hodnotení, výsledkov skúšok, poznámok z inšpekcie, záverov analýzy závislostí, záznamov o nezhodách, záznamov o preskúmaní a záznamov o rozhodnutiach o certifikácii.

Normatívna požiadavka: CAB MUSÍ uchovávať záznamy aspoň po dobu požadovanú schémou a v každom prípade aspoň päť rokov po uplynutí platnosti, odňatí alebo nahradení príslušného certifikátu EUDIW-SK, pokiaľ príslušné právne predpisy alebo certifikačný reťazec nevyžadujú dlhšiu dobu.

Normatívna požiadavka: Ak nový certifikát nahrádza predchádzajúci certifikát, CAB MUSÍ uchovávať dokumentáciu k predchádzajúcemu certifikátu spolu s dokumentáciou k novému certifikátu a po dobu jej uchovávania, a následne počas požadovanej doby uchovávania po uplynutí platnosti.

Normatívna požiadavka: Ak certifikačná autorita ukončí činnosti súvisiace so systémom EUDIW-SK, MUSÍ bez zbytočného odkladu informovať príslušný slovenský orgán, vypracovať plán ukončenia a prevodu, identifikovať dokumentáciu a dôkazy týkajúce sa aktuálne platných certifikátov a zabezpečiť prevod na inú akreditovanú a autorizovanú certifikačnú autoritu alebo na príslušný orgán.

Normatívna požiadavka: Počas prevodu alebo ukončenia sa osobné údaje, zdrojový kód, podrobnosti o zneužití zraniteľností a iné citlivé informácie MUSIA preniesť len v nevyhnutnom rozsahu a s primeranou technickou a organizačnou ochranou. Osobná neformálna komunikácia sa NESMIE preniesť, pokiaľ nie je súčasťou formálneho záznamu o hodnotení a nie je nevyhnutná pre kontinuitu certifikátu.

VIII.10 Matica krížových odkazov: Požiadavky CAB v súlade so slovenskými prílohami

Príloha SK / prvok schémy	Schopnosť CAB požadovaná prílohou VIII	Praktická kontrola počas akreditácie alebo autorizácie
Príloha I – Predmet certifikácie	Schopnosť overiť hranice modulov, architektonické profily, modifikátory ONL/PRX, závislosti, predpoklady a prvky predmetu zákona.	Svedecká kontrola vyhlásenia o predmete a mapovania architektonických profilov.
Príloha IV – Zoznam požiadaviek na informácie	Schopnosť posúdiť dostatočnosť dôkazov, úplnosť, verzie, kontrolovaný prístup, register dôkazov a technické artefakty.	Preskúmanie vzorového súboru dôkazov a kontrolného zoznamu dostatočnosti dôkazov.
Príloha X – Hodnotiace kritériá	Schopnosť porozumieť kritériám pre komplexné hodnotenie, kryptografickú infraštruktúru, správu a riadenie, inštanciu peňaženky, PID, validáciu, funkčnú zhodu a integráciu so slovenskými právnymi predpismi.	Technický pohovor a preskúmanie sledovateľnosti kritérií voči metódam.
Príloha XI – Metódy a postupy	Výkonnosť na vykonávanie alebo dohliadanie na hodnotenie návrhu, skúšanie rizík, analýzu závislostí, audit, inšpekciu, skúšanie, posúdenie zraniteľnosti, funkčné skúšanie a dohľad.	Pilotné hodnotenie alebo rovnocenná praktická demonštrácia.
Príloha IX – Prijateľnosť informácií o záruke	Schopnosť posúdiť autentickosť, platnosť, spôsobilosť vydavateľa, predmet pôsobnosti, predpoklady, nezhody, kompenzačné opatrenia a reziduálne skúšanie.	Prípadová štúdia analýzy závislostí s využitím EUCC, QTSP, ISMS a dôkazov zo správ o skúšaní.
Certifikát a prílohy k správe	Schopnosť vypracovať konzistentný certifikát, certifikačnú správu, CAR a informácie o zložení bez nadhodnocovania predmetu certifikácie.	Preskúmanie vzorových správ a odôvodnenia certifikačného rozhodnutia.
Slovenská národná integrácia	Schopnosť vyhodnotiť národný PID, validáciu, spoliehajúcu sa stranu, podávanie správ orgánom a slovenské zákonné povinnosti, ak je to relevantné.	Pohovor so scenárom národnej integrácie a zmapovaním zákonných povinností.

PRÍLOHA IX – Kritériá na posúdenie prijateľnosti informácií o záruke

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny popis – poznámka k vypracovaniu: Táto príloha zachováva logiku európskej prílohy IX ako hlavný základ: komplexné hodnotenie služieb, uznávané schémy a analýza závislostí podľa CEN TS 18072. Dopĺňa katalóg opätovného použitia záruk požadovaný v prílohe I, prílohe IV, prílohe X a prílohe XI, vrátane slovenských auditov kybernetickej bezpečnosti, dôkazov QTSP/eIDAS, skúšania FCAF/národnej integrácie a záruk komponentov špecifických pre profil.

IX.0 Účel, zásady a vzťah k prílohe I

Informatívny text: Príloha IX definuje, kedy sa CAB môže spoliehať na informácie o záruke vyprodukované mimo bezprostredného hodnotenia EUDIW-SK. Je mostom medzi modulárnym predmetom prílohy I, balíkom dôkazov prílohy IV a metódami hodnotenia prílohy XI.

Normatívna požiadavka: Opätovne použiteľné informácie o záruke MÔŽU podporiť certifikačný záver až po tom, čo CAB posúdila ich autentickosť, predmet, platnosť, spôsobilosť vydavateľa, predpoklady, nezhody, obmedzenia integrácie a relevantnosť pre aktuálny certifikovaný predmet na Slovensku.

Normatívna požiadavka: CAB zostáva zodpovedný za certifikačný záver aj v prípade, ak sa opiera o externé certifikáty, audítorské správy, testovacie správy, osvedčenia alebo iné informácie o záruke.

Normatívna požiadavka: Záverečný certifikačný verdikt NESMIE presiahnuť úroveň záruky podporený najslabšou kritickou závislosťou, pokiaľ kompenzačné opatrenia alebo zostávajúce činnosti CAB nepreukážu, že celkový predmet EUDIW-SK stále spĺňa úroveň záruky vysoká.

IX.1 Hodnotenie zložených služieb

Normatívna požiadavka: Pri hodnotení zložených služieb IKT sa zložená služba IKT hodnotí spolu s produktom IKT, službou IKT, procesom IKT, spravovanou bezpečnostnou službou alebo rámcom organizačných kontrol, ktoré už získali certifikát, správu z auditu, správu z testovania alebo iný výstup záruky, na ktorom zložená služba závisí.

Normatívna požiadavka: Ak sa certifikácia EUDIW-SK opiera o základnú certifikovanú zložku alebo službu, žiadateľ MUSÍ sprístupniť všetky potrebné prvky na analýzu závislostí, vrátane certifikátu, správy, predmetu, verzie, hodnotenej konfigurácie, predpokladov, usmernení, platnosti, zistení a obmedzení integrácie.

Normatívna požiadavka: Usmernenia pre používateľov v oblasti bezpečnosti, predpoklady týkajúce sa prevádzkového prostredia a obmedzenia integrácie základnej zložky alebo služby sa MUSIA považovať za hodnotiace kritériá pre zloženú službu EUDIW-SK.

Normatívna požiadavka: CAB MUSÍ overiť, či platnosť základného certifikátu alebo správy nevypršala, či neboli stiahnuté, nahradené spôsobom, ktorý ovplyvňuje predmet, alebo pozastavené. Pozastavený certifikát NESMIE byť podkladom pre konečný kladný záver, pokiaľ nie je pred ukončením hodnotenia plne obnovený.

Normatívna požiadavka: Ak sa základné informácie o záruke zmenia počas certifikácie alebo údržby, CAB MUSÍ vykonať diferenciálnu analýzu závislosti na tejto zmene a určiť, či je potrebné dodatočné hodnotenie, zmena certifikátu, osobitné hodnotenie alebo zrušenie.

Normatívna požiadavka: Nasledujúce zdroje záruky MOŽNO považovať za základ pre analýzu závislosti. Uznanie v tejto prílohe neznamená automatické prijatie; každá položka podlieha kritériám uvedeným v bodoch IX.3 a IX.4.

Zdroj záruky	Typické použitie v EUDIW-SK	Štandardné zaobchádzanie
Certifikát EUCC / Common Criteria	WSCD, HSM, bezpečnostný prvok, WSCA alebo iná bezpečnostne kritická súčasť produktu.	Silné dôkazy o predmete hodnotenia; predpoklady a usmernenia sa stávajú kritériami EUDIW-SK.
Certifikát EUDIW v rámci súčasnej alebo budúcej európskej schémy	Základná peňaženka, PID alebo služba validácie používaná v kompozitnej alebo zastrešujúcej certifikácii.	Pádny dôkaz, ak je predmet, odchýlky, nezhody a stav dohľadu vhodné.
Posudzovanie zhody QTSP alebo dôveryhodnej služby podľa eIDAS	Stav QTSP, vzdialené operácie QSCD/podobné QSCD, závislosti dôveryhodných služieb, certifikáty, podpisy alebo pečate.	Opätovne použiteľné pre kontrolné opatrenia dôveryhodných služieb, ktoré sú predmetom certifikácie; zostávajú reziduálne integračné riziká a riziká špecifické pre peňaženky.
Audítorské dôkazy založené na ISO/IEC 27001, ETSI EN 319 401 alebo ETSI EN 319 403-1	ISMS, operácie na pozadí, organizačné bezpečnostné opatrenia, riadenie podobné TSP.	Relevantné pre riadenie a prevádzkové opatrenia; samo o sebe nestačí na odolnosť produktu voči zraniteľnosti.
Slovenský audit kybernetickej bezpečnosti alebo dôkazy národného dohľadu	Národné opatrenia kybernetickej bezpečnosti, hlásenie incidentov, logovanie, kontinuita, rozhrania s orgánmi.	Opätovne použiteľné, ak je jasný predmet a spôsobilosť; vyžaduje sa dodatočné priradenie k kritériám EUDIW-SK.
Správy o skúškach funkčnej zhody FCAF alebo národné správy o skúškach funkčnej zhody	Protokol, formát údajov, základná funkčnosť, dôkazy o národnej integrácii a interoperabilite.	Vhodné iba na overenie funkčnej zhody; nenahrádza hodnotenie kybernetickej bezpečnosti.
Penetračné skúšanie, posúdenie zraniteľnosti, kontrola zdrojového kódu alebo dôkazy SBOM	Inštancia peňaženky, backendové API, mobilná/webová aplikácia, softvérový dodávateľský reťazec.	Môže znížiť potrebu dodatočného skúšania, ak sú metodika, predmet skúšania, spôsobilosť testerov a aktuálnosť primerané.
Informácie o dodávateľovi, cloude, hostingu alebo záruke HSM	Kľúčoví dodávatelia, dátové centrá, cloudové HSM, spravované služby a prevádzkové závislosti.	Prijímané iba pre presnú službu, konfiguráciu, umiestnenie a predmet opatrenia, na ktoré sa spoliehame.

IX.2.1 EUCC a Spoločné kritériá

Normatívna požiadavka: Certifikát EUCC alebo ekvivalentný certifikát Common Criteria MÔŽE poskytnúť silnú záruku o spôsobilosti vydavateľa, nestrannosti, prísnosti hodnotenia, analýze zraniteľnosti a zisteniach, ak predmet a konfigurácia hodnoteného produktu zodpovedajú použitiu EUDIW-SK.

Normatívna požiadavka: Ak certifikát uvádza zhodu s profilom ochrany alebo bezpečnostným cieľom vhodným pre komponent a jeho úlohu v prílohe I, CAB sa naň MÔŽE spoliehať, pokiaľ ide o príslušné kritériá produktu, s výhradou predpokladov, usmernení a verifikácie integrácie.

Normatívna požiadavka: Ak certifikát priamo nezodpovedá úlohe komponentu, stupňu záruky, konfigurácii alebo profilu, CAB MUSÍ určiť spoľahlivosť kritérium po kritériu a definovať zostávajúce hodnotiace činnosti.

IX.2.2 Certifikáty EUDIW a certifikáty modulov

Normatívna požiadavka: Certifikát EUDIW alebo certifikát modulu SA MÔŽE opätovne použiť, ak certifikovaná služba, držiteľ certifikátu, hranica modulu, architektonický profil, verzia, modifikátor prípadu použitia a doba platnosti zodpovedajú zloženej slovenskej pôsobnosti.

Normatívna požiadavka: Odchýlky, prebiehajúce dodatočné hodnotiace činnosti, nevyriešené nezhody alebo zmeny certifikátu v základnom certifikáte EUDIW sa MUSIA zohľadniť v zloženom hodnotiacom pláne.

IX.2.3 Dôkazy týkajúce sa eIDAS, QTSP a zoznamu dôveryhodných subjektov

Normatívna požiadavka: Stav QTSP, správy o posudzovaní zhody kvalifikovaných dôveryhodných služieb, stav zoznamu dôveryhodných subjektov a správy o audite dôveryhodných služieb MÔŽU podporiť posúdenie závislostí súvisiacich s QTSP alebo dôveryhodnými službami.

Normatívna požiadavka: CAB MUSÍ overiť aktuálny status zoznamu dôveryhodných subjektov, predmet kvalifikovaných služieb, predmet príslušnej správy o audite, akékoľvek nezhody a presnú úlohu QTSP alebo dôveryhodnej služby v architektúre EUDIW-SK.

Normatívna požiadavka: Zmluva s QTSP alebo dohoda o spoliehaní sa sama o sebe NESMIE preukazovať vhodnosť technickej integrácie. CAB MUSÍ vyhodnotiť predmet zmluvy, prevádzkovú zodpovednosť, rozhrania, predpoklady, povinnosti v súvislosti s incidentmi/zraniteľnosťou a reziduálne opatrenia.

IX.2.4 Systém manažérstva a prevádzková záruka

Normatívna požiadavka: ISO/IEC 27001, ETSI EN 319 401, ETSI EN 319 403-1, národné audítorské správy o kybernetickej bezpečnosti a rovnocenné záruky MÔŽU podporovať riadenie, ISMS, personál, Riadenie prístupov, incidenty, zraniteľnosť, zmeny, kontinuitu a opatrenia dodávateľov.

Normatívna požiadavka: Takéto dôkazy MUSIA byť priradené ku kritériám prílohy X a k skutočnému predmetu prevádzky EUDIW-SK. Všeobecné organizačné certifikáty NESMÚ byť akceptované na účely technickej záruky produktu, odolnosti inštancie peňaženky voči zraniteľnostiam, zabezpečenia kryptografického produktu alebo funkčnej zhody, pokiaľ tieto závery nepodporujú ďalšie dôkazy.

IX.2.5 Funkčné skúšanie a dôkazy o národnej integrácii

Normatívna požiadavka: Výsledky FCAF, správy o národných integračných testoch, správy o zhode protokolov a správy o testoch interoperability MÔŽU podporovať závery o funkčnej zhode pre presnú verziu, profil protokolu, formát údajov, národné rozhranie a tok prípadov použitia, ktoré boli testované.

Normatívna požiadavka: Funkčné dôkazy NESMÚ nahradiť posúdenie zraniteľnosti, penetračné testovanie, inšpekciu návrhu, analýzu závislostí alebo hodnotenie prevádzkovej účinnosti požadované pre úroveň záruky vysoká.

IX.3 Kritériá analýzy závislostí

Normatívna požiadavka: Predtým, ako sa CAB spolieha na informácie o záruke, MUSÍ posúdiť ich relevantnosť a prijateľnosť podľa metódy analýzy závislostí v súlade s CEN TS 18072 a touto prílohou.

Rozmer	Otázka na posúdenie CAB	Minimálny záznam o rozhodnutí
Autentickosť	Je certifikát, správa alebo dôkaz pravý a má sledovateľnosť k jeho vydavateľovi?	Zdroj, identifikátor, vydavateľ, metóda verifikácie.
Spôsobilosť a nestrannosť vydavateľa	Bol dôkaz vydaný orgánom alebo osobou s potrebnou spôsobilosťou a nestrannosťou?	Základ akreditácie, oprávnenia, kvalifikácie, certifikácie alebo spôsobilosti.
Primeranosť predmetu	Zahŕňa dôkaz službu, komponent, proces, opatrenie, verziu a konfiguráciu, na ktoré sa spoliehame?	Zhoda predmetu a presné zostávajúce nedostatky.
Aktualita	Sú dôkazy aktuálne a pokrývajú dostatočne nedávne obdobie?	Platnosť, stav dohľadu, preklenovací list alebo zostávajúce obdobie.
Prísnosť a hĺbka	Je hĺbka hodnotenia dostatočná vzhľadom na kritickosť a tvrdenie o záruke?	Metodika, výber vzoriek, hĺbka skúšania, úroveň záruky.
Predpoklady a usmernenia	Vytvárajú predpoklady, environmentálne obmedzenia alebo usmernenia požiadavky na kompozitnú službu?	Register predpokladov a kritériá integrácie.
Zistenia a výnimky	Existujú nezhody, výhrady, výnimky alebo zvyškové riziká?	Posúdenie vplyvu a stav nápravných opatrení.

Rozmer	Otázka na posúdenie CAB	Minimálny záznam o rozhodnutí
Relevancia integrácie	Zostávajú dôkazy platné v slovenskej architektúre a toku modulov/profilov/prípadov použitia?	Rozhodnutie o integračnom teste alebo zostávajúcej činnosti.

Normatívna požiadavka: CAB MUSÍ určiť spoľahlivosť na úrovni jednotlivých požiadaviek alebo kritérií, nielen na úrovni dokumentu.

Normatívna požiadavka: Ak informácie o záruke obsahujú predpoklady týkajúce sa používania, nasadenia alebo prevádzkového prostredia, certifikačný orgán MUSÍ tieto predpoklady premeniť na explicitné kritériá a požiadavky na dôkazy pre hodnotenie v rámci EUDIW-SK.

Normatívna požiadavka: Ak dokumentácia o záruke obsahuje nezhody, výhrady, výnimky, upozornenia, netestované konfigurácie alebo zostatkové zraniteľnosti, CAB MUSÍ posúdiť významnosť pre predmet certifikácie a NESMIE sa spoliehať na dôkazy bez zohľadnenia vplyvu.

IX.4 Výsledky posúdenia spoľahlivosti

Výsledok posúdenia spoľahlivosti	Význam	Následné opatrenia CAB
Prijaté / plná dôveryhodnosť	Dôkazy plne pokrývajú kritérium pre slovenský predmet a všetky predpoklady sú splnené.	Zaznamenať odôvodnenie; žiadne ďalšie činnosti pre dané kritérium okrem potvrdenia integrácie, ak je to potrebné.
Prijaté s kompenzačnými opatreniami	Dôkazy úplne nepokrývajú kritérium, ale opatrenia žiadateľa dostatočne zmierňujú tento nedostatok.	Vyhodnoťte kompenzačné opatrenia a zvyškové riziko.
Prijaté s dodatočným skúšaním CAB	Dôkazy sú relevantné, ale nedostatočné na to, aby sa na ne dalo priamo spoliehať.	Definujte a vykonajte reziduálnu inšpekciu, skúšanie, audit alebo odber vzoriek.
Zamietnuté / žiadna dôveryhodnosť	Dôkazy nie sú k dispozícii, sú neplatné, neautentické, nekompetentné, neaktuálne, irelevantné alebo nedostatočné.	Nespoliehajte sa na dôkazy; vyžadujte priame dôkazy, prepracovanie alebo vylúčenie z predmetu.

Normatívna požiadavka: Rozhodnutie o spoliehaní sa MUSÍ byť sledovateľné na základe prvkov predmetu v prílohe I, dôkazov v prílohe IV, kritérií v prílohe X a metód v prílohe XI.

Normatívna požiadavka: Rozhodnutie o spoľahlivosti MUSÍ byť zaznamenané v správe o posúdení certifikácie alebo v technickej správe o hodnotení zloženia, vrátane odôvodnenia, zostatkových činností a vplyvu na konečný záver certifikácie.

IX.5 Matica analýzy závislostí pre Slovensko

Informatívny popis: Nasledujúca matica poskytuje CAB minimálnu klasifikáciu typických zdrojov závislosti špecifickú pre Slovensko. Nenahrádza podrobné kritériá v bodoch IX.3 a IX.4.

Závislosť / typ dôkazu	Typické použitie v prílohe I	Kľúčové otázky pre CAB
Vzdialený certifikát HSM / WSCD	Profil A Vzdialený WSCD; kryptografická závislosť.	Zahŕňa ST/ETR presný model, režim, konfiguráciu, fyzické opatrenia a obmedzenia používania kľúčov?
Dôkazy z hodnotenia WSCA	Bezpečná kryptografická aplikácia peňaženky alebo externá závislosť.	Zachováva úroveň záruky a prostredie odolnosť voči vysokému potenciálu útoku? Je akceptovateľné odôvodnenie nižšieho stupňa záruky?
Dôkazy o mobilnej platforme alebo zabezpečenom prvku	Profily B-D a predpoklady inštancie peňaženky.	Dajú sa predpoklady overiť počas behu? Sú vylúčené nepodporované zariadenia?
Stav QTSP alebo zmluva	Právna spôsobilosť poskytovateľa peňaženky alebo závislosť od služby dôvery.	Zahŕňa stav/zmluva skutočnú službu a zodpovednosti? Sú povinnosti týkajúce sa incidentov/zraniteľností a integrácie jasné?

Závislosť / typ dôkazu	Typické použitie v prílohe I	Kľúčové otázky pre CAB
Národný audit kybernetickej bezpečnosti	Opatrenia na backendu, v prevádzkach, na rozhrani s orgánmi alebo v kritickej infraštruktúre.	Zodpovedá predmet auditu certifikovanej službe IKT, lokalitám, procesom a obdobiu?
Dôkazy podľa ISO/IEC 27001 / ETSI	ISMS a prevádzková bezpečnosť.	Je SoA relevantný pre operácie peňaženky/PID/validácie? Sú vylúčené opatrenia podstatné?
FCAF / národná sada testov	Funkčná zhoda a národná integrácia.	Zahŕňajú dôkazy z skúšania deklarovanú verziu, protokoly, toky ONL/PRX a formáty údajov?
Penetračné testovanie alebo kontrola zdrojového kódu	Inštancia peňaženky, backend, API.	Sú metodika, spôsobilosť testerov, aktuálnosť, cieľová verzia, nápravné opatrenia a dôkazy o opakovanom testovaní dostatočné?
Stav QTSP, dôkazy o zozname dôveryhodných subjektov alebo zmluvné dojednania s QTSP	Právna a prevádzková spôsobilosť poskytovateľa riešení peňaženky alebo závislosť od dôveryhodnej služby	Prijmite až po potvrdení predmetu, platnosti, stavu služby a zmluvného prepojenia.
Certifikát EUCC / Common Criteria pre WSCD, HSM alebo bezpečnostný prvok	Kritická kryptografická infraštruktúra a závislosť WSCD špecifická pre profil	Prijmite len v rámci vyhodnotenej konfigurácie a po priradení ST/ETR, predpokladov a usmernení k profilu v prílohe I.
Výsledky funkčnej zhody FCAF alebo národnej funkčnej zhody	Funkčná interoperabilita, správanie protokolu a funkčná správnosť relevantná pre bezpečnosť	Prijímať iba ako funkčný dôkaz; nepovažovať za náhradu za záruku kybernetickej bezpečnosti.
Výstupy auditu kybernetickej bezpečnosti podľa noriem ISO/IEC 27001, ETSI EN 319 401 alebo národných noriem	Operačné a riadiace opatrenia pre backendové služby a zdieľané procesy	Prijmite s dodatočným preskúmaním predmetu, prevádzkovej účinnosti, výnimiek a rozhraní podľa slovenských právnych predpisov.
Dôkazy o národnej infraštruktúre PID, validácii alebo dôveryhodnej strane	Integrácia so slovenskými mechanizmami identity, PID, validácie a dôveryhodných strán	Prijímať len po zmapovaní rozhrania, toku údajov, právnych úloh a prevádzkových zodpovedností.

IX.6 Monitorovanie záruky, na ktorú sa spolieha

Normatívna požiadavka: Držiteľ certifikátu MUSÍ monitorovať stav všetkých certifikátov, správ a informácií o zárukách, na ktoré sa spolieha pri certifikácii EUDIW-SK.

Normatívna požiadavka: Vypršanie platnosti, pozastavenie, zrušenie, zúženie predmetu, nepriaznivý výsledok dohľadu, novo zistená zraniteľnosť, nedostatok v prepojovacom liste alebo významné zistenie v záruke, na ktorú sa spolieha, SA MUSIA považovať za potenciálnu významnú udalosť podľa prílohy II.

Normatívna požiadavka: CAB MUSÍ pri každom ročnom hodnotení dohľadu preskúmať register závislostí a MUSÍ vykonať diferenciálnu analýzu závislostí v prípade, ak došlo k zmene akejkoľvek položky, na ktorú sa spolieha.

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny popis – poznámka k návrhu: Európska kandidátska schéma 0.4.614 považuje prílohu X za miesto pre hodnotiace kritériá a odkazuje na ETSI EN 319 401, prácu WSCA v oblasti profilov ochrany, metodiku inštancií peňaženiek, vyvíjajúce sa normy a dodatočné kritériá odvodené z ARF. Slovenská verzia zachováva túto európsku logiku, ale prispôsobuje ju slovenskému predmetu pôsobnosti prílohy I tým, že definuje kritériá pre komplexné hodnotenie, kryptografickú infraštruktúru, riadenie, inštanciu peňaženky, službu PID, službu validácie, funkčnú zhodu a integráciu do slovenského právneho poriadku.

X.0 Účel, úloha a výklad prílohy X

Informatívny text: Príloha X definuje kritériá, na základe ktorých sa hodnotí certifikovaná služba IKT. Nedefinuje súbor dôkazov, ktorý je uvedený v prílohe IV, a nedefinuje metódu hodnotenia, ktorá je uvedená v prílohe XI. CAB používa prílohu X na určenie toho, čo musí platiť, aby bol certifikovaný predmet definovaný v prílohe I akceptovaný.

Normatívna požiadavka: Služba IKT predložená na certifikáciu v rámci schémy EUDIW-SK MUSÍ byť minimálne hodnotená na základe príslušných kritérií definovaných v tejto prílohe spolu s kritériami vyplývajúcimi z predpokladov komponentov, usmernení pre používateľov, usmernení pre integráciu, analýzy závislostí a konkrétneho predmetu deklarovaného v prílohe I.

Normatívna požiadavka: Hodnotiace kritériá SA MUSIA interpretovať so zreteľom na profil a modul. Kritérium sa uplatňuje len vtedy, ak je relevantné pre certifikovaný modul, architektonický profil, modifikátor prípadu použitia ONL/PRX, závislosť alebo zákonnú úlohu.

Normatívna požiadavka: Ak sa na kritérium vzťahujú opakovane použiteľné informácie o záruke, CAB MUSÍ akceptovať tento rozsah len v rozsahu odôvodnenom analýzou závislostí. Akákoľvek zostávajúca medzera SA STANE dodatočným kritériom pre hodnotenú službu IKT.

X.1 Európske základné zdroje a normy

Informatívny text: Návrh kandidátskej schémy navrhuje použiť normu ETSI EN 319 401 ako základ pre požiadavky na služby, pretože služby IKT v rámci EUDIW sú z hľadiska riadenia, prevádzky, riadenia rizík a auditovateľnosti blízke dôveryhodným službám. Normy ETSI EN 319 403-1 a EN ISO/IEC 17065 poskytujú rámec pre orgány posudzovania zhody. CEN TS 18072 poskytuje koncepcie pre hodnotenie služieb IKT v celom spektre, analýzu závislostí a prevádzkovú účinnosť.

Normatívna požiadavka: Normy ETSI EN 319 401 a súvisiace normy ETSI pre dôveryhodné služby SA MUSIA používať ako základné kritériá pre riadenie služieb IKT, prevádzkovú bezpečnosť, riadenie rizík, Riadenie zmien, riadenie incidentov, riadenie zraniteľností, spoľahlivosť personálu, kontrolu dodávateľov a prevádzku služieb, ak je to vhodné.

Normatívna požiadavka: Hodnotenie WSCA MUSÍ zohľadňovať príslušný profil ochrany WSCA alebo následnú technickú špecifikáciu, ak je dostupná. Ak sa WSCA hodnotí v rámci certifikácie EUCC alebo ekvivalentnej certifikácie Common Criteria, výsledný bezpečnostný cieľ, certifikačná správa, usmernenia a informácie ETR sa MUSIA považovať za opätovne použiteľné záruky podliehajúce analýze závislostí.

Normatívna požiadavka: Pri hodnotení inštancie peňaženky SA MUSÍ zohľadniť primeraný profil ochrany inštancie peňaženky, metodika založená na FiTCEM, OWASP MASVS alebo následná technická špecifikácia primeraná pre variant inštancie peňaženky, platformu a vystavenie riziku.

Normatívna požiadavka: Funkčné požiadavky, na ktoré odkazujú vykonávacie akty Únie, referenčný rámec architektúry a rámec Komisie pre posudzovanie zhody, sa MUSIA použiť ako kritériá funkčnej zhody, ak je to vhodné. Samotná funkčná zhoda sa NESMIE považovať za dostatočnú na splnenie kritérií záruky kybernetickej bezpečnosti na úrovni záruky vysoká.

Normatívna požiadavka: Ak sa vydá nová verzia normy alebo technickej špecifikácie, táto verzia NESMIE automaticky nahradiť verziu, na ktorú sa odvolávajú príslušné akty Únie alebo táto schéma. Vlastník schémy, CAB a žiadateľ MUSIA zdokumentovať každé odôvodnené použitie novších verzií, prechodných verzií alebo návrhov noriem.

Normatívna požiadavka: Povinný externý technický odkaz: Bezpečnostné požiadavky na poskytovateľov služieb súvisiacich s peňaženkami, verzia 0.5.614, marec 2026.

Tabuľka X-1 – Kategórie hodnotiacich činností prevzaté z európskej základnej referenčnej úrovne

Kategória činností z európskej základnej úrovne	Význam v kritériách EUDIW-SK	Typická metóda podľa prílohy XI
Skúšanie zhody	Táto požiadavka je zahrnutá v špecifikáciách, pre ktoré sa vyžaduje zhoda, ako napríklad FCAF alebo národné integračné testy	Skúšanie funkčnej zhody

Kategória činností z európskej základnej úrovne	Význam v kritériách EUDIW-SK	Typická metóda podľa prílohy XI
Špecifické skúšanie	Požiadavka definuje funkciu, ktorej špecifikácia je špecifická pre danú implementáciu a musí byť skúšaná voči očakávanému správaniu	Funkčné alebo bezpečnostné skúšanie na základe schváleného plánu hodnotenia
Interaktívne skúšanie	Požiadavka zahŕňa interakciu s používateľom a vyžaduje pozornosť venovanú rizikám podvodu, súhlasu používateľa, potvrdenia alebo zníženia úrovne	Skúšanie pozorovaného toku používateľov a kontrola zameraná na podvody
inšpekcia	Požiadavka obmedzuje návrh, implementáciu, konfiguráciu alebo integráciu a nemožno ju úplne overiť funkčnými testami	Inšpekcia architektúry, konfigurácie a implementácie
Audit	Požiadavka sa týka politiky, procesu, riadenia alebo prevádzkovej účinnosti	Audit a verifikácia prevádzkovej účinnosti

X.2 Všeobecné zásady komplexného hodnotenia

Platí pre: Riešenie EUDIW-SK, službu SK-PID, službu SK-Validácia a zdieľané alebo externé závislosti.

Účel: Definovať všeobecné kritériá pre modulárne zloženie hodnoteného objektu a prípustnosť opakovane použiteľných informácií o záruke.

Kritériá: Zložená služba IKT MUSÍ spĺňať všeobecné ciele v oblasti kybernetickej bezpečnosti platné pre úroveň záruky vysoká podľa zákona o kybernetickej bezpečnosti a schémy EUDIW.

Kritériá: Služba IKT MUSÍ byť architektonicky navrhnutá tak, aby základné komponenty, podslužby a zdieľané auditovateľné procesy boli logicky oddelené, bezpečne integrované a s sledovateľnosťou podľa vyhlásenia o predmete v prílohe I.

Kritériá: Žiadateľ MUSÍ pre každú zložku určiť, či sa priamo nachádza v predmete pôsobnosti, ide o závislosť, predpoklad prevádzkového prostredia alebo je mimo predmetu pôsobnosti. Nejednoznačné zaobchádzanie nie je prijateľné.

Kritériá: Opätovne použiteľné informácie o záruke SÚ prípustné len vtedy, ak ich rozsah, platnosť, spôsobilosť vydavateľa, predpoklady, nezhody, úroveň záruky a obmedzenia integrácie sú vhodné pre aktuálny predmet certifikácie na Slovensku.

Kritériá: CAB MUSÍ určiť, či je opätovne použiteľná záruka prijatá bez zostatkových činností, prijatá s kompenzačnými opatreniami, prijatá so zostatkovým skúšaním CAB alebo zamietnutá.

Kritériá: Záverečný certifikačný záver najvyššej úrovne NESMIE prekročiť úroveň záruky podporenú najslabšou kritickou závislosťou, pokiaľ kompenzačné opatrenia alebo zvyškové hodnotiace činnosti neopodstatňujú celkový záver.

Očakávané dôkazy: Vyhlásenie o predmete v prílohe I, koncepcia architektúry, model závislostí, zoznam samostatne hodnotených komponentov, register opätovne použiteľnej záruky, usmernenia pre komponenty, dôkazy o integrácii a odôvodnenie zvyškového rizika.

Výsledok rozhodnutia: Validovaná zložená logika závislostí a formálna klasifikácia prípustnosti pre každú položku záruky opätovného použitia.

X.3 Kritériá pre kryptografickú infraštruktúru: WSCD a WSCA

Platí pre: Modul riešenia EUDIW-SK a všetky architektonické profily, v ktorých sa využívajú funkcie WSCD alebo WSCA.

Účel: Zabezpečiť, aby kritické aktíva peňaženky a kryptografické operácie boli chránené opatreniami WSCD/WSCA, ktoré odolávajú útočníkom s vysokým útočným potenciálom a sú v súlade s vybraným architektonickým profilom.

Kritériá: Hranica WSCD MUSÍ byť explicitne identifikovaná pre každý deklarovaný profil: Vzdialené WSCD, Lokálne externé WSCD, Lokálne interné WSCD alebo Lokálne natívne WSCD.

Kritériá: WSCD MUSÍ poskytovať prostredie odolné proti manipulácii na ochranu kritických aktív a vykonávanie kritických kryptografických operácií. Žiadateľ MUSÍ predložiť certifikát alebo rovnocenný dôkaz o záruke vhodný pre úroveň záruky vysoká.

Kritériá: Ak je WSCD alebo jeho časť súčasťou predmetu certifikácie, hodnotenie MUSÍ zahŕňať posúdenie zraniteľnosti na úrovni AVA_VAN.5 podľa normy EN ISO/IEC 15408-3:2026, ako je stanovené v prílohe I vykonávacieho nariadenia (EÚ) 2024/482 (EUCC), pokiaľ žiadateľ neposkytne formálne odôvodnenie prijaté CAB, že bezpečnostné charakteristiky usporiadania WSCA/WSCD umožňujú použitie nižšej úrovne pri zachovaní celkového stupňa záruky High.

Kritériá: Ak sa používa certifikácia EUCC, Common Criteria alebo ekvivalentná certifikácia, predmet, bezpečnostný cieľ, ETR, usmernenie, predpoklady a hodnotená konfigurácia MUSIA byť v súlade so slovenskou architektúrou a tokmi prípadov použitia.

Kritériá: WSCA MUSÍ byť prepojené s kryptografickými a nekryptografickými funkciami poskytovanými WSCD a využívať ich spôsobom, ktorý zachováva výhradnú kontrolu, zabraňuje neoprávnenému použitiu kľúčov a zachováva bezpečnostný model peňaženky.

: WSCA MUSÍ byť hodnotená na úrovni vhodnej pre úroveň záruky vysoká. Ak žiadateľ navrhuje nižšiu úroveň posúdenia zraniteľnosti pre WSCA nasadenú mimo WSCD, MUSÍ predložiť formálne odôvodnenie rizika založené na predpokladoch týkajúcich sa prostredia, závislostiach a zostatkovom vystavení.

Kritériá: Kryptografické algoritmy, parametre a mechanizmy MUSIA byť v súlade s platnými európskymi a slovenskými kryptografickými základnými normami, vrátane strojovo spracovateľných zoznamov alebo usmernení uverejnených príslušným slovenským orgánom, ak je to relevantné.

Kritériá: Generovanie kľúčov, ukladanie kľúčov, používanie kľúčov, zálohovanie, obnovenie, likvidácia, rotácia a riešenie kompromitácie MUSIA byť definované a zdokumentované pre každý profil a tok.

Tabuľka X-2 – Kryptografické kritériá zohľadňujúce profil

Profil prílohy I	Kryptografické kritérium	Očakávané dôkazy	Osobitná pozornosť CAB
Profil A – Vzdialený WSCD	Integrácia vzdialeného HSM alebo Cloud HSM a WSCA musí zachovať vysokú odolnosť proti potenciálnym útokom a záruku výhradnej kontroly	Certifikát HSM, ST/ETR, návrh WSCA, ochrana kanálov, zásady používania kľúčov, opatrenia prevádzkového prostredia	Vzdialené smerovanie, privilegovaný prístup, sieťový kanál, odôvodnenie nižšej úrovne záruky WSCA
Profil B – Lokálne externé WSCD	Externá čipová karta alebo identifikačná karta musia byť bezpečne vyvolané inštanciou peňaženky bez vystavenia materiálu súkromného kľúča operačnému systému zariadenia používateľa	Certifikát CC/EUCC, návrh rozhrania NFC/krátkeho dosahu, dôkaz vyvolania, analýza útokov	Ochrana kanála, riziká miestneho malvéru, predpoklady toku PRX a ONL
Profil C – Lokálny interný WSCD	Vstavaný bezpečnostný prvok alebo eSIM musia spĺňať zdokumentované predpoklady a musia byť overené pred poskytnutím	Dôkaz o zabezpečenom prvku, osvedčenie zariadenia, zásady poskytovania služieb, register predpokladov platformy	Heterogenita zariadení, verifikácia behu a nepodporované zariadenia
Profil D – Lokálny natívny WSCD	Natívna bezpečná enkláva operačného systému alebo jej ekvivalent je certifikovateľná len vtedy, ak žiadateľ môže poskytnúť dostatočnú záruku a vynútiteľné predpoklady	Dôkazy o záruke platformy, analýza bezpečnosti API, osvedčenie a odôvodnenie zvyškového rizika	Dostupnosť vhodnej certifikácie na trhu a nemožnosť overiť zariadenia vo vlastníctve používateľov

Výsledok rozhodnutia: Úspešný, neúspešný alebo prijatý len s dodatočnými hodnotiacimi činnosťami a kompenzačnými opatreniami.

X.4 Kritériá pre riadenie, prevádzku a stav dôveryhodnosti služieb IKT

Platí pre: všetky slovenské moduly a prevádzkovateľov služieb IKT v predmete pôsobnosti.

Kritériá: Poskytovateľ modulu riešenia EUDIW-SK MUSÍ spĺňať slovenské zákonné požiadavky na oprávnenosť poskytovať peňaženky, vrátane statusu QTSP alebo platnej zmluvnej dohody s QTSP, ak je to potrebné.

Kritériá: Každý prevádzkovateľ služieb IKT v predmete pôsobnosti MUSÍ zaviesť a uplatňovať politiky riadenia rizík, riadenia zmien, riadenia zraniteľností, riadenia incidentov, riadenia podvodov, riadenia dodávateľov, Riadenie prístupov a kontinuity.

Kritériá: Poskytovateľ MUSÍ zaviesť opatrenia na riadenie ľudských zdrojov a spôsobilostí, ktoré zabezpečia, že personál zapojený do vývoja, prevádzky, správy bezpečnosti, riešenia incidentov a podpory certifikácie má primerané odborné znalosti, oprávnenia a spoľahlivosť.

Kritériá: Backendové služby a centrá spracovania údajov MUSIA fungovať v rámci ISMS alebo ekvivalentného rámca riadenia bezpečnosti, ktorý je vhodný pre kritickosť služby a úroveň záruky vysoká.

Kritériá: Poskytovateľ MUSÍ definovať predpoklady prevádzkového prostredia a zaviesť mechanizmy na vynútenie alebo overenie predpokladov, ktoré nie sú podložené dôkazmi o zhode.

Kritériá: Poskytovateľ MUSÍ udržiavať opatrenia zabezpečujúce, aby sa v certifikovanom prostredí používali iba aktuálne certifikované alebo inak autorizované verzie príslušnej služby IKT.

Kritériá: Pre backendový softvér, inštanciu peňaženky, komponenty súvisiace s WSCA a iné nasaditeľné artefakty sa MUSIA implementovať mechanizmy bezpečnej aktualizácie, ak je to vhodné.

Kritériá: Riadenie podvodov MUSÍ zahŕňať detekciu a riešenie nezákonného alebo podvodného používania peňaženky, zneužitie registrácie spoliehajúcej sa strany, podvodné vydávanie alebo predkladanie PID a zneužitie služieb validácie.

Očakávané dôkazy: dôkazy QTSP, zmluvy, certifikáty alebo správy ISMS, politiky, SoA, mapovanie architektúry, odôvodnenie ošetrenia rizika, informácie o verejnej bezpečnosti a prevádzkové záznamy.

Výsledok rozhodnutia: Prijatá záruka, prijatá s nevykonanými činnosťami, nezhoda, pozastavenie hodnotenia alebo zamietnutie vydania v závislosti od závažnosti a nápravy.

X.5 Kritériá pre inštanciu peňaženky a hranice medzi zariadením používateľa

Vzťahuje sa na: Modul riešenia EUDIW-SK a všetky deklarované varianty inštancií peňaženky.

Kritériá: Inštancia peňaženky MUSÍ poskytovať robustnú ochranu aktív spracúvaných lokálne na zariadení používateľa, vrátane bezpečného lokálneho ukladania, lokálnej autentifikácie, ochrany integrity, opatrení proti manipulácii, napodobňovaniu a odolnosti voči malvéru, ktoré sú primerané danej platforme.

Kritériá: Inštancia peňaženky MUSÍ chrániť komunikáciu s WSCA, WSCD, backendovými službami, poskytovateľmi PID, službami validácie a rozhraniami spoliehajúcich sa strán v súlade s modelom hrozieb a profilom.

Kritériá: Žiadateľ MUSÍ definovať predpoklady týkajúce sa platformy zariadenia používateľa. Pre každý predpoklad, ktorý nie je podložený dôkazom o zhode, MUSÍ riešenie peňaženky obsahovať mechanizmy behu na overenie, či je predpoklad splnený pred poskytnutím alebo použitím.

Kritériá: Inštancia peňaženky MUSÍ implementovať mechanizmy bezpečnej aktualizácie a vynucovanie verzie, ktoré sú dostatočné na udržanie certifikovaného stavu.

Kritériá: Ak sa podporuje viacero verzií operačného systému, modelov zariadení, variantov aplikácií alebo distribučných kanálov, žiadateľ MUSÍ odôvodniť ekvivalenciu alebo predložiť dôkazy o jednotlivých variantoch.

Očakávané dôkazy: Binárne súbory aplikácie, SBOM, dôkazy o zdrojovom kóde, ak je to relevantné, predpoklady týkajúce sa platformy, návrh osvedčenia zariadenia, návrh lokálneho úložiska a autentifikácie, preskúmanie ochrany súkromia už v štádiu návrhu a dôkazy o penetračných testoch.

Výsledok rozhodnutia: Úspešný, neúspešný alebo nutnosť odstránenia zostatkových nedostatkov pred certifikáciou.

X.6 Kritériá pre poskytovanie PID a viazanie identity

Platí pre: Službu SK-PID a riešenie EUDIW-SK, kde je integrované vydávanie alebo prepojenie PID.

Kritériá: Služba PID MUSÍ implementovať overovanie identity, registráciu, vydávanie PID, životný cyklus PID a procesy zrušenia alebo aktualizácie v súlade s vysokým stupňom záruky, ak sa používa pre peňaženku alebo schému eID na tejto úrovni.

Kritériá: Vydávanie PID MUSÍ byť viazané na správnu peňaženku a používateľa prostredníctvom validácie osvedčenia peňaženky alebo iného povoleného mechanizmu autentizácie s vysokou úrovňou záruky.

Kritériá: Poskytovateľ PID MUSÍ chrániť zdrojové údaje PID, rozhrania národných registrov, transformácie údajov, formáty údajov a protokoly o vydávaní pred neoprávnenou úpravou, nahradením, opakovaným použitím alebo podvodným vydaním.

Kritériá: PID MUSÍ byť vydávané v dátových formátoch požadovaných platnými právnymi predpismi Únie a vnútroštátnymi technickými špecifikáciami.

Kritériá: Poskytovateľ PID MUSÍ uchovávať dôkazy o právnom základe, minimalizácii údajov, presnosti, stave životného cyklu, spracovaní zrušení/aktualizácií a auditovateľnosti.

Očakávané dôkazy: Dôkazy o procese overovania totožnosti, dátový model PID, záruka zdrojového registra, dôkazy o osvedčení peňaženky, protokoly o vydaní, proces zrušenia/aktualizácie a dôkazy o funkčných testoch.

Výsledok rozhodnutia: Úspešné, neúspešné alebo sú potrebné ďalšie dôkazy/skúšanie.

X.7 Kritériá pre platnosť služby validácie a spoliehajúcej sa strany

Vzťahuje sa na: Službu SK-Validácia a riešenie EUDIW-SK, kde sú integrované mechanizmy validácie.

Kritériá: Validácia MUSÍ podporovať verifikáciu pravosti a platnosti jednotiek peňaženky a spoliehajúcich sa strán, ak to vyžaduje predmet certifikácie a povinnosti členského štátu.

Kritériá: Mechanizmus validácie MUSÍ poskytovať správne výsledky validácie, umožňovať detekciu bezpečnostných problémov a udržiavať dostupnosť zodpovedajúcu kritickosti služby.

Kritériá: Registrácia, pozastavenie, zrušenie, aktualizácia certifikátu a podpora vzájomnej autentifikácie spoliehajúcej sa strany MUSIA byť implementované, ak to vyžadujú slovenské zákonné povinnosti alebo národná architektúra.

Kritériá: Dôveryhodné kotvy, informácie o stave certifikátov, identifikátory spoliehajúcich sa strán, rozhrania pre validáciu API a protokoly MUSIA byť chránené pred rizikami neoprávnených úprav, opakovaného prehrávania, nahradenia a odmietnutia služby.

Kritériá: Ak je služba pre validáciu externá voči poskytovateľovi peňaženky, jej záruka MUSÍ byť spracovaná prostredníctvom analýzy závislostí.

Očakávané dôkazy: Architektúra validácie, špecifikácia API, dôkazy o registri dôverujúcich strán, správa dôveryhodných kotiev, návrh dostupnosti, testovacie protokoly a prevádzkové záznamy.

Výsledok rozhodnutia: Vyhovel, nevyhovel, nezhoda alebo závislosť akceptovaná s dodatočnými opatreniami.

Vzťahuje sa na: všetky moduly, pre ktoré je relevantné funkčné skúšanie.

Kritériá: Skúšanie funkčnej zhody MUSÍ overiť integritu, základné funkcie, protokoly, rozhrania, formáty údajov a mechanizmy na ochranu súkromia požadované príslušnými aktmi Únie a vnútroštátnymi integračnými požiadavkami.

Kritériá: Funkčná zhoda SA MUSÍ posudzovať prostredníctvom FCAF, ak je to dostupné a primerané, a prostredníctvom slovenskej národnej sady integračných testov alebo ekvivalentnej národnej referenčnej základne pre povinnú interoperabilitu so slovenskou infraštruktúrou.

Kritériá: Riešenie peňaženky MUSÍ podporovať príslušné toky vzdialenej a bezkontaktnej prezentácie, vrátane protokolov a formátov údajov požadovaných právom Únie a certifikovaným predmetom.

Kritériá: Riešenie peňaženky MUSÍ podporovať mechanizmy ochrany súkromia už v štádiu návrhu, vrátane selektívneho zverejňovania, súhlasu používateľa, minimalizácie údajov a neodvysledovateľnosti v prípadoch, keď nie je vyžadovaná identifikácia používateľa.

Kritériá: Služby PID a validácie MUSIA preukázať funkčnú interoperabilitu s riešením peňaženky a národnou infraštruktúrou pre deklarované hranice modulov.

Kritériá: Funkčné skúšky NESMÚ nahradiť záruku kybernetickej bezpečnosti, posúdenie zraniteľnosti, penetračné skúšanie, inšpekciu návrhu ani audit ISMS.

Očakávané dôkazy: ICS, protokoly testov FCAF, protokoly národných integračných testov, protokoly testov protokolov, preskúmanie ochrany súkromia už v štádiu návrhu a zdôvodnené záznamy o neaplikovateľnosti.

Výsledok rozhodnutia: Vyhlásenie o funkčnej zhode alebo záver o neúspešnej funkčnej zhode.

X.9 Kritériá pre slovenské zákonné povinnosti a národnú integráciu

Vzťahuje sa na: moduly a úlohy, na ktoré sa vzťahujú slovenské národné povinnosti.

Kritériá: Predmet certifikácie MUSÍ zahŕňať auditovateľné mechanizmy na poskytovanie informácií potrebných na monitorovanie dodržiavania predpisov alebo zhody orgánu na požiadanie, ak je to relevantné.

Kritériá: Predmet certifikácie MUSÍ zahŕňať procesy na implementáciu nápravných opatrení uložených orgánom na odstránenie neplnenia, ak je to relevantné.

Kritériá: Predmet certifikácie MUSÍ zahŕňať mechanizmy na pozastavenie alebo zrušenie registrácie spoliehajúcej sa strany na základe rozhodnutia orgánu, ak je to relevantné.

Kritériá: Certifikovaný predmet MUSÍ podporovať automatizované podávanie správ spoliehajúcich sa strán Ministerstvu vnútra počas registrácie, ak je to relevantné.

Kritériá: Predmet certifikácie MUSÍ zahŕňať postupy na bezodkladné hlásenie podozrenia z nezákonného alebo podvodného používania európskej peňaženky orgánu, ak je to vhodné.

Kritériá: Predmet certifikácie MUSÍ umožňovať dôverujúcim stranám bezodkladne aktualizovať certifikáty a prostriedky vzájomnej autentifikácie s európskou peňaženkou, ak je to vhodné.

Kritériá: Národná integrácia s PID, mechanizmami validácie a mechanizmami spoliehajúcich sa strán MUSÍ byť skúšané a preukázané, ak sú tieto mechanizmy súčasťou certifikovaného modulu alebo povinnou závislosťou.

Očakávané dôkazy: Postupy, dôkazy o API, protokoly, komunikačné cesty orgánu, dôkazy o automatizovanom hlásení, dôkazy o eskalácii incidentov/podvodov a záznamy o testoch národnej integrácie.

Výsledok rozhodnutia: Potvrdené, nezhoda alebo mimo predmetu s zdokumentovaným odôvodnením.

X.10 Matica hodnotiacich kritérií

Tabuľka X-3 – Matica hodnotiacich kritérií v súlade s prílohou I a prílohou XI

Č.	Skupina kritérií	Vzťahuje sa na	Očakávané dôkazy	Výstup rozhodnutia	Hlavná metóda
X.2	Komplexné hodnotenie a opakovateľná záruka	Všetky moduly	Koncepcia architektúry, model závislostí, register informácií o záruke	Prijaté / Prijaté s kompenzačnými opatreniami / Prijaté s dodatočným skúšaním CAB / Zamietnuté	XI.3, XI.5
X.3	Kryptografická infraštruktúra: WSCD a WSCA	Riešenie EUDIW-SK, profily A–D, ak je to vhodné	ST, ETR, certifikát, usmernenia k integrácii, kryptografická špecifikácia, argument o výhradnej kontrole	Vyhovel / nevyhovel alebo je potrebné dodatočné skúšanie	XI.5, XI.7
X.4	Správa, prevádzka a stav dôveryhodnosti služieb IKT	Všetky moduly	Dôkazy QTSP, dôkazy ISMS, politiky, ľudské zdroje, zmeny, zraniteľnosť, incidenty a procesy týkajúce sa podvodov	Prijaté záruka / nezhoda / nevydanie	XI.3, XI.5, XI.6
X.5	Inštancia peňaženky a hranica medzi používateľom a zariadením	Riešenie EUDIW-SK	Binárne súbory, SBOM, dôkazy zdrojového kódu, predpoklady o zariadení, dôkazy o bezpečnom ukladaní a lokálnej autentifikácii	Úspešné / Neúspešné / Zostávajúce nápravné opatrenia	XI.7, XI.9
X.6	Poskytovanie PID a viazanie identity	Služba SK-PID a riešenie EUDIW-SK, ak sú integrované	Dôkaz overenia identity, životný cyklus PID, osvedčenie peňaženky, dôkaz formátu údajov	Úspešné / neúspešné / vyžadujú sa ďalšie dôkazy	XI.4, XI.6, XI.8
X.7	Validácia a platnosť dôveryhodnej strany	Služba validácie SK	Validácia, integrácia registra dôverujúcich strán, kotvy dôvery, dôkazy o dostupnosti	Úspešné / Neúspešné / nezhoda	XI.3, XI.8
X.8	Funkčná zhoda a interoperabilita	Všetky moduly, na ktoré sa vzťahujú funkčné testy	ICS, protokoly FCAF, protokoly národných integračných testov, dôkazy o zhode protokolov	Vyhlásenie o funkčnej zhode / neúspech	XI.8
X.9	Slovenské zákonné povinnosti a národná integrácia	Príslušné slovenské role/moduly	Postupy rozhrania s orgánmi, hlásenie spoliehajúcej sa strany, hlásenie nezákonného použitia, podpora aktualizácie certifikátov	Potvrdené / nezhoda / mimo predmetu s odôvodnením	XI.3, XI.4, XI.8

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny popis – poznámka k návrhu: Európska kandidátska schéma 0.4.614 definuje prílohu XI ako miesto pre metódy hodnotenia a vysvetľuje použitie noriem ETSI EN 319 403-1, CEN TS 18072, EUCC/Common Criteria, FiTCEM, hodnotenie návrhu, hodnotenie posúdenia rizík, posúdenie zraniteľnosti, funkčné testovanie a dozorné činnosti. Slovenská verzia zachováva túto metodickú architektúru a premieňa ju na postup CAB v súlade s prílohou I a prílohou X.

XI.0 Účel a metodické zásady

Informatívny text: Príloha XI definuje, ako CAB hodnotí dôkazy požadované v prílohe IV voči kritériám definovaným v prílohe X pre predmet definovaný v prílohe I.

Normatívna požiadavka: CAB MUSÍ použiť kombináciu auditu, inšpekcie, skúšania, analýzy závislostí, hodnotenia návrhu, preskúmania posúdenia rizík, posúdenia zraniteľnosti, penetračného skúšania a skúšania funkčnej zhody, ktorá je dostatočná na dosiahnutie vysokého stupňa záruky pre predmet certifikácie.

Normatívna požiadavka: CAB NESMIE obmedziť hodnotenie na audit dokumentácie. Ak je to potrebné na overenie architektúry, implementácie, prevádzkovej účinnosti alebo odolnosti voči zraniteľnosti, CAB MUSÍ vykonávať inšpekcie a skúšanie alebo sa spoliehať na vhodné opakovane použiteľné informácie o záruke, ktoré prešli analýzou závislostí.

Normatívna požiadavka: CAB MUSÍ zachovať sledovateľnosť od prvku predmetu v prílohe I do dôkazov v prílohe IV, kritérium v prílohe X, metódu v prílohe XI, zistenia a konečné rozhodnutie o certifikácii.

XI.1 Odkazy na normy a technické špecifikácie

Normatívna požiadavka: Základným rámcom auditu MUSÍ byť ETSI EN 319 403-1, ktorý vychádza z normy EN ISO/IEC 17065 pre certifikáciu služieb a je vhodný pre služby IKT EUDIW považované za služby podobné službám dôveryhodnosti.

Normatívna požiadavka: CAB použije externý technický referenčný dokument „Wallet-Related Service Provider Security Requirements, Version 0.5.614, March 2026“[3] , založený na norme EN 319 401, ako podporný technický zdroj pre plánovanie hodnotenia a výber metódy. Certifikačný orgán nesmie s uvedeným dokumentom zaobchádzať ako s mechanicky uplatniteľným kontrolným zoznamom. Namiesto toho certifikačný orgán určí uplatniteľnosť podľa predmetu prílohy I, kritérií prílohy X, architektúry žiadateľa, posúdenia rizika, opakovane použiteľných informácií o záruke a kontextu slovenskej národnej integrácie. Certifikačný orgán zaznamená, ako boli príslušné požiadavky z externého referenčného dokumentu použité, vylúčené, nahradené špecifickejšími kritériami alebo pokryté opakovane použiteľnými informáciami o záruke.

Normatívna požiadavka: CEN TS 18072 SA MUSÍ použiť ako metodická inšpirácia pre analýzu závislostí, hodnotenie prevádzkovej účinnosti, príspevok čiastkových služieb a hodnotenie služieb IKT v plnom rozsahu.

Normatívna požiadavka: EUCC, Spoločné kritériá, ISO/IEC 15408 a ISO/IEC 18045 SA MUSIA použiť na interpretáciu bezpečnostných cieľov, certifikačných správ, usmernení, ETR pre koncepcie zloženia a posudzovania zraniteľnosti, ak sa opätovne používajú certifikované produkty alebo komponenty.

Normatívna požiadavka: CEN EN 17640, schémy založené na FiTCEM, OWASP MASVS a následné metodiky inštancií peňaženiek MÔŽU byť použité na hodnotenie inštancií peňaženiek, ak sú vhodné pre deklarovanú variantu peňaženky.

Normatívna požiadavka: Funkčné skúšanie MUSÍ používať FCAF a Slovenskú národnú sadu integračných testov alebo ekvivalentnú národnú referenčnú základňu, ak je dostupná a uplatniteľná.

XI.2 Organizácia životného cyklu hodnotenia

Informatívny popis: Hodnotenie prebieha podľa fázovej logiky. V prvej fáze sa overuje prijateľnosť a pripravuje sa druhá fáza. V druhej fáze sa vykonáva hlavné hodnotenie. Fáza údržby zachováva záruku po certifikácii.

[3] alebo posledná dostupná verzia

Tabuľka XI-1 – Životný cyklus hodnotenia

Fáza	Hlavný účel	Výstup CAB
Príprava zo strany žiadateľa	Žiadateľ pripraví dôkazy podľa prílohy IV, architektúru, posúdenie rizík, mapovanie opatrení, certifikačný plán a opakovane použiteľné informácie o záruke	Balík podkladov pripravený na posúdenie prijateľnosti
Prvá fáza – prijateľnosť a plánovanie	CAB skontroluje úplnosť, predmet, model závislostí, počiatočné tvrdenie o návrhu, posúdenie rizík a vhodnosť navrhovaného plánu hodnotenia	Schválený plán hodnotenia, požiadavky na zber zvyškových dôkazov, plán analýzy závislostí a testovací plán
Druhá fáza – hlavné hodnotenie	CAB overuje presnosť popisu, vhodnosť návrhu, prevádzkovú účinnosť, funkčnú zhodu, primeranosť závislostí a odolnosť voči zraniteľnosti	Zistenia, nezhody, výsledky testov, klasifikácia závislostí a odporúčania na preskúmanie
Preskúmanie a rozhodnutie o certifikácii	Certifikačný orgán preskúma výsledky hodnotenia a rozhodne, či je možné certifikát vydať	Rozhodnutie o certifikácii, certifikát, certifikačná správa a v prípade potreby správa o zložení
Fáza údržby	Certifikačný orgán, držiteľ certifikátu a orgány monitorujú zmeny, zraniteľnosti, prostredie hrozieb a účinnosť procesov	Potvrdený certifikát, zmenený certifikát, osobitné hodnotenie, pozastavenie alebo zrušenie

Normatívna požiadavka: CAB MUSÍ definovať plán hodnotenia po preskúmaní žiadosti žiadateľa, posúdenia rizík, modelu závislostí a navrhovaného predmetu. Plán MUSÍ špecifikovať, ktoré kritériá sú pokryté opakovane použiteľnými informáciami o záruke a ktoré vyžadujú činnosti CAB.

Normatívna požiadavka: Plán hodnotenia MUSÍ výslovne identifikovať činnosti auditu, inšpekcie, skúšania, odberu vzoriek, analýzy závislostí a podávania správ pre každý modul, profil a modifikátor prípadu použitia v predmete pôsobnosti.

XI.3 Všeobecná metodika auditu, inšpekcie a prevádzkovej účinnosti

Vzťahuje sa na: Riešenie EUDIW-SK, službu SK-PID a službu SK-Validácia.

Hodnotí: X.2 Všeobecné zásady komplexného hodnotenia a X.4 Riadenie, prevádzka a stav dôveryhodnosti služieb IKT.

Vstupné údaje pre hodnotenie: Dokumentácia systémovej architektúry, bezpečnostné politiky, prevádzkové postupy, záznamy o procesoch, záznamy o testoch alebo pilotných projektoch, posúdenie rizík, záznamy o zmenách, záznamy o incidentoch, záznamy o zraniteľnostiach a opakovane použiteľné informácie o zabezpečení.

Postup CAB: CAB MUSÍ potvrdiť dostatočnosť a primeranosť dôkazov, aby poskytol dostatočnú záruku, že služby a procesy spĺňajú certifikačné požiadavky.

Postup CAB: CAB MUSÍ potvrdiť správnosť informácií uvedených v popisoch procesov a služieb.

Postup CAB: CAB MUSÍ potvrdiť vhodnosť návrhu a opatrení na riadenie procesov a služieb na splnenie hodnotiacich kritérií.

Postup CAB: CAB MUSÍ potvrdiť prevádzkovú účinnosť implementovaných opatrení počas špecifikovaného obdobia pred hodnotením, ak sú k dispozícii historické dôkazy.

Postup CAB: V prípade počiatočnej certifikácie, ak nie je možné sledovať historické prevádzkové obdobie, CAB MUSÍ potvrdiť prevádzkovú účinnosť pomocou dôkazov získaných priamo počas testov, pilotných projektov alebo kontrolovanej prevádzky.

Postup CAB: CAB MUSÍ na overenie účinnosti procesu podľa potreby využiť rozhovory, preskúmanie dokumentov, odber vzoriek záznamov, pozorovanie, opätovné vykonanie a technickú inšpekciu.

Logika rozhodovania: Zistenia týkajúce sa presnosti opisu, vhodnosti návrhu a prevádzkovej účinnosti MUSIA byť zaznamenané ako vstupné údaje pre rozhodnutie v správe o certifikačnom posúdení a pri certifikačnom preskúmaní.

XI.4 Metóda hodnotenia návrhu

Vzťahuje sa na: všetky moduly, profily a modifikátory prípadov použitia v deklarovanom predmete.

Účel: Vyhodnotiť, ako žiadateľ tvrdí, že spĺňa kritériá EUDIW, slovenské národné kritériá a register rizík Únie prostredníctvom architektúry, opatrení, závislostí a kompenzačných opatrení.

Kroky vývojára: Žiadateľ MUSÍ predložiť návrh, v ktorom identifikuje uplatniteľné hodnotiace kritériá, komponenty, opatrenia, závislosti, predpoklady, nedostatky, odchýlky, dodatočné kritériá a alternatívne hodnotiace činnosti.

Výstupy vývojára: Dokumentácia návrhu MUSÍ obsahovať návrh služby IKT, odkazy na komponenty, maticu krížových odkazov medzi komponentmi a posudzovanie zhody, zoznam hodnotiacich kritérií po analýze závislostí, popis nedostatkov a odchýlok, ovplyvnené riziká a plány zmierňovania.

Postup CAB: CAB MUSÍ identifikovať architektúru a hlavné komponenty služby IKT.

Postup CAB: CAB MUSÍ overiť zoznam platných hodnotiacich kritérií vo vzťahu k predmetu, hraniciam modulu, profilom, modifikátorom prípadov použitia a výsledkom analýzy závislostí.

Postup CAB: CAB MUSÍ identifikovať odchýlky od platných kritérií EUDIW, slovenských kritérií a metód posudzovania.

Postup CAB: Ak sú odchýlky podstatné a CAB navrhuje, aby hodnotenie pokračovalo, CAB MUSÍ zdokumentovať odôvodnenie a predložiť ho certifikačnému orgánu na preskúmanie, skôr ako sa v certifikačnom závere spolieha na túto odchýlku.

Postup CAB: V prípade celkového certifikátu zahŕňajúceho riešenie peňaženky a schému eID by sa podstatné odchýlky mali eskalovať v súlade s vnútroštátnym procesom preskúmania definovaným vlastníkom schémy pred prijatím konečného rozhodnutia.

Logika rozhodovania: Odchýlka v návrhu môže byť akceptovaná len vtedy, ak CAB môže preukázať, že požadovanú úroveň záruky a pokrytie rizika sú zachované. V opačnom prípade MUSÍ odchýlka viesť k nezhode, zostatkovým činnostiam alebo zamietnutiu plánu hodnotenia.

XI.5 Metóda analýzy závislosti a prípustnosti záruky

Vzťahuje sa na: všetky moduly a všetky opakovane použiteľné informácie o záruke.

Hodnotí: X.2, X.3, X.4, X.5, X.6, X.7 a X.9, kde kritériá pokrýva iný certifikát, audit alebo správa o záruke.

Vstupné údaje pre hodnotenie: Osvedčenia o zhode, certifikačné správy, ETR, bezpečnostné ciele, vyhlásenia o použiteľnosti, audítorské správy ETSI, dôkazy podľa ISO/IEC 27001, zmluvy QTSP, preklenovacie listy, správy o dohľade, správy FCAF a dôkazy o verifikácii behu.

Postup CAB: CAB MUSÍ vyhotoviť zoznam dokumentácie o záruke, ktorá je k dispozícii pre každú príslušnú zložku, podslužbu, proces alebo závislosť.

Postup CAB: CAB MUSÍ posúdiť typ dokumentácie o záruke, dobu platnosti, verziu, uplatniteľný rámec, hodnotenú konfiguráciu, úroveň záruky a priradenie k požiadavkám schémy.

Postup CAB: CAB MUSÍ posúdiť spôsobilosť a nestrannosť vydavateľa, vrátane akreditácie, autorizácie, osobnej certifikácie alebo iných dôkazov o spôsobilosti.

Postup CAB: CAB MUSÍ overiť, či informácie o záruke pokrývajú požiadavku na očakávanom stupni záruky, alebo určiť presný nedostatok.

Postup CAB: Ak informácie o záruke úplne nepokrývajú predmet, CAB MUSÍ určiť, či sú nedostatky zmiernené kompenzačnými opatreniami alebo vyžadujú zostávajúce skúšanie alebo inšpekciu CAB.

Postup CAB: Ak dokumentácia o záruke uvádza nezhody, CAB MUSÍ overiť, či nápravné opatrenia sú primerané a relevantné pre aktuálny predmet certifikácie.

Postup CAB: Pre každý predpoklad prevádzkového prostredia, ktorý nie je podložený dôkazmi z certifikátu, CAB MUSÍ považovať mechanizmus vynútiteľnosti alebo verifikácie behu za bezpečnostné opatrenie a vyhodnotiť jeho vhodnosť a účinnosť.

Postup CAB: Ak sa na splnenie požiadaviek slovenskej právnej spôsobilosti alebo závislosti od služby dôvery používa status QTSP alebo zmluva s QTSP, CAB MUSÍ overiť právnu platnosť a predložiť záruku QTSP do tejto analýzy závislosti.

Tabuľka XI-2 – Klasifikácia prípustnosti opakovane použiteľnej záruky

Klasifikácia	Význam	Požiadavky na ďalšie kroky
Prijaté	Dôkazy plne pokrývajú kritérium a predpoklady integrácie sú splnené	Zaznamenať odôvodnenie a použiť ako podklad pre rozhodnutie
Prijaté s kompenzačnými opatreniami	Dôkazy síce úplne nespĺňajú dané kritérium, avšak opatrenia žiadateľa túto medzeru dostatočne kompenzujú	Vyhodnoťte kompenzačné opatrenia a zaznamenajte zvyškové riziko
Prijaté s dodatočným skúšaním CAB	Dôkazy sú relevantné, ale nedostatočné na priamy záver	Definujte a vykonajte inšpekciu, skúšanie alebo audit zostatkového rizika
Zamietnuté	Dôkazy nie sú autentické, platné, relevantné, kompetentné ani dostatočné	Nespoliehajte sa na dôkazy; vyžadujte priame dôkazy alebo prepracovanie plánu hodnotenia

XI.6 Metodika posudzovania rizík a revízie

Platí pre: všetky moduly a profily.

Vstupné údaje pre hodnotenie: posúdenie rizík žiadateľa, plán ošetrenia rizika, mapovanie registra rizík Únie, mapovanie opatrení, predpoklady, architektúra a model závislostí.

Postup CAB: CAB MUSÍ preskúmať každý scenár rizika z registra rizík Únie a skontrolovať, či má priamy ekvivalent, či je nahradený špecifickejším rizikom alebo či je odôvodnené, že sa neuplatňuje.

Postup CAB: CAB MUSÍ skontrolovať, či riziká pokrývajú externé rozhrania, interné rozhrania, hranice dôveryhodnosti, predpoklady prevádzkového prostredia a národné integračné body.

Postup CAB: CAB MUSÍ overiť, či boli identifikované riziká špecifické pre implementáciu, vrátane rizík vyplývajúcich zo smerovania Remote WSCD, integrácie WSCA/WSCD, predpokladov týkajúcich sa mobilných zariadení, vydávania PID, procesov validácie, registrácie spoliehajúcej sa strany a slovenských zákonných procesov.

Postup CAB: CAB MUSÍ posúdiť kvalitu hodnotenia vplyvu a pravdepodobnosti a odôvodnenie akceptácie zvyškového rizika.

Postup CAB: CAB MUSÍ overiť, či je každé riziko pokryté opatreniami s prijateľným tvrdením o záruke a či vhodnosť a účinnosť týchto opatrení bude vyhodnotená v hlavnom posúdení.

Logika rozhodovania: Ak CAB zistí nezmiernené kritické alebo vysoké riziká, alebo ak sú relevantné riziká z registra rizík Únie vynechané bez primeraného odôvodnenia, CAB MUSÍ vydať oznámenie o nezhode a NESMIE odporučiť certifikáciu, kým sa problém nevyrieši alebo neprijme prostredníctvom zdokumentovaného procesu v súlade so schémou.

XI.7 Metodika posudzovania zraniteľnosti a penetračného skúšania

Informatívne – účel: Vyhodnotiť odolnosť voči skúseným útočníkom a potvrdiť, že riadenie zraniteľností a technické obranné mechanizmy podporujú úroveň záruky vysoká.

Normatívna požiadavka: Ak sa v rámci certifikovaného predmetu vyžaduje hodnotenie WSCD alebo sa naň spolieha ako na kritickú závislosť, CAB MUSÍ overiť, či dôkazy o záruke WSCD zahŕňajú posúdenie zraniteľnosti na úrovni AVA_VAN.5 podľa normy EN ISO/IEC 15408-3:2026, alebo či je akákoľvek nižšia úroveň formálne odôvodnená, akceptovaná a kompenzovaná v súlade s prílohou X.3, prílohou IX a príslušnými požiadavkami Únie.

XI.7.1 Brána odôvodnenia nižšej úrovne záruky WSCA

Platí pre: Modul riešenia EUDIW-SK, najmä profil A Remote WSCD, kde WSCA môže bežať mimo WSCD.

Postup CAB: CAB MUSÍ preskúmať formálne odôvodnenie žiadateľa týkajúce sa rizika, prečo sa na WSCA uplatňuje nižšia úroveň posúdenia zraniteľnosti namiesto predvoleného očakávania vysokej odolnosti.

Postup CAB: CAB MUSÍ overiť výslovnú identifikáciu predpokladov týkajúcich sa prostredia, závislostí a zostatkového vystavenia riziku v súvislosti s WSCA.

Postup CAB: CAB MUSÍ overiť, či bezpečnostné charakteristiky architektúry WSCA a prevádzkového prostredia majú účinnú ochranu proti vektorom útoku, na ktoré sa zvyčajne vzťahuje vyššia úroveň posúdenia zraniteľnosti.

Postup CAB: CAB MUSÍ overiť, či odôvodnenie WSCA nie je v rozpore s predpokladmi v bezpečnostnom cieli WSCD, ETR, usmerneniach alebo certifikačnej správe.

Postup CAB: CAB MUSÍ zdokumentovať formálny záver o tom, či kombinácia WSCA, WSCD a prostredia zachováva odolnosť voči útočníkom s vysokým útočným potenciálom.

Logika rozhodovania: Prijatie umožňuje spoliehať sa na odôvodnenú cestu s nižšou zárukou s reziduálnymi činnosťami. Zamietnutie vyžaduje predvolenú cestu s vyššou zárukou alebo prepracovanie návrhu.

XI.7.2 Posúdenie zraniteľnosti inštancie peňaženky

Platí pre: Modul riešenia EUDIW-SK a všetky deklarované varianty inštancií peňaženky.

Postup CAB: CAB MUSÍ vykonať alebo sa spoliehať na vhodné posúdenie zraniteľnosti inštancie peňaženky s použitím príslušnej metodiky, ako je CEN EN 17640/FiTCEM, OWASP MASVS alebo následný profil inštancie peňaženky.

Postup CAB: CAB MUSÍ preskúmať návrh a, ak je to vhodné a na základe rizika, zdrojový kód pomocou techník statickej a/alebo dynamickej analýzy.

Postup CAB: CAB MUSÍ vykonať alebo preskúmať aktívne penetračné testovanie inštancie peňaženky, vrátane pokusov o obídenie lokálnej autentifikácie, extrakciu údajov zo zabezpečeného úložiska, riadenie peňaženky prostredníctvom malvéru, manipuláciu s aplikáciou alebo nasadenie napodobňujúcich aplikácií.

Postup CAB: CAB MUSÍ overiť bezpečnú aktualizáciu, ochranu integrity, vynútenie predpokladov platformy a vynútenie verzie.

XI.7.3 Posúdenie zraniteľnosti služieb IKT a backendových služieb

Vzťahuje sa na: riešenie EUDIW-SK, službu SK-PID a backendové služby a rozhrania API služby SK-Validácia.

Postup CAB: CAB MUSÍ preskúmať sieťovú architektúru, špecifikácie API, návrh backendu a dôkazy zdrojového kódu, ak je to vhodné, na základe kritickosti a rizika.

Postup CAB: CAB MUSÍ preskúmať výsledky posúdenia zraniteľnosti a penetračného skúšania zameraného na verejne dostupné rozhrania API a backendovú infraštruktúru.

Postup CAB: CAB MUSÍ vykonať alebo vyžadovať dodatočné skúšanie, ak predchádzajúce správy nezahŕňajú certifikovaný predmet, deklarované profily, toky prípadov použitia alebo národné integračné body.

Postup CAB: CAB MUSÍ overiť prevádzkovú účinnosť procesu riadenia zraniteľností prostredníctvom náhodného výberu nedávnych skenov zraniteľností, záznamov o nápravných opatreniach a harmonogramov opravy kritických a vysokých zraniteľností.

Postup CAB: Ak zostanú zneužiteľné zraniteľnosti nezmiernené alebo je riadenie zraniteľností neefektívne, CAB MUSÍ vydať oznámenie o nezhode.

XI.8 Vykonávanie skúšania funkčnej zhody

Platí pre: všetky moduly, kde je relevantná funkčná zhoda.

Postup CAB: CAB MUSÍ pred aktívnym skúšaním preskúmať vyhlásenie žiadateľa o zhode implementácie alebo ekvivalentný vstup týkajúci sa zhody.

Postup CAB: CAB MUSÍ overiť odôvodnené tvrdenia o neaplikovateľnosti porovnaním so schválenou architektúrou, predmetom a hranicami modulu.

Postup CAB: CAB MUSÍ vykonať, sledovať alebo sa spoliehať na vhodné testovacie sady FCAF pre príslušné protokoly, formáty údajov, požiadavky na integritu a základné funkcie.

Postup CAB: CAB MUSÍ vykonať alebo dodržiavať súbor testov slovenskej národnej integrácie alebo ekvivalentnú národnú základnú líniu pre integráciu s národným PID, validáciou a infraštruktúrou spoliehajúcej sa strany, ak je to relevantné.

Postup CAB: CAB MUSÍ overiť, či validačné mechanizmy poskytujú správne výsledky validácie, umožňujú detekciu bezpečnostných problémov a spĺňajú deklarované požiadavky na dostupnosť.

Postup CAB: CAB MUSÍ zaznamenať ciele testov, vstupy, očakávané výsledky, skutočné výsledky, odchýlky a závery spôsobom, ktorý umožňuje sledovateľnosť.

Logika rozhodovania: Ak sú všetky príslušné skúšky úspešné a tvrdenia o neaplikovateľnosti sú odôvodnené, CAB môže potvrdiť vyhlásenie o funkčnej zhodnosti. Nedostatky v oblasti funkčnej zhody MUSIA byť pred certifikáciou odstránené alebo vylúčené z predmetu s odôvodnenými obmedzeniami.

XI.9 Pravidlá hodnotenia podskupín a odberu vzoriek

Platí pre: všetky moduly, pri ktorých CAB netestuje každé zariadenie, operačný systém, API, zostavenie, variant transakcie alebo testovací prípad vývojára.

Postup CAB: CAB NESMIE používať odber vzoriek, aby sa vyhlo hodnoteniu zásadne odlišných architektúr, kryptografických smerovacích ciest, mechanizmov autentifikácie alebo hraníc dôveryhodnosti.

Postup CAB: V prípade inštancií peňaženiek MÔŽE CAB skúšať reprezentatívnu vzorku zariadení, verzií operačných systémov alebo zostavení len vtedy, ak žiadateľ preukáže technologickú ekvivalenciu, spoločnú kódovú základňu alebo ekvivalentné bezpečnostné správanie.

Postup CAB: V prípade služby SK-PID a služby SK-Validácia môže CAB odobrať vzorku ekvivalentných variantov API, nasadenia alebo zostavenia len vtedy, ak varianty, z ktorých nebola odobratá vzorka, nezavádzajú podstatne odlišné funkčné alebo bezpečnostné správanie.

Postup CAB: Ak sa CAB spolieha na pozorovanie opätovného vykonania testov vývojárom namiesto nezávislého vykonania CAB, CAB MUSÍ odobrať dostatočný počet testov na potvrdenie zdokumentovaných výsledkov a odôvodnenie, prečo nebolo potrebné nezávislé vykonanie.

Postup CAB: CAB MUSÍ zdokumentovať odôvodnenie vzorkovania, hranice vzorky, odôvodnenie ekvivalencie a zvyškové riziko v hodnotiacom pláne a záverečnej správe.

Logika rozhodovania: Nedostatočné odôvodnenie vzorkovania MUSÍ viesť k dodatočnému skúšaniu, vyradeniu variantov z predmetu skúšania alebo k nezhode.

XI.10.1 Posúdenie vplyvu zmien služby

Postup CAB/žiadateľa: Pri každom hodnotení dohľadu alebo recertifikácie MUSÍ žiadateľ opísať zmeny vykonané v certifikovanej službe IKT od posledného hodnotenia a posúdiť ich vplyv na certifikovaný predmet, posúdenie rizík, opatrenia a závislosti.

Postup CAB/žiadateľa: Posúdenie MUSÍ zohľadňovať zmeny architektúry, profilov, tokov ONL/PRX, verzií softvéru, konfigurácie, komponentov tretích strán, kryptografických mechanizmov, integrácie PID, validáciach, prevádzkových lokalít a opakovane použiteľných informácií o záruke.

Postup CAB/žiadateľa: Žiadateľ MUSÍ odhadnúť významnosť a predložiť posúdenie vplyvu CAB, ak je zmena významná. CAB MUSÍ preskúmať posúdenie a určiť, či je potrebné osobitné hodnotenie.

XI.10.2 Posúdenie vplyvu zmien v prostredí hrozieb

Postup CAB/žiadateľa: Žiadateľ MUSÍ viesť register rizík špecifický pre peňaženku, ktorý odráža aktuálne prostredie hrozieb.

Postup CAB/žiadateľa: Pri aktualizácii registra rizík Únie sa register rizík špecifických pre peňaženku MUSÍ zodpovedajúcim spôsobom aktualizovať a MUSÍ sa posúdiť významnosť nových alebo zmenených rizík.

Postup CAB/žiadateľa: Ak sa v rámci riadenia zraniteľností zistí zraniteľnosť alebo nová kategória hrozieb, ktorá mení prostredie hrozieb, register rizík MUSÍ byť aktualizovaný.

Postup CAB/žiadateľa: Aktualizácia registra rizík sa POVAŽUJE za významnú, pokiaľ žiadateľ nepreukáže, že nové riziká nie sú relevantné alebo sú plne zmiernené existujúcimi opatreniami.

XI.10.3 Preskúmanie vplyvu zraniteľnosti a nápravných opatrení

Postup CAB/žiadateľa: Ak potenciálna zraniteľnosť ovplyvňuje certifikovanú službu IKT, držiteľ certifikátu MUSÍ vykonať analýzu vplyvu zraniteľnosti na certifikovaný predmet, predpoklady, vyhlásenia o záruke a závislosti.

Postup CAB/žiadateľa: Ak má zraniteľnosť podstatný vplyv, držiteľ certifikátu MUSÍ bez zbytočného odkladu predložiť certifikačnému orgánu správu o analýze vplyvu zraniteľnosti a plán nápravných opatrení.

Postup CAB/žiadateľa: CAB MUSÍ preskúmať, či sú plán nápravných opatrení, kompenzačné kontrolné mechanizmy a dôkazy o vykonaní nápravných opatrení dostatočné. V závislosti od závažnosti a rizika MÔŽE byť potrebné osobitné hodnotenie.

Postup CAB/žiadateľa: Zvyšné zraniteľnosti SA MUSIA monitorovať a prehodnocovať počas hodnotení údržby.

XI.11 Matica sledovateľnosti metódy voči kritériám

Tabuľka XI-3 – Sledovateľnosť metódy vo vzťahu ku kritériám

Ref.	Skupina metód	Vzťahuje sa na	Hlavný výstup
XI.2	Hodnotenie životného cyklu a fázovania	Všetky moduly	Príprava, prijateľnosť v prvej fáze a plánovanie hodnotenia, hlavné hodnotenie v druhej fáze, údržba
XI.3	Audit, inšpekcia a prevádzková účinnosť	Všetky moduly	Presnosť popisov, vhodnosť návrhu a opatrenia, prevádzková účinnosť
XI.4	Hodnotenie návrhu	Všetky moduly	Tvrdenie o architektúre, hodnotiace kritériá, nedostatky, odchýlky, kompenzačné opatrenia a dodatočné činnosti
XI.5	Analýza závislostí a prípustnosti záruky	Všetky moduly a závislosti	Opätovne použiteľné informácie o záruke, predpoklady, spôsobilosť vydavateľa a klasifikácia zostatkových činností
XI.6	Posúdenie rizík a revízia	Všetky moduly	Mapovanie registra rizík Únie, riziká špecifické pre implementáciu, zvyškové riziká a rozsah opatrení
XI.7	Hodnotenie zraniteľnosti a penetračné skúšanie	Riešenie EUDIW-SK, služba SK-PID, služba SK-Validácia	Brána WSCA, inštancia peňaženky, odolnosť proti zraniteľnosti na úrovni backendu a služieb
XI.8	Skúšanie funkčnej zhody	Moduly podliehajúce skúšaniu funkčnosti	FCAF, ICS, národné integračné testy, testy protokolov a formátov údajov
XI.9	Hodnotenie podskupín a odber vzoriek	Všetky moduly, z ktorých sa odoberajú vzorky variantov/testov	Ekvivalencia zariadenia/OS/API/verzie, pozorovanie vývojárskych testov a odôvodnenie výberu vzoriek
XI.10	Hodnotenie dohľadu a údržby	Certifikované služby	Vplyv zmien, zmeny prostredia hrozieb, vplyv zraniteľností a preskúmanie nápravných opatrení

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

PRÍLOHA XII – Značka a štítky Zakázané zneužitie

XII.0 Účel a vzťah k certifikačnej značke EUDI Wallet

Informatívny text – poznámka k návrhu: Táto príloha zachováva európsky návrh pravidiel prílohy XII pre značku a štítky ako základ a vizuálne sa zosúlaďuje s ostatnými prílohami. Nepredpokladá sa, že značka a štítky budú používané pred prechodom na európsku certifikačnú schému. Táto príloha bude vychádzať z aktuálneho znenia pravidiel pre značku a štítky z budúcej schválenej európskej certifikačnej schémy.

XII.1 Zakázané použitie

Normatívna požiadavka: Držiteľ certifikátu, dodávatelia komponentov, subdodávatelia a iné strany NESMÚ používať žiadnu značku, štítok, logo ani formuláciu špecifickú pre Slovensko, ktorá naznačuje existenciu národnej značky zhody EUDIW. NESMÚ používať dôveryhodnú značku EUDIW-SK mimo predmetu, podmienok a časového rámca povoleného právom Únie a príslušným certifikátom.

Normatívna požiadavka: Certifikačné tvrdenia sa MUSIA obmedziť na predmet, moduly, profily, modifikátory prípadov použitia, verzie, predpoklady a závislosti výslovne uvedené v certifikáte a verejnej certifikačnej správe.

Normatívna požiadavka: Dodávatelia, subdodávatelia, poskytovatelia komponentov alebo spoliehajúce sa strany NESMÚ tvrdiť, že ich komponenty alebo služby sú certifikované v rámci tejto certifikačnej schémy výlučne na základe toho, že ich používa certifikovaná služba IKT, pokiaľ nemajú vlastný certifikát alebo nie sú výslovne zahrnuté v predmete certifikátu.

XII.2 Zneužitie a náprava

Normatívna požiadavka: Zneužitie certifikačných tvrdení alebo značky dôveryhodnosti EUDIW-SK sa MUSÍ považovať za nedodržiavanie požiadaviek zo strany držiteľa certifikátu a riešiť v súlade s hlavnou časťou schémy, prílohou II a príslušnými postupmi pozastavenia, odňatia a opravy verejných informácií.

Normatívna požiadavka: Ak sa zistí zavádzajúce používanie, CAB MUSÍ požadovať nápravné opatrenie a môže požadovať aktualizáciu verejných informácií, obmedzenie tvrdení, pozastavenie alebo odňatie v závislosti od závažnosti.

XII.0 Účel a vzťah k dôveryhodnej značke EUDI Wallet

Rezervovaná

Priloha de facto caka na buduce rozhodnutie EU -

Normatívna požiadavka:Normatívna požiadavka:Normatívna požiadavka:Normatívna požiadavka:Normatívna požiadavka:Normatívna požiadavka:

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

PRÍLOHA XIII – Predmet a zloženie tímu pre partnerské hodnotenie

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Rezervovaná

Informatívny popis – poznámka k návrhu: Táto príloha zachováva európsky návrh modelu vzájomného hodnotenia podľa prílohy XIII ako hlavný základ a rozširuje predmet pôsobnosti tak, aby odrážal slovenské moduly prílohy I, spôsobilosti CAB podľa prílohy VIII, logiku závislostí podľa prílohy IX a metódy podľa prílohy XI, hoci sa očakáva, že vzájomné hodnotenie nebude uplatniteľné skôr, ako nadobudne účinnosť európska certifikačná schéma.

PRÍLOHA XIV – Integrácia do národnej certifikácie

Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK

Informatívny text – poznámka k vypracovaniu: Táto príloha používa európsky návrh prílohy XIV ako hlavný základ a prevádza ho do slovenskej národnej koordinačnej logiky. Vysvetľuje, ako slovenský systém integruje certifikáciu kybernetickej bezpečnosti, funkčnú zhodu, ochranu súkromia, povinnosti podľa článku 5c nariadenia eIDAS, národné zákonné povinnosti, opakovateľné záruky a budúcu migráciu do európskeho systému.

XIV.0 Účel a stav

Informatívny text: Príloha XIV vysvetľuje, ako systém EUDIW-SK zapadá do širšej národnej certifikačnej schémy požadovanej pre európske digitálne identifikačné peňaženky a systémy elektronickej identifikácie, v rámci ktorých sa poskytujú. Nenahrádza podrobné prílohy týkajúce sa predmetu, dôkazov, kritérií alebo metód. Poskytuje integračnú logiku, ktorá ich spája.

Normatívna požiadavka: Slovenská národná certifikačná schéma MUSÍ zabezpečiť, aby certifikačný záver pokrýval požiadavky uplatniteľné na certifikovanú peňaženku EUDI a systém elektronickej identifikácie, v rámci ktorého je poskytovaná, v rozsahu vyžadovanom právom Únie, slovenským právom a predmetom deklarovaným v prílohe I.

Normatívna požiadavka: Ak sa opätovne použije samostatný európsky certifikát kybernetickej bezpečnosti, certifikát funkčnej zhody, certifikát komponentu, posúdenie ochrany súkromia alebo národné posúdenie dohľadu, MUSÍ sa s ním zaobchádzať ako s opätovne použiteľnými informáciami o záruke a vyhodnotiť sa podľa prílohy IX a prílohy XI, skôr ako bude slúžiť na podporu záveru národnej certifikácie.

XIV.1 Architektúra národnej certifikačnej schémy

Informatívny text: Kandidátska schéma európskeho systému uznáva, že certifikácia peňaženiek nie je jednotná. Slovenský systém sa riadi tým istým princípom tým, že definuje národnú koordinačnú vrstvu, ktorá dokáže zlúčiť priame hodnotenie, certifikáty komponentov, funkčné testovanie, opakovateľné záruky a národné zákonné dôkazy do jedného sledovateľného certifikačného záveru.

Normatívna požiadavka: Národná certifikačná schéma MUSÍ byť schopná kombinovať, podľa potreby: hodnotenie kybernetickej bezpečnosti podľa tohto systému; skúšanie funkčnej zhody; hodnotenie ochrany súkromia a údajov; posúdenie

zostávajúcich požiadaviek článku 5c nariadenia eIDAS; posúdenie slovenských zákonných povinností; a analýzu závislostí certifikátov komponentov alebo služieb.

Normatívna požiadavka: Národný certifikačný systém MUSÍ zachovať sledovateľnosť od certifikovaného objektu v prílohe I po dôkazy v prílohe IV, hodnotiace kritériá v prílohe X, metódy v prílohe XI, klasifikácie opakovateľných záruk v prílohe IX, obsah certifikátu v prílohe V, verejné podávanie správ v prílohe VI a podávanie správ o dôvernom zložení v prílohe VII.

Normatívna požiadavka: Vlastník schémy MÔŽE organizovať tieto činnosti ako samostatné schémy posudzovania zhody, ako samostatné hodnotiace činnosti v rámci schémy EUDIW-SK alebo ako zložený certifikačný systém, za predpokladu, že zodpovednosti, rozhodovacie body, opätovné použitie dôkazov a výstupy podávania správ sú jednoznačné.

Normatívna požiadavka: Certifikácia kybernetickej bezpečnosti v rámci EUDIW-SK MUSÍ zahŕňať požiadavky na kybernetickú bezpečnosť, technické bezpečnostné opatrenia, prevádzkové opatrenia, odolnosť voči zraniteľnosti, zabezpečenie závislostí a aspekty záruky kontinuity v rámci deklarovaného predmetu.

Normatívna požiadavka: Funkčná zhoda MUSÍ byť pokrytá rámcom Európskej komisie na posudzovanie funkčnej zhody, ak je to dostupné a primerané, a slovenským národným súborom integračných testov alebo ekvivalentnou národnou testovacou základňou pre integráciu so slovenskou infraštruktúrou.

Normatívna požiadavka: Výsledky funkčnej zhody MÔŽU byť vyhodnotené v rámci schémy EUDIW-SK alebo opätovne použité ako informácie o zabezpečení od iného príslušného orgánu. V oboch prípadoch funkčná zhoda NESMIE nahradiť činnosti hodnotenia kybernetickej bezpečnosti požadované pre úroveň záruky vysoká.

Normatívna požiadavka: Dôkazy o súkromí a ochrane údajov MUSIA byť zahrnuté, ak sa týkajú certifikovaného predmetu, vrátane selektívneho zverejňovania, neprepojiteľnosti, minimalizácie údajov, súhlasu používateľa, logovania transakcií, izolácie osobných údajov a verejných informácií o používateľoch. Existujúce posúdenia súkromia alebo ochrany údajov MÔŽU byť opätovne použité len v prípade, ak sú relevantné a dostatočné.

XIV.3 Slovenské národné moduly a integrácia certifikátov

Normatívna požiadavka: Moduly EUDIW-SK Solution, SK-PID Service a SK-Validácia MÔŽU byť certifikované samostatne alebo kombinované do jedného certifikačného záveru, za predpokladu, že všetky hranice modulov, predpoklady, závislosti a zdieľané auditovateľné procesy sú výslovne zaznamenané.

Normatívna požiadavka: Ak je modul certifikovaný samostatne, jeho certifikát, certifikačná správa a informácie o zložení uvedené v prílohe VII MUSIA byť vhodné na použitie certifikačným orgánom vykonávajúcim celkové alebo zastrešujúce hodnotenie.

Normatívna požiadavka: Ak sa celkové certifikačné rozhodnutie opiera o viacero modulov alebo externé závislosti, certifikačný orgán MUSÍ zabezpečiť, aby rozhodnutie na najvyššej úrovni neprekročilo úroveň záruky podporenú hranicami hodnotených modulov a klasifikáciami závislostí.

Normatívna požiadavka: Vnútroštátne zákonné povinnosti týkajúce sa registrácie spoliehajúcej sa strany, komunikácie s orgánmi, hlásenia nezákonného používania, integrácie PID, validačných mechanizmov alebo bezplatných validačných mechanizmov MUSIA byť integrované buď ako priame hodnotiace kritériá, alebo ako dôkaz závislosti, v závislosti od predmetu certifikácie.

XIV.4 Oznamovanie a výmena informácií s orgánmi

Normatívna požiadavka: Národná certifikačná schéma MUSÍ definovať rozhranie medzi certifikačnými orgánmi, vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti, dozornými orgánmi eIDAS, vlastníkom schémy, agentúrou ENISA, Európskou komisiou, skupinou pre spoluprácu a ďalšími príslušnými slovenskými orgánmi, ak je to vhodné.

Normatívna požiadavka: Certifikáty, certifikačné správy, správy o posúdení certifikácie, zmeny a doplnenia certifikátov, pozastavenia, zrušenia a informácie o podstatných zraniteľnostiach MUSIA byť zasielané príslušným orgánom v súlade so základom schémy, právom Únie a slovenskými vnútroštátnymi postupmi.

Normatívna požiadavka: Ak sa informácie zdieľajú medzi certifikačnými orgánmi pre kybernetickú bezpečnosť a dozornými orgánmi eIDAS, pri zdieľaní MUSÍ byť zachovaná dôvernosť, ochrana citlivých informácií z hľadiska bezpečnosti, ochrana osobných údajov a ochrana duševného vlastníctva.

Normatívna požiadavka: Slovenský národný certifikačný systém MUSÍ slúžiť ako rozhranie medzi európskym ekosystémom certifikácie kybernetickej bezpečnosti a dohľadovým ekosystémom EUDI Wallet, pretože je najlepšie umiestnený na interpretáciu povinností v oblasti záruky kybernetickej bezpečnosti aj povinností v oblasti zavádzania eIDAS na národnej úrovni.

XIV.5 Podmienky používania certifikátu kybernetickej bezpečnosti na optimalizáciu iných procesov

Normatívna požiadavka: Certifikát kybernetickej bezpečnosti EUDIW-SK alebo budúci európsky certifikát kybernetickej bezpečnosti EUDIW SA MÔŽE použiť na optimalizáciu národných certifikačných činností len v rozsahu, v akom predmet certifikátu, správy, hodnotiace kritériá, metódy a úroveň záruky pokrývajú príslušné požiadavky.

Normatívna požiadavka: Certifikát kybernetickej bezpečnosti MÔŽE podporovať certifikáciu funkčnej zhody len vtedy, ak hodnotenie zahŕňalo príslušné testy zhody, ciele testov, očakávané výsledky, skutočné výsledky a odôvodnené rozhodnutia o neaplikovateľnosti potrebné na národný záver o funkčnej zhode.

Normatívna požiadavka: Certifikát kybernetickej bezpečnosti MÔŽE podporovať posudzovanie súladu s ochranou súkromia len vtedy, ak hodnotené kritériá a dôkazy zahŕňajú uplatniteľné opatrenia ochrany súkromia už v štádiu návrhu, minimalizáciu údajov, kontrolu používateľov, selektívne zverejňovanie, neprepojiteľnosť a požiadavky na izoláciu osobných údajov.

Normatívna požiadavka: Akékoľvek zostávajúce požiadavky, na ktoré sa certifikát kybernetickej bezpečnosti nevzťahuje, MUSIA byť hodnotené osobitne alebo pokryté vhodnými opakovane použiteľnými zárukami prijatými podľa prílohy IX.

XIV.6 Prechod na budúcu európsku schému a zachovanie súladu

Normatívna požiadavka: NBÚ / vlastník schémy MUSÍ udržiavať, pravidelne preskúmavať a aktualizovať slovenský národný systém, ak to vyžadujú zmeny v práve Únie, slovenskom práve, európskych usmerneniach, normách, technických špecifikáciách, rámcoch funkčnej zhody, registroch rizík, profiloch architektúry, skúsenostiach s certifikáciou alebo akreditáciou. Podstatné revízie MUSIA byť zdokumentované a odoslané skupine pre spoluprácu, ak to vyžaduje nariadenie (EÚ) č. 910/2014 a vykonávacie nariadenie Komisie (EÚ) 2024/2981.

Normatívna požiadavka: Schéma EUDIW-SK MUSÍ byť udržiavané tak, aby jeho štruktúra, terminológia, mapovanie dôkazov a výstupy podávania správ mohli byť zosúladené s budúcou prijatou európskou certifikačnou schémou EUDIW pre kybernetickú bezpečnosť s minimálnymi úpravami.

Normatívna požiadavka: Keď sa stane platným európsky systém, vlastník slovenského systému MUSÍ určiť, ktoré vnútroštátne požiadavky sa nahradia, ktoré zostanú ako vnútroštátne integračné alebo eIDAS povinnosti a ktoré dôkazy alebo certifikáty sa môžu počas prechodu opätovne použiť.

Normatívna požiadavka: Existujúce národné certifikáty MÔŽU byť počas prechodného obdobia preskúmané, zmenené, nahradené alebo použité ako opätovne použiteľné informácie o záruke, s výhradou platnosti, predmetu, analýzy závislostí a pravidiel stanovených príslušnými orgánmi.

XIV.7 Matica národnej integrácie

Integračná vrstva	Úloha v slovenskej národnej certifikácii	Hlavné prílohy
Certifikácia kybernetickej bezpečnosti	Hodnotí bezpečnostné opatrenia, odolnosť voči zraniteľnosti, kontinuitu záruky, komplexné zabezpečenie a prevádzkovú bezpečnosť	Príloha I, IV, VIII, IX, X, XI
Funkčná zhoda	Overuje protokoly, rozhrania, formáty údajov, základné funkcie a národnú interoperabilitu	Príloha I, IV, X, XI
Ochrana súkromia a opatrenia na riadenie používateľov	Zahŕňa minimalizáciu údajov, selektívne zverejňovanie, neprepojiteľnosť, súhlas a izoláciu údajov, ak to spadá do predmetu pôsobnosti	Príloha III, IV, X, XI

Integračná vrstva	Úloha v slovenskej národnej certifikácii	Hlavné prílohy
Zákonné povinnosti v Slovenskej republike	Zahŕňa rozhrania orgánov, registráciu spoliehajúcich sa strán, hlásenie nezákonného používania a vnútroštátne mechanizmy validácie/PID	Príloha I, III, IV, X, XI
Záruka opätovného použitia komponentov a služieb	Certifikáty, audity a správy sa prijímajú až po posúdení predmetu, platnosti, predpokladov a zostávajúcich nedostatkov	Príloha IV, VII, IX, XI
Verejné a dôverné podávanie správ	Zabezpečuje, aby certifikáty, verejné správy a CAR/ETR podporovali národný a európsky dohľad	Príloha III, V, VI, VII, XII
Dohľad zo strany kolegov a orgánov	Podporuje konzistentnosť CAB a opatrenie na vysokej úrovni stupňa záruky	Príloha VIII, XIII

Termín	Definícia
Riadenie prístupov	znamená zabezpečenie toho, aby bol fyzický a logický prístup k aktívam autorizovaný a obmedzený na základe požiadaviek na bezpečnosť podnikania a informačnú bezpečnosť [ZDROJ: Z ISO/IEC 27002:2022, 3.1.1]
Prístupové práva	povolenie pre subjekt na prístup k určitému objektu na vykonanie konkrétneho typu operácie [ZDROJ: Z ISO/IEC 2382:2015, 2126298]
akreditácia	osvedčenie tretej strany týkajúce sa orgánu posudzovania zhody, ktoré formálne preukazuje jeho spôsobilosť, nestrannosť a konzistentnú výkonnosť pri vykonávaní konkrétnych činností posudzovania zhody [ZDROJ: Z ISO/IEC 17000:2020(en), 7.7]
akreditačný orgán	orgán posudzovania zhody, ktorý vykonáva akreditáciu Poznámka 1 k heslu: Právomoc akreditačného orgánu vo všeobecnosti vyplýva z vládnej moci. [ZDROJ: Z ISO/IEC 17000:2020(en), 2.6]
Správa infraštruktúry	súbor činností na inštaláciu, odstránenie, úpravu a konzultáciu konfigurácie systému, ktorý je súčasťou informačného systému služby a môže ovplyvniť jej prevádzku alebo bezpečnosť [ZDROJ: Z SecNumCloud verzia 3.2, odsek 1.3.2. Definície (8. marec 2022)]
anonymizácia	proces, ktorým sa osobne identifikovateľné informácie (PII) nezvratne menia takým spôsobom, že dotknutá osoba (PII) už nemožno priamo ani nepriamo identifikovať, a to ani samotným prevádzkovateľom PII, ani v spolupráci s akoukoľvek inou stranou [ZDROJ: Z ISO/IEC 29100:2011(en), 2.2]
typ aplikačných funkcií	typ cloudových funkcií, pri ktorom môže zákazník cloudovej služby používať aplikácie poskytovateľa cloudových služieb [ZDROJ: Z ISO/IEC 22123-1:2023(en), 3.5.2]
dokument o aplikácii	dokument poskytnutý poskytovateľom cloudových služieb (CSP) certifikačnému orgánu (CAB) pri podaní žiadosti o certifikáciu, ktorý obsahuje informácie o cloudovej službe, ktorá má byť certifikovaná
primeraná úroveň riadenia	osoba alebo skupina osôb, na ktorú vrcholový manažment delegoval úlohu alebo zodpovednosť s požadovaným mandátom a právomocou Poznámka 1 k heslu: V rámci bezpečnostných opatrení by primeraná úroveň riadenia bola zvyčajne zodpovedná za politiky a postupy týkajúce sa konkrétnej témy. [ZDROJ: Z CEN-CENELC TS 18026:2024, 3.8]
primeranosť dôkazov	Miera kvality dôkazov [ZDROJ: Z ISAE3000: 12.i.ii]
majetok	všetko, čo má pre organizáciu hodnotu Poznámka 1 k položke: V kontexte informačnej bezpečnosti možno rozlíšiť dva druhy aktív: Primárne aktíva: — informácie; — obchodné procesy a činnosti; — podporné aktíva (na ktorých závisia primárne aktíva) všetkých typov, napríklad: — hardvér; — softvér; — sieť; — personál; — lokality; — štruktúra organizácie. [ZDROJ: Z ISO/IEC 27002:2022(en), 3.1.2]

Termín	Definícia
životnosť majetku	obdobie od vytvorenia majetku po koniec jeho životnosti [ZDROJ: Z ISO 55000:2014(en), 3.2.2]
predpoklad	faktor v procese posudzovania zhody, ktorý sa považuje za pravdivý, skutočný alebo istý bez dôkazu alebo preukázania [Z normy ISO/IEC/IEEE 24765:2017(en), 3.276]
záruka	dôvody pre oprávnenú istotu, že výrobok, služba alebo proces spĺňa určené požiadavky [ZDROJE: Inšpirované normou ISO/IEC 15408-1:3(2009).1.4 a normou ISO/IEC/IEEE 15026-1(2019):3.1]
informácie o záruke	informácie obsahujúce tvrdenie o systéme, dôkazy podporujúce toto tvrdenie, argumentáciu ukazujúcu, ako dôkazy podporujú dosiahnutie tvrdenia, a kontext týchto položiek [ZDROJ: Z ISO/IEC/IEEE 15026-1(2019):3.4]
úroveň záruky	[CSA] základ pre istotu, že produkt IKT, služba IKT alebo proces IKT spĺňa bezpečnostné požiadavky konkrétnej európskej certifikačnej schémy pre kybernetickú bezpečnosť, označuje úroveň, na ktorej bol produkt IKT, služba IKT alebo proces IKT hodnotený, ale ako taký nemeria bezpečnosť príslušného produktu IKT, služby IKT alebo procesu IKT Poznámka 1 k heslu: Schéma často definuje diskrétne stupne záruky a každá takáto diskrétna úroveň definuje mieru istoty, že produkt IKT, služba IKT alebo proces IKT spĺňa požiadavky. [ZDROJ: Z (EÚ) 2019/881, 2.21]
úroveň záruky	[eIDAS] základ pre definovanú úroveň dôvery v deklarovanú alebo potvrdenú identitu osoby, charakterizovaný s odkazom na technické špecifikácie, normy a postupy s tým súvisiace, vrátane technických opatrení, ktorých účelom je zmierniť riziko zneužitia alebo zmeny identity na definovanej úrovni. Poznámka 1 k heslu: Táto definícia zahŕňa spoločné prvky troch úrovní definovaných v článku 8. [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 8]
útok	úspešný alebo neúspešný neoprávnený pokus o zničenie, zmenu, vyradenie z prevádzky, získanie prístupu k majetku alebo akýkoľvek pokus o odhalenie, krádež alebo neoprávnené použitie majetku. [ZDROJ: Z ISO/IEC 27002:2022, 3.1.3]
osvedčenie	vydanie vyhlásenia na základe rozhodnutia, že bolo preukázané splnenie určených požiadaviek Poznámka 1 k heslu: Výsledné vyhlásenie (...) má za cieľ vyjadriť záruku, že určené požiadavky boli splnené. Takáto záruka samo osebe neposkytuje zmluvné ani iné právne záruky. Poznámka 2 k heslu: Osvedčenie prvej strany a osvedčenie tretej strany sa odlišujú pojmami vyhlásenie, certifikácia a akreditácia, ale neexistuje žiadny zodpovedajúci pojem, ktorý by sa dal použiť pre osvedčenie druhej strany. [ZDROJ: Z ISO/IEC 17000:2020(en), 7.3]
atribút	charakteristika, vlastnosť, právo alebo povolenie fyzickej alebo právnickej osoby alebo predmetu [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 43]
audit	proces získavania relevantných informácií o predmete posudzovania zhody a ich objektívneho vyhodnocovania s cieľom určiť, do akej miery sú splnené určené požiadavky Poznámka 1 k heslu: Určené požiadavky sa definujú pred vykonaním auditu, aby bolo možné získať relevantné informácie. Poznámka 2 k heslu: Príkladmi predmetov auditu sú systémy manažérstva, procesy, výrobky a služby. Poznámka 3 k heslu: Na účely akreditácie sa proces auditu nazýva „posudzovanie“. [ZDROJ: Z ISO 17000:2020(en), 6.4]

Termín	Definícia
záver auditu	výsledok auditu po zohľadnení cieľov auditu a všetkých zistení auditu [ZDROJ: Z ISO 9000:2015, 3.13.10]
kritériá auditu	súbor požiadaviek používaných ako referenčný rámec, s ktorým sa porovnávajú cieľové dôkazy Poznámka 1 k heslu: Požiadavky môžu zahŕňať politiky, postupy, pracovné pokyny, zákonné požiadavky, zmluvné záväzky atď. [ZDROJ: ISO 19011:2018(en), 3.7]
audítorské dôkazy	záznamy, vyhlásenia o skutočnostiach alebo iné informácie, ktoré sú relevantné pre kritériá auditu a overiteľné [ZDROJ: Z ISO/IEC 19011:2018, 3.9]
zistenia auditu	výsledky hodnotenia zhromaždených dôkazov auditu vo vzťahu k kritériám auditu [ZDROJ: Z ISO/IEC 19011:2018, 3.10]
plán auditu	opis činností a opatrení pre audit [ZDROJ: Z ISO 19011:2018, 3. 6]
program auditu	opatrenia pre súbor jedného alebo viacerých auditov plánovaných na konkrétne časové obdobie a zameraných na konkrétny účel [ZDROJ: ISO 19011:2018, 3.4]
audítorský tím	jedna alebo viac osôb vykonávajúcich audit, v prípade potreby s podporou technických expertov Poznámka 1 k heslu: Jeden audítor z audítorského tímu je menovaný za vedúceho audítorského tímu. [ZDROJ: ISO 9000:2015(en), 3.13.14]
doba trvania auditu	čas potrebný na naplánovanie a vykonanie úplného a účinného auditu služby klienta [ZDROJ: Z ISO/IEC 17021-1:2015, 3.16]
audítor	osoba, ktorá vykonáva audit Poznámka 1 k heslu: V schémach a súvisiacich dokumentoch sa pojem „audítor“ zvyčajne používa ako subjekt požiadaviek týkajúcich sa auditu vo forme „audítor musí (...)“. [ZDROJ: Z ISO/IEC 17021-1:2015(en), 3.6]
autentický zdroj	repozitár alebo systém, za ktorý zodpovedá orgán verejného sektora alebo súkromný subjekt, ktorý obsahuje a poskytuje atribúty o fyzickej alebo právnickej osobe alebo predmete a ktorý sa považuje za primárny zdroj týchto informácií alebo je uznaný za autentický v súlade s právom Únie alebo vnútroštátnym právom, vrátane správnej praxe [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 47]
overenie	[kyberbezpečnosť] poskytnutie záruky, že deklarovaná charakteristika subjektu je správna [ZDROJ: Z normy ISO/IEC 27022:2022, 3.1.4 [identita] elektronický proces, ktorý umožňuje potvrdenie elektronickej identifikácie fyzickej alebo právnickej osoby alebo potvrdenie pôvodu a integrity údajov v elektronickej forme [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 5]
autentickosť	vlastnosť, že subjekt je tým, za čo sa vydáva [ZDROJ: Z ISO/IEC 27000:2018(en), 3.6]
autorizácia	činnosť vykonávaná NCCA s cieľom overiť, či akreditovaná CAB spĺňa špecifické alebo dodatočné požiadavky definované v európskej certifikačnej schéme pre kybernetickú bezpečnosť [ZDROJ: Z nariadenia EUCSA, článok 60 ods. 3]
automatizované monitorovanie **monitorovanie s automatizáciou**	Zhromažďovať a predspracovávať údaje s cieľom analyzovať niektoré aspekty sledovanej činnosti v diskrétnych intervaloch s dostatočnou frekvenciou pomocou automatizovaných prostriedkov Poznámka 1 k heslu: Pojmy „automatizované monitorovanie“ a „monitor s automatizáciou“ majú v tomto dokumente rovnaký význam
prechodný list	Dokument, ktorý je dostupný pre servisnú organizáciu na pokrytie časového obdobia medzi dátumom ukončenia vykazovaného obdobia aktuálnej správy ISAE a zverejnením novej správy ISAE. Poznámka k heslu: prechodné listy sú potrebné ako doplnok k správam ISAE, ktoré neobsahujú výhľadové vyhlásenia, aby poskytli určitú záruku, že dodávateľ stále uplatňuje opatrenia, ktoré boli auditované v predchádzajúcich správach, a aby oznámil akékoľvek zmeny vo svojom kontrolnom rámci [ZDROJ: ISAE]

Termín	Definícia
kontinuita činnosti	schopnosť organizácie pokračovať v dodávaní produktov a služieb v prijateľných časových rámcoch pri vopred definovanej kapacite počas narušenia [ZDROJ: Z ISO 22301:2019(en), 2019, 3.3]
plán kontinuity činnosti	zdokumentované informácie, ktoré usmerňujú organizáciu pri reagovaní na narušenie a pri obnovení, zotavení a obnovenie dodávok produktov a služieb v súlade s jej cieľmi v oblasti kontinuity činnosti [ZDROJ: Z ISO 22301:2019(en), 2019, 3.4]
analýza vplyvu na podnikanie	proces analýzy vplyvu narušenia na organizáciu v čase Poznámka 1 k heslu: Výsledkom je vyhlásenie a odôvodnenie požiadaviek na kontinuitu činnosti. [ZDROJ: Z ISO 22301:2019(en), 2019, 3.5]
Riadenie kapacít	proces monitorovania, analýzy, podávania správ a zlepšovania kapacity [ZDROJ: Z ISO/IEC TS 22237-7:2018(en), 3.1.2]
metóda vyčlenenia	Metóda zaobchádzania so službami poskytovanými organizáciou poskytujúcou čiastkové služby, pri ktorej popis systému organizácie poskytujúcej služby zahŕňa povahu služieb poskytovaných organizáciou poskytujúcou čiastkové služby, avšak príslušné ciele opatrení tejto organizácie poskytujúcej čiastkové služby a súvisiace opatrenia sú vylúčené z popisu systému organizácie poskytujúcej služby a z predmetu poverenia audítora služieb. Popis systému poskytovateľa služieb a predmet poverenia audítora služieb zahŕňajú opatrenia v poskytovateľovi služieb na monitorovanie účinnosti opatrení v organizácii poskytujúcej čiastkové služby, čo môže zahŕňať preskúmanie správy o záruke týkajúcej sa opatrení v organizácii poskytujúcej čiastkové služby zo strany poskytovateľa služieb. [ZDROJ: Z ISAE3402: 9.a]
certifikácia	osvedčenie treťou stranou týkajúce sa predmetu posudzovania zhody, s výnimkou akreditácie [ZDROJ: Z ISO/IEC 17000:2020(en), 7.6]
certifikačný audit **spoločný audit** **kombinovaný audit** **integrovaný audit**	audit vykonávaný audítorskou organizáciou nezávislou od klienta a strán, ktoré sa spoliehajú na certifikáciu, za účelom certifikácie služby klienta Poznámka 1 k heslu: Pokiaľ nie je výslovne uvedené inak (napr. „interný audit“), v nasledujúcich definíciách sa pojem „audit“ z dôvodu zjednodušenia používa na označenie certifikačného auditu treťou stranou. Poznámka 2 k heslu: Certifikačné audity zahŕňajú počiatočné, dozorné a recertifikačné audity a môžu zahŕňať aj špeciálne audity. Poznámka 3 k heslu: Spoločný audit je situácia, keď dve alebo viac audítorských organizácií spolupracuje na audite jedného klienta. Poznámka 4 k heslu: Kombinovaný audit je situácia, keď je klient auditovaný podľa požiadaviek dvoch alebo viacerých noriem súčasne. Poznámka 5 k heslu: Integrovaný audit je situácia, keď klient integroval uplatňovanie požiadaviek dvoch alebo viacerých noriem do jednej služby a je auditovaný podľa viac ako jednej normy. Poznámka 6 k položke: Odstránené odkazy na systémy manažérstva a pôvodnú poznámku 3. [ZDROJ: Z ISO/IEC 17021-1:2015, 3.4]
certifikačný orgán	orgán posudzovania zhody tretej strany prevádzkujúci certifikačné schémy Poznámka 1 k heslu: Certifikačný orgán môže byť mimovládny alebo vládny (s regulačnou právomocou alebo bez nej). Poznámka k heslu: V tomto dokumente sa pojem certifikačný orgán používa konkrétne na označenie orgánu posudzovania zhody, ktorý vydáva certifikáty, a pojem orgán posudzovania zhody sa používa pri odkazovaní na úlohy hodnotenia, ktoré môžu byť delegované na iné orgány. [ZDROJ: Z ISO/IEC 17065:2012, 3.12, doplnená poznámka]
certifikačná správa	dokument, ktorý sprevádza certifikát a poskytuje jednoduchú prezentáciu certifikovanej služby a zhrnutie činností posudzovania zhody

požiadavka na certifikáciu	určená požiadavka, vrátane požiadaviek na službu, ktorú klient splní ako podmienku na získanie alebo udržanie certifikácie Poznámka k heslu: Ide o definíciu na najvyššej úrovni, ktorá zahŕňa všetky druhy požiadaviek, ktoré je potrebné splniť na získanie certifikácie. [ZDROJ: Z ISO/IEC 17065:2012, definícia 3.7]
certifikačná schéma	Výsledok systému posudzovania zhody, ktorý zahŕňa certifikačnú činnosť Poznámka 1 k heslu: V certifikačnej schéme vedie úspešné posúdenie k vydaniu certifikátu.

Termín	Definícia
Riadenie zmien	proces zaznamenávania, koordinácie, schvaľovania a monitorovania všetkých zmien [ZDROJ: Z ISO/IEC TS 22237-7:2018(en), 3.1.3]
charakteristika	rozlišovací znak Poznámka 1 k heslu: Charakteristika môže byť vrodená alebo priradená. Poznámka 2 k heslu: Charakteristika môže byť kvalitatívna alebo kvantitatívna. [ZDROJ: Z ISO 9000:2015(en), 3.10.1]
požiadavka	informácia deklarovaná zákazníkom (3.13) Poznámka 1 k heslu: Tvrdenie je predmetom posudzovania zhody prostredníctvom validácie (3.2)/verifikácie (3.3). Poznámka 2 k heslu: Tvrdenie môže predstavovať situáciu v určitom časovom bode alebo sa môže vzťahovať na určité časové obdobie. Poznámka 3 k heslu: Tvrdenie by malo byť jasne identifikovateľné a malo by umožňovať konzistentné hodnotenie alebo meranie vo vzťahu k určeným požiadavkám zo strany orgánu pre validáciu (3.4)/orgánu pre verifikáciu (3.5). Poznámka 4 k položke: Tvrdenie možno predložiť vo forme správy, vyhlásenia, deklarácie, projektového plánu alebo súhrnných údajov. [ZDROJ: Z ISO/IEC 17029:2019(en), 3.1]
klient	organizácia, ktorej služba je predmetom auditu na účely certifikácie Poznámka 1 k heslu: „systém manažérstva“ bol nahradený pojmom „služba“ [ZDROJ: Upravené podľa ISO/IEC 17021-1:2015(en), 3.5]
kódex správania	dokument, ktorý špecifikuje etické alebo osobné správanie, ktoré CSP vyžaduje od svojich zamestnancov [ZDROJ: Upravené podľa ISO/IEC TS 17027:2014, 2.23]
kompenzačné opatrenie	interná kontrola, ktorá znižuje riziko existujúcej alebo potenciálnej slabiny opatrenia vedúcej k chybám a opomenutiam [ZDROJ: SOC2]
spôsobilosť	schopnosť uplatňovať vedomosti a zručnosti na dosiahnutie zamýšľaných výsledkov [ZDROJ: Z ISO/IEC 17021:2015(en), 3.7]
sťažnosť	vyjadrenie nespokojnosti akejkoľvek osoby alebo organizácie voči CAB alebo orgánu akreditácie alebo voči NCCA CAB, týkajúce sa činnosti daného CAB, pri ktorom sa očakáva odpoveď [ZDROJ: Upravené podľa ISO/IEC 17000:2020, 8.7]
doplňujúce opatrenie pre používateľskú entitu **CUEC**	opatrenie, ktoré CSP predpokladá, že ho budú mať zavedené ich CSC, aby mohli bezpečne používať ich cloudovú službu POZNÁMKA: Termín pochádza z audítorskej komunity, preto sa vzťahuje na užívateľskú entitu namiesto zákazníka, ale význam je rovnaký. [ZDROJ: SOC2]
doplňujúce opatrenie pre riadenie organizácie poskytujúcej služby **CSOC**	opatrenie, ktoré CSP predpokladá, že ho budú mať zavedené ich poskytovatelia podslužieb, aby mohli bezpečne prevádzkovať svoju cloudovú službu POZNÁMKA: Termín pochádza z audítorskej komunity, preto sa vzťahuje na organizáciu poskytujúcu podslužby namiesto poskytovateľa podslužieb, ale význam je rovnaký. [ZDROJ: SOC2]

dodržiavanie (predpisov/zhody)	zhoda v kontexte pravidiel a požiadaviek definovaných v certifikačnej schéme, ktoré sa vzťahujú na poskytovateľa certifikovaného produktu, služby alebo procesu Poznámka 1 k heslu: Ide o spresnenie normy ISO 19011, ktorá definuje dodržiavanie ako zhodu v kontexte zákonnej alebo regulačnej požiadavky. V tomto prípade je zhoda zhodou v kontexte daného schému. Poznámka 2 k heslu: Termín sa používa na rozlíšenie medzi dodržiavaním požiadaviek definovaných v schéme zo strany poskytovateľa cloudových služieb a zhodou cloudovej služby s požiadavkami na opatrenia definovanými v schéme. [ZDROJ: Inšpirované normou ISO 19011:2018(en), 3.7]
komponenta	najmenšia voliteľná množina prvkov, na ktorých môžu byť založené požiadavky [ZDROJ: Z ISO/IEC 15408-1:2022(en), 3.17]

Termín	Definícia
ohrozenie	strata dôvernosti, integrity alebo dostupnosti informácií, vrátane akéhokoľvek výsledného poškodenia (1) integrity procesu spracovania alebo dostupnosti systémov alebo (2) integrity alebo dostupnosti vstupov alebo výstupov systému [ZDROJ: TSC]
Riadenie konfigurácie	riadiaca činnosť, ktorá uplatňuje technické a administratívne usmernenia počas životného cyklu produktu a služby, identifikácie a stavu ich konfigurácie a súvisiacich informácií o konfigurácii produktov a služieb [ZDROJ: Z ISO/IEC TS 10007:2017(en), Úvod]
zhoda	splnenie požiadavky Poznámka 1 k heslu: keď sa pojem zhoda používa v protiklade k pojmu súlad, vzťahuje sa skôr na požiadavky týkajúce sa predmetu posudzovania zhody ako na požiadavky týkajúce sa certifikačnej schémy. [ZDROJ: Z ISO/IEC 19011:2018(en), 3.20]
posudzovanie zhody	preukázanie, že sú splnené určené požiadavky Poznámka 1 k heslu: Proces posudzovania zhody (...) môže mať negatívny výsledok, t. j. preukázanie, že určené požiadavky nie sú splnené. Poznámka 2 k heslu: Predmetná oblasť posudzovania zhody zahŕňa výberové činnosti, určovacie činnosti, ako sú skúšanie, inšpekcia a audit, revízne činnosti a osvedčovacie činnosti, ako je certifikácia, ako aj akreditáciu orgánov posudzovania zhody. Poznámka 3 k heslu: Norma EN ISO/IEC 17000 neobsahuje definíciu pojmu „zhoda“. Pojem „zhoda“ sa nevyskytuje v definícii pojmu „posudzovanie zhody“. Norma EN ISO/IEC 17000 sa tiež nezaoberá pojmom dodržiavanie (predpisov/zhody). [ZDROJ: Z ISO/IEC 17000:2020(en), 4.1, s niektorými úpravami v poznámkach]
orgán posudzovania zhody CAB	orgán, ktorý vykonáva služby posudzovania zhody, s výnimkou akreditácie Poznámka k heslu: Pojem orgán posudzovania zhody sa používa na označenie orgánov, ktoré vykonávajú úlohy posudzovania zhody vo všeobecnosti, a pojem certifikačný orgán na označenie orgánov, ktoré vydávajú certifikáty. [ZDROJ: Z ISO/IEC 17000:2020, 4.6, doplnená poznámka]
schéma posudzovania zhody	súbor pravidiel a postupov, ktorý opisuje predmety posudzovania zhody, identifikuje určené požiadavky a poskytuje metodiku na vykonávanie posudzovania zhody Poznámka 1 k heslu: Schéma posudzovania zhody môže byť riadená v rámci systému posudzovania zhody. Poznámka 2 k heslu: Schéma posudzovania zhody môže fungovať na medzinárodnej, regionálnej, národnej, subnárodnej alebo odvetvovej úrovni. Poznámka 3 k heslu: Schéma môže pokrývať všetky alebo časť funkcií posudzovania zhody. [ZDROJ: Z ISO/IEC 17000:2020(en), 4.9]
systém posudzovania zhody	súbor pravidiel a postupov na riadenie podobných alebo súvisiacich schém posudzovania zhody Poznámka 1 k heslu: Systém posudzovania zhody môže fungovať na medzinárodnej, regionálnej, národnej, subnárodnej alebo odvetvovej úrovni. [ZDROJ: Z ISO/IEC 17000:2020, 4.8]
vlastné posudzovanie zhody	činnosti posudzovania zhody vykonávané prvou stranou, ktoré posudzujú, či dané produkty IKT, služby IKT alebo procesy IKT spĺňajú požiadavky konkrétnej európskej certifikačnej schémy v oblasti kybernetickej bezpečnosti Poznámka 1 k záznamu: Pôvodná definícia z nariadenia (EÚ) 2019/881 bola preformulovaná, aby sa vytvorilo prepojenie s definíciou činnosti posudzovania zhody vykonávanej prvou stranou, význam však zostáva nezmenený. [ZDROJ: Z (EÚ) 2019/881:2.22]

poradenstvo	účasť na a) navrhovania, výroby, inštalácie, údržby alebo distribúcie certifikovaného výrobku alebo výrobku, ktorý má byť certifikovaný, alebo b) navrhovania, zavádzania, prevádzky alebo údržby certifikovaného procesu alebo procesu, ktorý má byť certifikovaný, alebo c) navrhovanie, poskytovanie alebo údržba certifikovanej služby alebo služby, ktorá má byť certifikovaná [ZDROJ: Z ISO/IEC 17065:2012, 3.2]
opatrenie	opatrenie, ktoré udržiava a/alebo mení riziko Poznámka 1 k heslu: Opatrenia zahŕňajú, ale nie sú obmedzené na, akýkoľvek proces, politiku, zariadenie, postup alebo iné podmienky a/alebo opatrenia, ktoré udržiavajú a/alebo menia riziko. Poznámka 2 k heslu: Opatrenia nemusia vždy vyvolať zamýšľaný alebo predpokladaný modifikačný účinok. [ZDROJ: Z ISO 31000:2018, 3.8 / ISO/IEC 27002:2022(en), 3.1.8]

Termín	Definícia
cieľ opatrení	vyhlásenie opisujúce, čo sa má dosiahnuť v dôsledku implementácie opatrení na riadenie [ZDROJ: ISO/IEC 27000:2018(en), 3.15]
riziko riadenie	riziko, že udalosť, ktorá bráni splneniu bezpečnostnej požiadavky, nebude včas zabránená alebo zistená a napravená prostredníctvom opatrení [Upravované podľa ISAE]
Koordinovaný svetový čas UTC	časová stupnica založená na sekunde, ako je definované v odporúčaní ITU-R TF.460-6. [ZDROJ: EN 319 401]
osvedčenie	zobrazenie identity Poznámka 1 k heslu: Preukaz sa zvyčajne vytvára s cieľom uľahčiť overenie údajov o identite, ktoré reprezentuje. Poznámka 2 k heslu: Informácie o identite reprezentované poverením môžu byť vytlačené na papieri alebo uložené vo fyzickom tokenu, ktorý je zvyčajne pripravený tak, aby potvrdzoval platnosť týchto informácií. PRÍKLAD: Preukazom môže byť používateľské meno, používateľské meno s heslom, PIN, čipová karta, token, odtlačok prsta, pas atď. [ZDROJ: Z ISO/IEC 24760-1:2011, 3.3.5]
kritériá	pravidlá, na ktorých sa môže zakladať úsudok alebo rozhodnutie, alebo podľa ktorých sa môže hodnotiť produkt, služba, výsledok alebo proces [ZDROJ: Z ISO/IEC/IEEE 15289:2019(en), 3.1.6]
kritické aktíva	aktíva v rámci peňaženky alebo súvisiace s ňou, ktoré majú taký mimoriadny význam, že ak by bola ohrozená ich dostupnosť, dôvernosť alebo integrita, malo by to veľmi závažný a oslabujúci vplyv na schopnosť spoliehať sa na peňaženku POZNÁMKA: Aktíva, o ktorých sa tu hovorí, sú iba dátové aktíva a nezahŕňajú kód, hardvér ani iné aktíva [ZDROJ: Z nariadenia (EÚ) 2024/2981 (EUDIF Implementation Act - IA), 2.11, doplnená poznámka]
kybernetické riziko	riziko spôsobené kybernetickou hrozbou Poznámka 1 k heslu: Kybernetické riziká zahŕňajú riziká spojené so stratou dôvernosti, integrity a dostupnosti informácií
kybernetická bezpečnosť	činnosti potrebné na ochranu sieťových a informačných systémov, používateľov týchto systémov a iných osôb, ktorých sa týkajú kybernetické hrozby [ZDROJ: Z nariadenia (EÚ) 2019/881, článok 2 ods. 1]
Nariadeni o kybernetickej bezpečnosti EU CSA	Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií, ktorým sa zrušuje nariadenie (EÚ) č. 526/2013
kybernetická hrozba	akákoľvek potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak nepriaznivo ovplyvniť sieťové a informačné systémy, používateľov týchto systémov a iné osoby [ZDROJ: Z nariadenia (EÚ) 2019/881, článok 2 ods. 8]
uložené údaje	dáta zaznamenané na stabilnom, nevolatílnom úložisku [ZDROJ: Z normy ISO/IEC 27040:2024, 3.2.3]
dátové centrum	štruktúra alebo skupina štruktúr určená na centralizované umiestnenie, prepojenie a prevádzku informačných technológií a sieťových telekomunikačných zariadení poskytujúcich služby ukladania, spracovania a prenosu údajov spolu so všetkými zariadeniami a infraštruktúrami na distribúciu energie a reguláciu prostredia, ako aj s potrebnou úrovňou odolnosti a bezpečnosti vyžadovanou na zabezpečenie požadovanej dostupnosti služieb

	Poznámka 1 k heslu: Štruktúra môže pozostávať z viacerých budov a/alebo priestorov so špecifickými funkciami na podporu primárnej funkcie. Poznámka 2 k heslu: Hranice štruktúry alebo priestoru považovaného za dátové centrum, ktoré zahŕňa zariadenia informačných a komunikačných technológií a podporné systémy riadenia prostredia, môžu byť definované v rámci väčšej štruktúry alebo budovy. [ZDROJ: Z ISO/IEC 30134-1:2016, 3.6]
dáta v pohybe **dáta v tranzite**	dáta prenášané z jedného miesta na druhé Poznámka 1 k heslu: Tieto prenosy zvyčajne zahŕňajú rozhrania, ktoré sú prístupné, a nezahŕňajú interné prenosy (t. j. nikdy nie sú vystavené mimo rozhrania, čipu alebo zariadenia). [ZDROJ: Z ISO/IEC 27040:2015(en), 3.8]

Termín	Definícia
záznam údajov	elektronické údaje zaznamenané spolu s príslušnými metadátami, ktoré podporujú proces spracovania údajov [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 56]
záver	záver na základe výsledkov posúdenia, že splnenie určených požiadaviek bolo alebo nebolo preukázané [ZDROJ: Z ISO/IEC 17000:2020(en), 7.2]
vyhlásenie	osvedčenie prvej strany [ZDROJ: Z ISO/IEC 17000:2020(en), 7.5]
proces deidentifikácie	proces odstránenia prepojenia medzi súborom identifikačných atribútov a dotknutou osobou [ZDROJ: Z ISO/IEC 20889:2018(en), 3.6]
účinnosť návrhu	Vzťahuje sa na vhodnosť opatrenia k určitému dátumu alebo na určité obdobie (zvyčajne 6 až 12 mesiacov) na základe záveru audítora o tom, či (i) vedenie identifikovalo riziká, ktoré ohrozujú dosiahnutie cieľov opatrení; (ii) ak by fungovali efektívne, poskytovali primeranú záruku, že tieto riziká nezabránia dosiahnutiu cieľov opatrení. [ZDROJ: Inšpirované normou ISAE3402]
detekčné opatrenie	Opatrenie, ktoré zistí a nahlási výskyt chýb, opomenutí a neoprávneného použitia alebo záznamov [ZDROJ: SOC2]
určenie	činnosti vykonávané s cieľom získať úplné informácie o splnení určených požiadaviek predmetom posudzovania zhody alebo jeho vzorkou [ZDROJ: Z ISO/IEC 17000:2020(en), A.3.1]
vývojové prostredie	Prostredie, v ktorom sa vyvíjajú zmeny softvéru POZNÁMKA: Prostredie môže byť lokálne na pracovnej stanici jednotlivého vývojára alebo distribuované, prípadne založené na externých službách
narušenie	incident, či už predpokladaný alebo nepredpokladaný, ktorý spôsobuje neplánovanú, negatívnu odchýlku od očakávaného dodania produktov a služieb v súlade s cieľmi organizácie [ZDROJ: Z ISO 22301:2019(en), 2019, 3.10]
dokument	zaznamenaná informácia alebo hmotný predmet, ktorý možno považovať za jednotku [ZDROJ: Z ISO 5127:2001, 1.2.02]
účinnosť	miera, v akej sa realizujú plánované činnosti a dosahujú plánované výsledky [ZDROJ: Dodatok k ISO: 3.6]
Európsky rámec digitálnej identity **EUDIF**	Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení a dopĺňa nariadenie (EÚ) č. 910/2014 z 23. júla 2014, pokiaľ ide o vytvorenie európskeho rámca digitálnej identity
elektronické osvedčenie atribútov **EAA**	osvedčenie v elektronickej forme, ktoré umožňuje overenie atribútov [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 44]
elektronická identifikácia eID	proces používania identifikačných údajov osoby v elektronickej forme, ktoré jednoznačne reprezentujú fyzickú alebo právnickú osobu, alebo fyzickú osobu zastupujúcu inú fyzickú osobu alebo právnickú osobu [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 1]

prostriedky elektronickej identifikácie prostriedky eID	hmotná a/alebo nehmotná jednotka obsahujúca identifikačné údaje osoby, ktorá sa používa na overenie pre online službu alebo, ak je to primerané, pre offline službu [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 2]
schéma elektronickej identifikácie **schéma eID**	systém elektronickej identifikácie, v rámci ktorého sa vydávajú prostriedky elektronickej identifikácie fyzickým alebo právnickým osobám alebo fyzickým osobám zastupujúcim iné fyzické alebo právnické osoby [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 4]

Termín	Vymedzenie pojmu
elektronický podpis	údaje v elektronickej forme, ktoré sú pripojené k iným údajom v elektronickej forme alebo s nimi logicky súvisia a ktoré podpisujúci používa na podpis [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 10]
zamestnanec	osoba, ktorá má zmluvu s poskytovateľom a na ktorú sa vzťahujú opatrenia v oblasti riadenia ľudských zdrojov
vyhlásenie EÚ o zhode	vyhlásenie vyhotovené dodávateľom produktu IKT, procesu IKT alebo služby IKT po vykonaní vlastného posudzovania zhody v kontexte európskej certifikačnej schémy kybernetickej bezpečnosti, v ktorom sa uvádza, že konkrétny produkt IKT, služba IKT alebo proces IKT spĺňa požiadavky európskej certifikačnej schémy kybernetickej bezpečnosti [ZDROJ: Inšpirované nariadením (EÚ) 2019/881, odôvodnenie (81)]
Európska certifikačná skupina pre kybernetickú bezpečnosť **ECCG**	Skupina zložená zo zástupcov vnútroštátnych certifikačných orgánov pre kybernetickú bezpečnosť alebo iných príslušných vnútroštátnych orgánov [ZDROJ: Upravené podľa zákona o kybernetickej bezpečnosti, článok 62]
Európska certifikačná schéma pre kybernetickú bezpečnosť	komplexný súbor pravidiel, technických požiadaviek, noriem a postupov, ktoré sú stanovené na úrovni Únie a ktoré sa vzťahujú na certifikáciu alebo posudzovanie zhody konkrétnych produktov IKT, služieb IKT alebo procesov IKT Poznámka 1 k heslu: Táto definícia je spresnením definície certifikačnej schémy. [ZDROJ: Z nariadenia EK 2019/881:2.9]
Európsky rámec digitálnej identity eIDAS	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. Júla 2014, v znení novelizácie (EU) 2024/1183 z 11. Apríla 2024, ktorým sa mení a dopĺňa nariadenie (EÚ) č. 910/2014 , pokiaľ ide o vytvorenie európskeho rámca digitálnej identity
Európska peňaženka digitálnej identity EUDI Wallet **peňaženka**	elektronický identifikačný prostriedok, ktorý používateľovi umožňuje bezpečne uchovávať, spravovať a vykonávať validáciu identifikačných údajov osoby a elektronických osvedčení o atribútoch s cieľom poskytovať ich dôveryhodným stranám a iným používateľom peňaženiek európskej digitálnej identity, ako aj podpisovať prostredníctvom kvalifikovaných elektronických podpisov alebo pečiatkovať prostredníctvom kvalifikovaných elektronických pečiatok [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 42]
Značka dôveryhodnosti digitálnej peňaženky EÚ	overiteľné, jednoduché a rozpoznateľné označenie, ktoré jasným spôsobom informuje o tom, že európska peňaženka digitálnej identity bola poskytnutá v súlade s nariadením eIDAS [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 50, mierne upravené]
hodnotenie	kombinácia funkcií výberu a určovania v rámci činností posudzovania zhody [ZDROJ: Z normy ISO/IEC 17065:2012(en), 3.3]
úroveň hodnotenia	kombinácia zložiek záruky v rámci metodiky hodnotenia, ktorá zodpovedá stupňu záruky a primeranému stupňu hĺbky a prísnosti, zodpovedajúcej kategórii bezpečnostných problémov [ZDROJ: Z nariadenia EK 881/2019, 52.8]
správa o hodnotení	dokument vypracovaný CAB, ktorý opisuje hodnotiace činnosti a ich výsledky, vrátane auditu a analýzy závislostí
technická správa o hodnotení ETR	[CC] dokumentácia celkového verdiktu a jeho odôvodnenia, vypracovaná hodnotiteľom a predložená hodnotiacemu orgánu [ZDROJ: Z ISO 15408-1: 2022, 3.43]
protokol udalostí	protokol, ktorý zaznamenáva údaje o audítorskej stope súvisiace s prevádzkou systému [ZDROJ: Z ISO 14641:2018, 3.2]

vypršanie	ukončenie platnosti vyhlásenia o zhode po uplynutí stanoveného obdobia [ZDROJ: Z ISO/IEC 17000:2020(en), 8.4]
rozšírená požiadavka	požiadavka na službu definovaná v CSEP
spravodlivé zobrazenie	presný, pravdivý a transparentný popis Poznámka: Toto sa zvyčajne vzťahuje na popis služby zo strany klienta [ZDROJ: Inšpirované AICPA SOC2]
funkcia	abstraktná funkčná charakteristika systému, ktorú môžu pochopiť koncoví používatelia a ďalšie zainteresované strany Poznámka 1 k heslu: V systémovom inžinierstve sú funkcie syntézou potrieb zainteresovaných strán. Tieto funkcie sa budú používať okrem iného na vytvorenie základných technických požiadaviek. [ZDROJ: Z ISO/IEC 26550:2015(en), 3.14]

Termín	Definícia
prvá strana	osoba alebo organizácia, ktorá poskytuje predmet posudzovania zhody [ZDROJ: Z ISO/IEC 17000:2020(en), 2.2]
činnosť posudzovania zhody prvej strany	činnosť posudzovania zhody, ktorú vykonáva osoba alebo organizácia, ktorá poskytuje predmet posudzovania zhody [ZDROJ: Z ISO/IEC 17000:2020(en), 4.3]
podvod	úmyselné nečestné konanie spôsobujúce skutočný alebo potenciálny zisk alebo stratu, ktoré vedie k sociálnej alebo ekonomickej ujme Poznámka 1 k heslu: Podvod zahŕňa aj úmyselné falšovanie, utajovanie, ničenie alebo používanie falšovaných dokumentov, ktoré sa používajú alebo sú určené na použitie na bežné obchodné účely, alebo nesprávne využívanie informácií alebo postavenia na dosiahnutie osobného finančného prospechu. Poznámka 2 k heslu: Podvodné konanie nemusí nevyhnutne predstavovať porušenie zákona. Poznámka 3 k heslu: Podvod môže zahŕňať podvodné konanie vnútorných a/alebo vonkajších strán zamerané na organizáciu alebo podvodné konanie samotnej organizácie zamerané na vonkajšie strany. Poznámka 4 k heslu: Podvod môže zahŕňať stratu peňazí alebo iného majetku spôsobenú osobami vnútri aj mimo organizácie, pričom k podvodu dochádza v čase vykonania činnosti, bezprostredne pred ňou alebo bezprostredne po nej. Poznámka 5 k heslu: Podvod môže byť externý, interný alebo obidva. Externý podvod je taký, pri ktorom páchateľ nie je zamestnancom cieľovej organizácie ani s ňou nemá úzke spojenie. Interný podvod je taký, pri ktorom je aspoň jeden páchateľ zamestnancom cieľovej organizácie alebo s ňou má úzke spojenie a má podrobné vnútorné znalosti o prevádzke, systémoch a postupoch organizácie. [ZDROJ: Z ISO/IEC 37003:2025(en), 3.1]
prípad podvodu	prípad podvodu spáchaného proti organizácii alebo organizáciou [ZDROJ: Z ISO/IEC 37003:2025(en), 3.2]
funkčná zložka	funkčný stavebný blok potrebný na vykonávanie činnosti, podporený implementáciou [ZDROJ: Z ISO/IEC 22123-1:2023(en), 3.3.9]
sprievodca	osoba vymenovaná klientom na pomoc audítorskému tímu [ZDROJ: Z ISO/IEC 17021-1:2015, 3.8]
Proces IKT	súbor činností vykonávaných s cieľom navrhnúť, vyvinúť, dodať alebo udržiavať produkt IKT alebo službu IKT Poznámka 1 k heslu: Tento termín sa používa v prípade, ak má byť proces predmetom certifikácie kybernetickej bezpečnosti. Termín „proces“ je všeobecnejší a mal by sa používať v iných situáciách. [ZDROJ: Z EUCSA, článok 2 ods. 14]
IKT produkt	prvok alebo skupina prvkov siete alebo informačného systému Poznámka 1 k heslu: V definícii certifikačných schém sa pojem „produkt IKT“ používa v súlade s touto definíciou z nariadenia EK 881/2019 a bude sa väčšinou používať na označenie certifikačných schém a produktov certifikovaných pomocou týchto schém. Ide o podmnožinu všeobecnejšieho pojmu „produkt“, ktorého definícia pochádza z normy ISO 9000. [ZDROJ: Z EUCSA, článok 2 ods. 12]
Služba IKT	služba spočívajúca úplne alebo prevažne v prenose, ukladaní, vyhľadávaní alebo spracúvaní informácií prostredníctvom sieťových a informačných systémov Poznámka 1 k heslu: V definícii certifikačných schém sa pojem „služba IKT“ riadi touto definíciou z nariadenia ES 881/2019 a bude sa používať hlavne na označenie certifikačných schém a produktov certifikovaných pomocou týchto schém. Pre všeobecnejšie použitie je vhodnejšie používať pojem „služba“. [ZDROJ: Z EUCSA, článok 2 ods. 13]

porovnávanie totožnosti / stotožnenie	proces, pri ktorom sa identifikačné údaje osoby alebo prostriedky elektronickej identifikácie porovnávajú s existujúcim účtom patriacim tej istej osobe alebo sa s ním prepoja [ZDROJ: Nariadenie (EÚ) č. 910/2014, článok 3 ods. 55]
dopad	výsledok narušenia ovplyvňujúceho cieľ [ZDROJ: Z normy ISO 22301:2019(en), 3.10]

Termín	Definícia
nezaujatosť	prítomnosť objektivity [ZDROJ: Z ISO/IEC 17065:2012, 3.13]
incident	akákoľvek udalosť, ktorá ohrozuje dostupnosť, autentickosť, integritu alebo dôvernosť uložených, prenášaných alebo spracúvaných údajov alebo služieb ponúkaných prostredníctvom sieťových a informačných systémov alebo prostredníctvom nich dostupných. [ZDROJ: EN 319 401]
riešenie incidentov	opatrenia zamerané na zisťovanie, hlásenie, posudzovanie, reagovanie na incidenty v oblasti informačnej bezpečnosti, ich riešenie a Poučenie z incidentov informačnej bezpečnosti [ZDROJ: Z ISO/IEC 27035-1:2023, 3.1.8]
reakcia na incident	opatrenia prijaté na zmiernenie alebo vyriešenie incidentu v oblasti informačnej bezpečnosti, vrátane opatrení prijatých na ochranu a obnovenie normálnych prevádzkových podmienok informačného systému a informácií v ňom uložených [ZDROJ: Z ISO/IEC 27035-1:2023, 3.1.9]
inkluzívna metóda	Metóda zaobchádzania so službami poskytovanými organizáciou poskytujúcou podporné služby, pri ktorej popis systému organizácie poskytujúcej služby zahŕňa povahu služieb poskytovaných organizáciou poskytujúcou podporné služby a príslušné ciele opatrení tejto organizácie poskytujúcej podporné služby a súvisiace opatrenia sú zahrnuté v popise systému organizácie poskytujúcej služby a v predmete poverenia audítora služieb [ZDROJ: Z ISAE3402: 9.g]
informácie	významné údaje [ZDROJ: ISO 9000:2015, 3.8.2]
informačná bezpečnosť	zachovanie dôvernosti, integrity a dostupnosti informácií [ZDROJ: Z ISO/IEC 27000:2016, 2.33]
porušenie informačnej bezpečnosti	ohrozenie informačnej bezpečnosti, ktoré vedie k nežiaducemu zničeniu, strate, zmene, zverejneniu alebo prístupu k chráneným informáciám, ktoré sú prenášané, ukladané alebo inak spracúvané. [ZDROJ: Z ISO/IEC 27002:2022, 3.1.13]
udalosť v oblasti informačnej bezpečnosti bezpečnostná udalosť	udalosť naznačujúca možné porušenie informačnej bezpečnosti alebo zlyhanie opatrení [ZDROJ: Z ISO/IEC 27035-1:2023, 3.1.4]
incident informačnej bezpečnosti bezpečnostný incident **incident**	jedna alebo viacero súvisiacich a identifikovaných udalostí v oblasti informačnej bezpečnosti, ktoré môžu poškodiť aktíva organizácie alebo ohroziť jej činnosť [ZDROJ: Z ISO/IEC 27035-1:2023, 3.1.5]
riadenie incidentov v oblasti informačnej bezpečnosti **riadenie incidentov**	uplatňovanie konzistentného a účinného prístupu k riešeniu incidentov v oblasti informačnej bezpečnosti [ZDROJ: Z ISO/IEC 27002:2022, 3.1.16]
systém manažérstva pre informačnú bezpečnosť **ISMS**	súčasť celkového systému manažérstva, založená na prístupe zohľadňujúcom podnikateľské riziká, používaná na zavádzanie, implementáciu, prevádzku, monitorovanie, preskúmavanie, udržiavanie a zlepšovanie informačnej bezpečnosti [ZDROJ: Z ISO/TS 12812-2:2017(en), 3.11]

informačná služba	akákoľvek služba, ktorá sa zvyčajne poskytuje za odmenu, na diaľku, elektronickými prostriedkami a na individuálnu žiadosť príjemcu služieb. Poznámka 1 k heslu: Na účely tejto definície: (i) „na diaľku“ znamená, že služba sa poskytuje bez toho, aby boli strany súčasne prítomné; (ii) „elektronickými prostriedkami“ znamená, že služba je pôvodne odoslaná a prijatá v mieste určenia prostredníctvom elektronického zariadenia na spracovanie (vrátane digitálnej kompresie) a ukladanie údajov a je v celom rozsahu prenášaná, doručovaná a prijímaná drôtom, rádiom, optickými prostriedkami alebo inými elektromagnetickými prostriedkami; (iii) „na individuálnu žiadosť príjemcu služieb“ znamená, že služba sa poskytuje prostredníctvom prenosu údajov na individuálnu žiadosť. [ZDROJ: Z EC1535/2015:1.b]
vyhľadávanie	činnosť spočívajúca v získavaní informácií od informovaných osôb v rámci subjektu alebo mimo neho [ZDROJ: Z IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, vydanie z roku 2017, Slovník pojmov]

Termín	Definícia
inšpekcia	[CASCO] preskúmanie predmetu posudzovania zhody a stanovenie jeho zhody s podrobnými požiadavkami alebo, na základe odborného úsudku, so všeobecnými požiadavkami Poznámka 1 k heslu: Preskúmanie môže zahŕňať priame alebo nepriame pozorovania, ktoré môžu zahŕňať merania alebo výstupy z prístrojov. Poznámka 2 k heslu: Schémy posudzovania zhody alebo zmluvy môžu špecifikovať inšpekciu iba ako preskúmanie. [ZDROJ: Z ISO/IEC 17000:2020, 6.3]
inšpekcia	[IAASB] činnosť zahŕňajúca preskúmanie záznamov alebo dokumentov, či už interných alebo externých, v papierovej forme, elektronickej forme alebo na iných médiách, alebo fyzické preskúmanie dôkazov [ZDROJ: Z IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, vydanie z roku 2017, Slovník pojmov]
zainteresovaná strana	osoba alebo organizácia, ktorá môže ovplyvniť rozhodnutie alebo činnosť, môže byť nimi ovplyvnená alebo sa môže vnímať ako ovplyvnená [ZDROJ: Dodatok ISO: 3.2]
interný audit	audit vykonávaný samotnou organizáciou alebo v jej mene na účely preskúmania manažmentom a na iné interné účely, ktorý môže slúžiť ako základ pre vlastné vyhlásenie organizácie o zhode Poznámka 1 k heslu: V mnohých prípadoch, najmä v menších organizáciách, možno nezávislosť preukázať tým, že audítor nie je zodpovedný za činnosť, ktorá je predmetom auditu. [ZDROJ: Z ISO 22300:2021(en), 3.1.134]
incident kybernetickej bezpečnosti veľkého rozsahu	udalosť, ktorej rozsah presahuje schopnosti členského štátu na ňu reagovať alebo ktorá má významný vplyv na najmenej dva členské štáty [ZDROJ: Zo smernice (EÚ) 2022/2555]
životný cyklus	etapy spojené s riadením aktív Poznámka 1 k heslu: Názvy a počet fáz a činností v rámci každej fázy sa zvyčajne líšia v rôznych odvetviach priemyslu a určuje ich organizácia. [ZDROJ: Z ISO 55000:2014(en), 3.2.3]
obmedzená záruka	typ uistenia, pri ktorom boli povaha a rozsah hodnotiacich činností navrhnuté tak, aby poskytovali zníženú úroveň záruky. Poznámka 1 k heslu: Záver hodnotiteľa je vyjadrený formou, ktorá vyjadruje, či na základe vykonaných hodnotiacich činností a získaných dôkazov upútala pozornosť hodnotiteľa nejaká záležitosť (záležitosti), ktorá ho vedie k presvedčeniu, že predmet posudzovania zhody vykazuje nezhody. Poznámka 2 k heslu: Záver hodnotiteľa v prípade objednaných služieb s obmedzenou zárukou je formulovaný v negatívnom zmysle, napríklad: „Na základe vykonaných postupov sme nezistili nič, čo by naznačovalo, že cloudová služba XYZ nespĺňa certifikačné požiadavky **dokumentu Error! Unknown** na stupni záruky LLL.“ [ZDROJ: Inšpirované normou ISO 14064-3:2019, 3.6.7]
závažná nezhoda	nezhoda, ktorá ovplyvňuje schopnosť systému manažérstva dosiahnuť zamýšľané výsledky Poznámka 1 k heslu: Nezhody sa môžu klasifikovať ako závažné v nasledujúcich prípadoch: - ak existujú značné pochybnosti o tom, či je zavedená účinná kontrola procesov alebo či výrobky alebo služby budú spĺňať určené požiadavky; - viacero menších nezhôd súvisiacich s tou istou požiadavkou alebo problémom môže svedčiť o systémovom zlyhaní a tým predstavovať závažnú nezhodu.

	[ZDROJ: Upravené podľa ISO/IEC 17021-1:2015(en), 3.12]
malvér škodlivý softvér	Škodlivý softvér navrhnutý špeciálne na poškodenie alebo narušenie systému, ktorý ohrozuje dôvernosť, integritu a/alebo dostupnosť Poznámka 1 k heslu: Príkladmi škodlivého softvéru sú vírusy a trójski kone. [ZDROJ: ISO/IEC 27033-1:2015, 3.22]

Termín	Definícia
systém manažérstva	súbor vzájomne prepojených alebo vzájomne pôsobiacich prvkov organizácie na stanovenie politík a cieľov a procesov na dosiahnutie týchto cieľov Poznámka 1 k heslu: Systém manažérstva sa môže týkať jednej alebo viacerých disciplín. Poznámka 2 k pojmu: Prvky systému zahŕňajú štruktúru organizácie, úlohy a zodpovednosti, plánovanie a prevádzku. Poznámka 3 k heslu: Predmet systému manažérstva môže zahŕňať celú organizáciu, špecifické a identifikované funkcie organizácie, špecifické a identifikované časti organizácie alebo jednu alebo viacero funkcií v rámci skupiny organizácií. [ZDROJ: Z ISO/IEC 27000:2018(en), 3.41]
podstatný	významný pre zamýšľaných používateľov Poznámka 1 k pojmu: Významnosť je pojem, ktorý vyjadruje, že nesprávne údaje, individuálne alebo v súhrne, môžu ovplyvniť spoľahlivosť tvrdenia alebo rozhodnutí zamýšľaného používateľa. Poznámka 2 k heslu: Významnosť môže byť kvalitatívna alebo kvantitatívna. [ZDROJ: Z ISO/IEC 17029:2019, 3.16]
menej závažná nezhoda	nezhoda, ktorá nemá vplyv na schopnosť systému manažérstva dosiahnuť zamýšľané výsledky [ZDROJ: Upravené podľa ISO/IEC 17021-1:2015(en), 3.12]
monitorovanie	určenie stavu systému, procesu alebo činnosti Poznámka 1 k heslu: Na určenie stavu môže byť potrebné vykonávať kontrolu, dohľad alebo kritické pozorovanie. [ZDROJ: ISO/IEC 27000:2018(en), 3.46]
viacfaktorová autentifikácia	autentifikačný mechanizmus pozostávajúci z dvoch alebo viacerých nezávislých kategórií poverení (faktor znalosti, vlastníctva a vlastnosti) na overenie identity používateľa pri prihlásení alebo inej transakcii [ZDROJ: EN 319 401
národná certifikačná schéma kybernetickej bezpečnosti **národná schéma**	komplexný súbor pravidiel, technických požiadaviek, noriem a postupov vypracovaných a prijatých národným verejným orgánom, ktoré sa vzťahujú na certifikáciu alebo posudzovanie zhody produktov IKT, služieb IKT a procesov IKT spadajúcich do predmetu pôsobnosti konkrétneho schému Poznámka 1 k heslu: Táto definícia je spresnením definície certifikačnej schémy. [ZDROJ: Nariadenie (EÚ) 2019/881, 2.10]
národný orgán pre akreditáciu NAB	jediný orgán v členskom štáte, ktorý vykonáva akreditáciu na základe právomoci udelenej štátom [ZDROJ: Nariadenie (ES) č. 765/2008, 2.1]
takmer došlo k incidentu	udalosť, ktorá mohla ohroziť dostupnosť, autentickosť, integritu alebo dôvernosť uložených, prenášaných alebo spracúvaných údajov alebo služieb ponúkaných prostredníctvom sieťových a informačných systémov alebo prostredníctvom nich dostupných, ale ktorej výskytu sa podarilo úspešne zabrániť alebo ku ktorej nedošlo. [ZDROJ: Smernica (EÚ) 2022/2555, článok 6 ods. 5]
nezhoda	nezhoda v kontexte pravidiel a požiadaviek definovaných v certifikačnej schéme Poznámka 1 k heslu: Ide o spresnenie normy ISO 19011, ktorá definuje nesúlad ako nezhodu v kontexte zákonnej alebo regulačnej požiadavky. V tomto prípade je držiavanie (predpisov/zhoda) zhodou v kontexte danej schémy. [ZDROJ: Inšpirované normou ISO 19011:2018(en), 3.7]

nezhoda	nesplnenie požiadavky Poznámka 1 k heslu: keď sa používa v protiklade k nedodržiavaniu, zhoda sa vzťahuje na požiadavky týkajúce sa predmetu posudzovania zhody, a nie na požiadavky týkajúce sa certifikačnej schémy. [ZDROJ: Z ISO/IEC 17021-1:2015, 3.11]
predmet posudzovania zhody **predmet**	subjekt, na ktorý sa vzťahujú určené požiadavky PRÍKLAD: Výrobok, proces, služba, systém, inštalácia, projekt, údaje, návrh, materiál, tvrdenie, osoba, orgán alebo organizácia, alebo akákoľvek ich kombinácia. [ZDROJ: Z ISO/IEC 17000:2020(en), 4.2, poznámka 2]

Termín	Definícia
cieľ	výsledok, ktorý sa má dosiahnuť Poznámka 1 k heslu: Cieľ môže byť strategický, taktický alebo operačný. Poznámka 2 k heslu: Ciele sa môžu týkať rôznych disciplín (napr. finančné, zdravotné a ciele v oblasti ochrany a environmentálne ciele) a môžu sa uplatňovať na rôznych úrovniach [napr. strategická, celopodniková, projektová, produktová a procesná]. Poznámka 3 k heslu: Cieľ môže byť vyjadrený aj inými spôsobmi, napr. ako zamýšľaný výsledok, účel, operačné kritérium, ako cieľ informačnej bezpečnosti alebo použitím iných slov s podobným významom (napr. zámer, cieľ alebo zámer). Poznámka 4 k heslu: V kontexte systémov manažérstva informačnej bezpečnosti stanovuje organizácia ciele informačnej bezpečnosti v súlade s politikou informačnej bezpečnosti s cieľom dosiahnuť konkrétne výsledky. [ZDROJ: Z ISO/IEC 27000:2018(en), 3.49]
cieľový dôkaz **dôkaz**	údaje potvrdzujúce existenciu alebo pravdivosť niečoho Poznámka 1 k heslu: Cieľové dôkazy možno získať pozorovaním, meraním, testovaním alebo inými prostriedkami. Poznámka 2 k heslu: Cieľové dôkazy na účely auditu zvyčajne pozostávajú zo záznamov, vyhlásení o skutočnostiach alebo iných informácií, ktoré sú relevantné pre kritériá auditu a overiteľné. [ZDROJ: Z ISO 9000:2015(en), 3.8.3]
pozorovanie	činnosť spočívajúca v sledovaní procesu alebo postupu vykonávaného inými osobami [ZDROJ: Z IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, vydanie z roku 2017, Slovník pojmov]
pozorovateľ	osoba, ktorá sprevádza audítorský tím, ale nevykonáva audit [ZDROJ: Z ISO/IEC 17021-1:2015(en), 3.9]
režim offline	pokiaľ ide o používanie európskych peňaženiek digitálnej identity, interakcia medzi používateľom a treťou stranou na fyzickom mieste s využitím technológií blízkej blízkosti, pri ktorej sa na účely interakcie nevyžaduje, aby európska peňaženka digitálnej identity pristupovala k vzdialeným systémom prostredníctvom elektronických komunikačných sietí [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 57]
prevádzková účinnosť	Opatrenie funguje efektívne, ak (i) bola počas stanoveného obdobia dôsledne uplatňovaná tak, ako bola navrhnutá, a (ii) v prípade manuálnych opatrení boli uplatňované osobami, ktoré majú primeranú spôsobilosť a oprávnenie. [ZDROJ: Inšpirované normou ISAE 3402]
prevádzková požiadavka	požiadavka, ktorá sa priamo týka prevádzky služby, špecifikovaná v normách alebo v iných normatívnych dokumentoch určených certifikačnou schémou [ZDROJ: Inšpirované normou ISO/IEC 17065:2012(en), 3.8]
prevádzkové riziko	Riziko vyplývajúce z vykonávania obchodných činností spoločnosti
organizácia	osoba alebo skupina osôb, ktorá má svoje vlastné funkcie so zodpovednosťami, právomocami a vzťahmi na dosiahnutie svojich cieľov Poznámka 1 k pojmu: Pojem organizácia zahŕňa, ale nie je obmedzený na, živnostníka, spoločnosť, korporáciu, firmu, podnik, orgán, partnerstvo, charitatívnu organizáciu alebo inštitúciu, alebo ich časť či kombináciu, bez ohľadu na to, či sú zaregistrované alebo nie, verejné alebo súkromné. [ZDROJ: Z ISO/IEC 27000:2018(en), 3.50]

výstup	výsledok procesu Poznámka 1 k heslu: To, či je výstupom organizácie produkt alebo služba, závisí od prevahy príslušných charakteristík, napr. obraz na predaj v galérii je produkt, zatiaľ čo dodanie obrazu na objednávku je služba, hamburger zakúpený v maloobchodnej predajni je produkt, zatiaľ čo prijatie objednávky a podanie hamburgeru objednaného v reštaurácii je súčasťou služby. [ZDROJ: Z ISO 9000:2015(en), 5.6]
outsourcing	získavanie služieb (s produktmi alebo bez nich) na podporu podnikovej funkcie s cieľom vykonávať činnosti s využitím zdrojov dodávateľa namiesto zdrojov nadobúdateľa Poznámka 1 k heslu: Na účely tohto dokumentu sa pojmy „outsourcing“ a „subdodávanie“ považujú za synonymá. [ZDROJ: Z ISO/IEC 27036-1:2015, 3.6] [ZDROJ Poznámka 1: Z ISO/IEC 17065:2012(en), $ 6.2.2.1]

Termín	Definícia
vzájomné hodnotenie	hodnotenie orgánu vo vzťahu k určeným požiadavkám zástupcami iných orgánov v dohodovej skupine alebo kandidátmi na členstvo v nej Poznámka 1 k heslu: Toto heslo nie je uspokojivé z viacerých dôvodov, a to najmä preto, že odkazuje na pojmy, ktoré nie sú v súčasnosti definované (dohodová skupina) a pre nás nemajú veľký význam, a tiež spomína „orgán“, čo je nejasné. Poznámka 2 k heslu: Na druhej strane by to mohlo zahŕňať aj CAB na úrovni „vysokej“ aj NCCA, ale je potrebné to preformulovať. [ZDROJ: Z ISO/IEC 17000:2020(en), 4.5]
penetračné skúšanie	Autorizovaný simulovaný kybernetický útok na počítačový systém, vykonaný s cieľom vyhodnotiť bezpečnosť systému. [ZDROJ: ENISA, NIST SP 800-115]
trvalé údaje	dáta, ktoré sú uchovávané v informačnom systéme dlhšie ako jednu reláciu správy dát [ZDROJ: Z ISO/IEC TR 10032: 2003(en), 2.54]
identifikačné údaje osoby	súbor údajov, ktorý sa vydáva v súlade s právom Únie alebo vnútroštátnym právom a ktorý umožňuje zistiť totožnosť fyzickej alebo právnickej osoby, alebo fyzickej osoby zastupujúcej inú fyzickú osobu alebo právnickú osobu [ZDROJ: Nariadenie (EÚ) č. 910/2014, článok 3 ods. 3]
personál	osoby vykonávajúce prácu pod vedením CSP Poznámka 1 k heslu: Pojem personál zahŕňa členov CSP, ako sú riadiaci orgán, vrcholový manažment, zamestnanci, dočasní zamestnanci, dodávatelia a dobrovoľníci. [ZDROJ: Upravené podľa ISO/IEC 27002:2022, 3.1.20]
kontaktná osoba	definovaná organizačná funkcia alebo úloha slúžiaca ako koordinátor alebo kontaktný bod pre informácie týkajúce sa činností riadenia incidentov [ZDROJ: Z ISO/IEC 27035-1:2023, 3.1.10]
politika	zámery a smerovanie organizácie, formálne vyjadrené jej vrcholovým manažmentom [ZDROJ: Z ISO/IEC 27000:2018(en), 3.53]
predprodukčné prostredie	Zrkadlo produkčného prostredia používané na záverečné skúšanie alebo odstraňovanie chýb
preventívne opatrenie	Vnútorné opatrenie, ktoré sa používa na zabránenie nežiaducim udalostiam, chybám a iným javom, o ktorých podnik usúdil, že by mohli mať negatívny podstatný vplyv na proces alebo konečný produkt [ZDROJ: SOC2]
postup	špecifikovaný spôsob vykonávania činnosti alebo procesu Poznámka 1 k heslu: V tomto kontexte je proces definovaný ako súbor vzájomne súvisiacich alebo vzájomne pôsobiacich činností, ktoré využívajú vstupy na dosiahnutie zamýšľaného výsledku. [ZDROJ: Z ISO/IEC 17000:2020(en), 5.2]
proces	súbor vzájomne súvisiacich alebo vzájomne pôsobiacich činností, ktoré transformujú vstupy na výstupy [ZDROJ: Z doplnku ISO: 3.12]

výrobok	výsledok procesu Poznámka 1 k heslu: V norme ISO 9000:2005 sú uvedené štyri všeobecné kategórie produktov: — služby (napr. doprava) (pozri definíciu v 3.6); — softvér (napr. počítačový program, slovník); — hardvér (napr. motor, mechanická súčiastka); — spracované materiály (napr. mazivo). Mnohé výrobky obsahujú prvky, ktoré patria do rôznych všeobecných kategórií výrobkov. To, či sa výrobok nazýva služba, softvér, hardvér alebo spracovaný materiál, závisí od dominantného prvku. Poznámka 2 k heslu: Výrobky zahŕňajú výsledky prírodných procesov, ako je rast rastlín a tvorba iných prírodných zdrojov. Poznámka 3 k heslu: Upravené podľa ISO/IEC 17000:2004, definícia 3.3. [ZDROJ: Z ISO/IEC 17065:2012(en), 3.4]
výrobné prostredie	Prostredie, ktoré slúži zákazníkom

Termín	Definícia
kvalifikované elektronické osvedčenie atribútov	elektronické osvedčenie atribútov, ktoré vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a ktoré spĺňa požiadavky stanovené v prílohe V k nariadeniu eIDAS [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 45]
kvalifikovaný elektronický podpis	pokročilý elektronický podpis, ktorý je vytvorený kvalifikovaným zariadením na vytváranie elektronických podpisov a ktorý je založený na kvalifikovanom certifikáte pre elektronické podpisy [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 12]
kvalifikovaná dôveryhodná služba	dôveryhodná služba, ktorá spĺňa príslušné požiadavky stanovené v nariadení eIDAS [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 17]
poskytovateľ kvalifikovaných dôveryhodných služieb	poskytovateľ dôveryhodných služieb, ktorý poskytuje jednu alebo viacero kvalifikovaných dôveryhodných služieb a ktorému dozorný orgán udelil status kvalifikovaného poskytovateľa [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 20]
primeraná záruka	typ uistenia, pri ktorom sú povaha a rozsah hodnotiacich činností navrhnuté tak, aby poskytovali vysoký, ale nie absolútny úroveň záruky. Poznámka 1 k heslu: Záver hodnotiteľa je vyjadrený formou, ktorá vyjadruje názor hodnotiteľa na výsledok hodnotenia predmetu hodnotenia na základe uplatniteľných kritérií. Poznámka 2 k záznamu: Záver hodnotiteľa v prípade úlohy s primeranou istotou je formulovaný v pozitívnom zmysle, napríklad: „Na základe vykonaných činností sa podľa nášho názoru cloudová služba XYZ spĺňa certifikačné požiadavky **dokumentu Error! Unknown** na úrovni hodnotenia LLL.“ [ZDROJ: Inšpirované normou ISO 14064-3:2019, 3.6.6]
spoliehajúca sa strana	fyzická alebo právnická osoba, ktorá sa spolieha na elektronickú identifikáciu alebo dôveryhodnú službu [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 6]
opätovné vykonanie	Nezávislé vykonanie postupov alebo opatrení audítorom, ktoré boli pôvodne vykonané v rámci vnútorných kontrol zákazníka [ZDROJ: Z príručky IAASB o medzinárodnej kontrole kvality, audite, revízii, iných zárukách a súvisiacich službách, vydanie z roku 2017, slovník pojmov]
požiadavka	potreba alebo očakávanie, ktoré je uvedené, všeobecne implikované alebo povinné Poznámka 1 k heslu: „Všeobecne implikovaná“ znamená, že je zvykom alebo bežnou praxou pre organizáciu a zainteresované strany, že daná potreba alebo očakávanie je implikované. Poznámka 2 k heslu: Určená požiadavka je taká, ktorá je uvedená, napríklad v zdokumentovaných informáciách. Poznámka 3 k heslu: Kvalifikátor sa môže použiť na označenie konkrétneho typu požiadavky, napr. požiadavka na výrobok, požiadavka na službu, požiadavka zákazníka. [ZDROJ: Z ISO/IEC 27000:2018(en), 3.56]
zvyškové riziko	riziko zostávajúce po ošetrení rizika Poznámka 1 k heslu: Zvyškové riziko môže obsahovať neidentifikované riziko. Poznámka 2 k heslu: Zvyškové riziko sa môže tiež označovať ako „zachované riziko“. [ZDROJ: Z ISO Guide73:2009(en), 3.8.1.6]
obnovenie	obnovenie úplného alebo čiastočného vyhlásenia o zhode [ZDROJ: Z ISO/IEC 17000:2020(en), 8.5]

posúdenie	určenie vhodnosti, primeranosti alebo účinnosti objektu na dosiahnutie stanovených cieľov PRÍKLAD: Preskúmanie manažmentom, prehľad návrhu a vývoja, prehľad požiadaviek zákazníka, prehľad nápravných opatrení a vzájomný prehľad. Poznámka 1 k heslu: Preskúmanie môže zahŕňať aj stanovenie efektívnosti. [ZDROJ: Z EN ISO 9000:2015, 3.11.2]
preskúmanie	<CERTIFIKÁCIA> posúdenie vhodnosti, primeranosti a účinnosti činností výberu a určovania, ako aj výsledkov týchto činností, so zreteľom na splnenie určených požiadaviek predmetom posudzovania zhody [ZDROJ: Z ISO/IEC 17000:2020(en), 7.1]

Termín	Definícia
správa o preskúmaní	dokument vypracovaný CAB po vykonaní preskúmania hodnotenia vykonaného audítorským tímom
riziko	vplyv neistoty na ciele Poznámka 1 k heslu: Vplyv je odchýlka od očakávaného – pozitívna a/alebo negatívna. Poznámka 2 k heslu: Ciele môžu mať rôzne aspekty (napríklad finančné, zdravotné a opatrenia na ochranu a environmentálne ciele) a môžu sa uplatňovať na rôznych úrovniach (napríklad strategická, celopodniková, projektová, produktová a procesná). Poznámka 3 k heslu: Riziko sa často charakterizuje odkazom na potenciálne udalosti a dôsledky alebo ich kombináciu. Poznámka 4 k heslu: Riziko sa často vyjadruje ako kombinácia dôsledkov udalosti (vrátane zmien okolností) a súvisiacej pravdepodobnosti výskytu. Poznámka 5 k heslu: Neistota je stav, aj čiastočný, nedostatku informácií týkajúcich sa udalosti, jej dôsledkov alebo pravdepodobnosti, alebo nedostatku ich pochopenia či poznania. [ZDROJ: Z ISO 31073:2022(en), 3.1.1]
analýza rizík	proces na pochopenie povahy rizika a stanovenie úrovne rizika Poznámka 1 k heslu: Analýza rizika poskytuje základ pre hodnotenie rizika a rozhodnutia o ošetrení rizika. Poznámka 2 k heslu: Analýza rizika zahŕňa odhad rizika. [ZDROJ: Z ISO 31073:2022(en), 3.3.1]
posúdenie rizika	celkový proces identifikácie rizík, analýzy rizík a hodnotenia rizík [ZDROJ: Z ISO 31073:2022(en), 3.3.8]
hodnotenie rizika	proces porovnávania výsledkov analýzy rizík s kritériami rizík s cieľom určiť, či je riziko a/alebo jeho veľkosť prijateľná alebo tolerovateľná Poznámka 1 k heslu: Hodnotenie rizika pomáha pri rozhodovaní o ošetrení rizika. [ZDROJ: Z ISO 31073:2022(en), 3.3.2]
identifikácia rizika	proces vyhľadávania, rozpoznávania a opisovania rizík Poznámka 1 k heslu: Identifikácia rizika zahŕňa identifikáciu zdrojov rizika, udalostí, ich príčin a potenciálnych dôsledkov. Poznámka 2 k heslu: Identifikácia rizík môže zahŕňať historické údaje, teoretickú analýzu, informované a odborné stanoviská a potreby zainteresovaných strán. [ZDROJ: Z ISO 31073:2022(en), 3.3.9]
riadenie rizík	koordinované činnosti zamerané na riadenie a kontrolu organizácie s ohľadom na riziko [ZDROJ: Z ISO 31073:2022(en), 3.2.1]
riziko významného nesprávneho uvedenia	Riziko, že informácie o predmete auditu budú pred začatím audítorskej činnosti významne nesprávne uvedené [ZDROJ: Z ISAE 3000: 12.w]
vlastník rizika	osoba alebo subjekt, ktorý má zodpovednosť a právomoc riadiť riziko [ZDROJ: Z ISO 31073:2022(en), 3.3.14]

ošetrenie rizika	proces na úpravu rizika (1.1) Poznámka 1 k heslu: Ošetrenie rizika môže zahŕňať: • vyhnutie sa riziku rozhodnutím nezačať alebo nepokračovať v činnosti, ktorá riziko spôsobuje; • prijatie alebo zvýšenie rizika s cieľom využiť príležitosť; • odstránenie zdroja rizika; • zmenu pravdepodobnosti; • zmenu dôsledkov; • zdieľanie rizika s inou stranou alebo stranami [vrátane zmlúv a financovania rizika]; a • zachovanie rizika na základe informovaného rozhodnutia. Poznámka 2 k položke: Ošetrenie rizika, ktoré sa zaoberá negatívnymi dôsledkami, sa niekedy označuje ako „zmierňovanie rizika“, „odstraňovanie rizika“, „prevencia rizika“ a „znižovanie rizika“. Poznámka 3 k heslu: Ošetrenie rizika môže vytvoriť nové riziká alebo zmeniť existujúce riziká. [ZDROJ: Z ISO 31073:2022(en), 3.3.32]

Termín	Definícia
úloha	súbor činností, ktoré slúžia spoločnému účelu [ZDROJ: Z ISO/IEC 22123-1:2023(en), 3.3.10]
Riadenie prístupov na základe rolí RBAC	Bezpečnostná technika overovania, ktorá autorizuje operácie alebo umožňuje prístup k zdrojom na základe identity používateľa a jeho vzťahu k iným používateľom a subjektom PRÍKLAD 1: Učiteľ má prístup na čítanie/zapisovanie k známkam svojich žiakov (rola: „učiteľ žiaka“), ale nemá prístup k známkam iných žiakov PRÍKLAD 2: Dotknutá osoba má prístup len na čítanie k známkam všetkých žiakov svojich učiteľov (rola: „riaditeľ učiteľov žiakov“), ale dotknutá osoba nemá povolenie meniť žiadne známky [ZDROJ: Z ISO/IEC 20944-1:2013(en), 3.21.20.2]
odber vzoriek	výber a/alebo zber materiálu alebo údajov týkajúcich sa predmetu posudzovania zhody Poznámka 1 k heslu: Výber môže byť na základe postupu, automatizovaného systému, odborného posúdenia atď. Poznámka 2 k heslu: Výber a zber môžu vykonávať rovnaké alebo rôzne osoby alebo organizácie. [ZDROJ: Z ISO/IEC 17000:2020(en), 6.1]
predmet certifikácie	identifikácia — služby (služieb), pre ktoré sa certifikácia udeľuje, — príslušná certifikačná schéma a možnosti schémy, a — normy a iné normatívne dokumenty, vrátane dátumu ich uverejnenia, s ktorými sa služba (služby) považuje (považujú) za zhodnú (zhodné) Poznámka k záznamu: Definícia bola zmenená tak, aby zahŕňala „možnosti schémy“, ktoré môžu v kontexte EUCS zahŕňať najmä vybranú úroveň hodnotenia a profily rozšírenia. [ZDROJ: Upravené podľa ISO/IEC 17065:2012(en), 3.10]
bezpečnostná zóna	oblasť ohraničená bezpečnostnými perimetermi, v rámci ktorej nie je prístup riadený
záruka bezpečnosti	dôvody pre oprávnenú istotu, že tvrdenie o splnení bezpečnostných cieľov bolo alebo bude dosiahnuté [ZDROJ: Z ISO/IEC/IEEE 15026-1(2019):3.4]
bezpečnostný perimeter	fyzická hranica obklopujúca miesta, kde sa nachádza zariadenie a personál CSP, do ktorých je prístup riadený
bezpečnostný problém	vyhlásenie, ktoré formálnym spôsobom definuje povahu a rozsah bezpečnosti, ktorú má predmet posudzovania zhody riešiť Poznámka 1 k heslu: Toto vyhlásenie pozostáva z kombinácie: — hrozieb, ktorým má predmet posudzovania zhody čeliť, — OSP vynucovaných predmetom posudzovania zhody a — predpokladov, ktoré platia pre predmet posudzovania zhody a jeho prevádzkové prostredie. [ZDROJ: Upravené podľa ISO/IEC 15408-1:2009(en), 3.1.61]
bezpečnostná zóna	oblasť siete, v ktorej je povolená obmedzená výmena údajov s oblasťami mimo nej [ZDROJ: Z ISO/TR 11636:2009(en), 2.13]
výber	plánovacie a prípravné činnosti s cieľom zhromaždiť alebo vypracovať všetky informácie a vstupné údaje potrebné na následné stanovenie funkcia Poznámka 1 k heslu: Činnosti výberu sa veľmi líšia počtom a zložitosťou. V niektorých prípadoch môže byť potrebná len veľmi malá činnosť výberu. [ZDROJ: Z ISO/IEC 17000:2020(en), A.2.1]

služba	výstup organizácie, pri ktorom sa nevyhnutne vykonáva aspoň jedna činnosť medzi organizáciou a zákazníkom Poznámka 1 k heslu: Táto definícia z normy ISO 9000 odráža definíciu produktu a je spresnená do pojmu informačná služba podľa európskeho nariadenia 1535/2015. [ZDROJ: Z ISO 9000:2000, 3.7.7]

Termín	Definícia
požiadavka na službu	požiadavka, ktorá sa priamo týka služby, špecifikovaná v normách alebo v iných normatívnych dokumentoch určených certifikačnou schémou [ZDROJ: Upravené podľa ISO/IEC 17065:2012(en), 3.8]
určená požiadavka	potreba alebo očakávanie, ktoré je uvedené Poznámka 1 k heslu: Určené požiadavky môžu byť uvedené v normatívnych dokumentoch, ako sú nariadenia, normy a technické špecifikácie. Poznámka 2 k heslu: Určené požiadavky môžu byť podrobné alebo všeobecné Poznámka 3 k heslu: V kontexte európskej certifikačnej schémy kybernetickej bezpečnosti sú určené požiadavky zvyčajne rovnaké ako požiadavky špecifikované v schéme, buď priamo, alebo nepriamo (v normatívnych dokumentoch, na ktoré sa schéma odvoláva). [ZDROJ: Z ISO/IEC 17000:2020(en), 5.1]
Skupina zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti **SCCG**	Poradná skupina zložená z členov vybraných spomedzi uznávaných odborníkov zastupujúcich príslušné zainteresované strany [ZDROJ: Upravené podľa zákona o kybernetickej bezpečnosti, článok 22]
najnovší	v danom čase najvyspelejšia úroveň technických schopností v oblasti výrobkov, procesov a služieb, založená na relevantných konsolidovaných poznatkoch vedy, techniky a skúseností Poznámka 1 k heslu: Najnovší stav techniky predstavuje to, čo je v súčasnosti a všeobecne prijaté ako osvedčená prax v oblasti technológie a medicíny. Najnovší stav techniky nemusí nutne znamenať technologicky najpokročilejšie riešenie. Najnovší stav techniky opísaný v tomto texte sa niekedy označuje ako „všeobecne uznávaný najnovší stav techniky“. [ZDROJ: Z ISO/IEC Guide 63:2019, 3.18]
dokument o najnovšom stave techniky	dokument, ktorý špecifikuje metódy, techniky a nástroje hodnotenia, ktoré sa vzťahujú na certifikáciu cloudových služieb, alebo bezpečnostné požiadavky na všeobecnú kategóriu cloudových služieb, alebo akékoľvek iné požiadavky potrebné na certifikáciu, s cieľom harmonizovať hodnotenie [ZDROJ: Upravené podľa (EÚ) 2024/482 (EUCC), článok (2)(14)]
stratégia	plánované činnosti na dosiahnutie dlhodobého alebo celkového cieľa [ZDROJ: ISO 9000:2015, 3.5.12]
silný	ťažko poraziteľný, s nadpriemernou alebo neočakávanou silou alebo mocou, schopný odolať útoku alebo pevne postavený [ZDROJ: Z ISO/IEC 19790:2012, 3.123]
silné overenie používateľa	overenie založené na použití najmenej dvoch overovacích faktorov z rôznych kategórií, a to buď znalosti (niečo, čo vie len používateľ), vlastníctva (niečo, čo vlastní len používateľ) alebo vlastnosti (niečo, čím používateľ je), ktoré sú nezávislé v tom zmysle, že porušenie jedného z nich neohrozuje spoľahlivosť ostatných, a ktoré je navrhnuté tak, aby chránilo dôvernosť overovacích údajov [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 51]
subsystém	súbor prvkov, ktorý je sám osebe systémom a súčasťou väčšieho systému [ZDROJ: Wikipédia]
dostatočnosť dôkazov	Miera množstva dôkazov [ZDROJ: Z ISAE3000: 12.i.i]

doplňujúce informácie o kybernetickej bezpečnosti	Informácie týkajúce sa kybernetickej bezpečnosti, ktoré majú byť dostupné pre každého výrobcu alebo poskytovateľa certifikovaných produktov IKT, služieb IKT alebo procesov IKT, alebo produktov IKT, služieb IKT a procesov IKT, pre ktorá má byť vydané prehlásenie o zhodeEÚ POZNÁMKA: Informácie zahŕňajú usmernenia a odporúčania, obdobie, počas ktorého bude poskytovaná bezpečnostná podpora, kontaktné informácie na prijímanie informácií o zraniteľnostiach a odkaz na online repozitáre, v ktorých sú uvedené zraniteľnosti. [Z nariadenia (EÚ) 2019/881, článok 55]
dodávateľ	organizácia alebo fyzická osoba, ktorá uzatvára zmluvu s nadobúdateľom o dodávke produktu alebo služby Poznámka 1 k heslu: Medzi ďalšie bežne používané výrazy pre dodávateľa patria zmluvný partner, výrobca, predajca alebo dodávateľ. Poznámka 2 k heslu: termín „poskytovateľ služieb“ sa v tomto schéme zvyčajne používa pre dodávateľov služieb Poznámka 3 k heslu: V protiklade k pojmu „poskytovateľ služieb“ sa pojem „dodávateľ“ vzťahuje na dodávateľa výrobkov [ZDROJ: Upravené podľa ISO/IEC 27036:1-2014, 3.9]

Termín	Definícia
podpora	súbor činností potrebných na zabezpečenie toho, aby prevádzkový systém alebo komponent spĺňal svoje pôvodné požiadavky a akékoľvek následné úpravy týchto požiadaviek. POZNÁMKA: Príklady zahŕňajú údržbu softvéru alebo hardvéru, trénovanie používateľov. [ZDROJ: Z ISO/IEC/IEEE 24756:2017, 3.4054]
dohľad	systematické opakovanie činností posudzovania zhody ako základ pre zachovanie platnosti vyhlásenia o zhode Poznámka 1 k heslu: Možno nebudeme chcieť tento termín zachovať kvôli možnej zámene s dohľadom nad trhom, ale zatiaľ ho ponecháme, pretože tento pojem musí byť nejakým termínom vyjadrený. [ZDROJ: Z ISO/IEC 17000:2020(en), 8.1]
pozastavenie	dočasné obmedzenie vyhlásenia o zhode orgánom, ktorý vyhlásenie vydal, pre celý alebo časť predmetu osvedčenia [ZDROJ: Z ISO/IEC 17000:2020(en), 8.2]
systém	Samostatný celok, ktorý pozostáva z viacerých vzájomne pôsobiacich častí tak, že odstránenie alebo zlyhanie jednej časti môže spôsobiť nefunkčnosť celého celku [ZDROJ: Z www.oxfordreference.com]
systémová zložka	funkčná zložka potrebná na zabezpečenie informačnej bezpečnosti v rámci cloudovej služby počas vytvárania, spracovávania, ukladania, prenosu, vymazania alebo zničenia informácií v oblasti zodpovednosti poskytovateľa cloudovej služby POZNÁMKA: Súčasti systému môžu zahŕňať softvér, hardvér alebo oboje. PRÍKLADY: firewally, vyvažovače zaťaženia, webové servery, aplikačné servery, databázové servery. [Zdroj: Upravené podľa C5:2020]
technický expert	osoba, ktorá poskytuje audítorskému tímu špecifické znalosti alebo odborné znalosti [ZDROJ: Z ISO/IEC 17021-1:2015(en), 3.14]
nájomca	jeden alebo viacerí používatelia cloudových služieb, ktorí zdieľajú prístup k súboru fyzických a virtuálnych zdrojov [ZDROJ: Z ISO/IEC 22123-1:2023(en), 3.4.2]
testovacie prostredie	Prostredie, v ktorom sa skúša nový a zmenený kód
skúšanie	<vývoj>činnosť, pri ktorej sa systém alebo komponent spúšťa za špecifikovaných podmienok, výsledky sa pozorujú alebo zaznamenávajú a vykonáva sa hodnotenie niektorých aspektov systému alebo komponentu [ZDROJ: IEEE Std 610.12-1990]
skúšanie	<POSUDZOVANIE zhody>určenie jednej alebo viacerých charakteristík predmetu posudzovania zhody podľa postupu Poznámka 1 k heslu: Postup môže byť určený na riadenie premenných v rámci skúšania ako príspevok k presnosti alebo spoľahlivosti výsledkov. Poznámka 2 k heslu: Výsledky skúšania môžu byť vyjadrené v špecifikovaných jednotkách alebo cieľovým porovnaním s dohodnutými referenciami. Poznámka 3 k heslu: Výstup skúšania môže obsahovať komentáre (napr. názory a interpretácie) o výsledkoch skúšania a splnení určených požiadaviek. [ZDROJ: Z ISO/IEC 17000:2020(en), 6.2]
tretia strana	osoba alebo orgán, ktorý je nezávislý od osoby alebo organizácie, ktorá poskytuje predmet posudzovania zhody, a od záujmov používateľov týkajúcich sa tohto predmetu [ZDROJ: Z ISO/IEC 17000:2020(en), 2.2]
činnosť posudzovania zhody treťou stranou	činnosť posudzovania zhody, ktorú vykonáva osoba alebo organizácia, ktorá je nezávislá od poskytovateľa predmetu posudzovania zhody a nemá žiadny záujem používateľa na tomto predmete

	[ZDROJ: Z ISO/IEC 17000:2020(en), 4.5]

Termín	Definícia
hrozba	potenciálna príčina nežiaducej udalosti, ktorá môže spôsobiť poškodenie systému alebo organizácie [ZDROJ: Z ISO/IEC 27000:2018, 3.74]
vrcholový manažment	osoba alebo skupina osôb, ktorá riadi a kontroluje organizáciu na najvyššej úrovni Poznámka 1 k heslu: Vrcholový manažment má právomoc delegovať právomoci a poskytovať zdroje v rámci organizácie. Poznámka 2 k heslu: Ak predmet systému manažérstva vzťahuje sa len na časť organizácie, vrcholový manažment sa vzťahuje na tých, ktorí riadia a riadia túto časť organizácie. [ZDROJ: Dodatok ISO: 3.5]
dôveryhodná služba	elektronická služba, ktorá sa zvyčajne poskytuje za odmenu a pozostáva z: (a) vydávania certifikátov pre elektronické podpisy, certifikátov pre elektronické pečate, certifikátov pre overovanie webových stránok alebo certifikátov pre poskytovanie iných dôveryhodných služieb; (b) validácia certifikátov pre elektronické podpisy, certifikátov pre elektronické pečate, certifikátov pre overovanie webových stránok alebo certifikátov pre poskytovanie iných dôveryhodných služieb; (c) vytvárania elektronických podpisov alebo elektronických pečiatok; (d) validácia elektronických podpisov alebo elektronických pečiatok; (e) uchovávania elektronických podpisov, elektronických pečiatok, certifikátov pre elektronické podpisy alebo certifikátov pre elektronické pečiatky; (f) správa zariadení na vytváranie elektronických podpisov na diaľku alebo zariadení na vytváranie elektronických pečiatok na diaľku; (g) vydávanie elektronických osvedčení o atribútoch; (h) validácia elektronických osvedčení o atribútoch; (i) vytváranie elektronických časových pečiatok; (j) validácia elektronických časových pečiatok; (k) poskytovanie služieb elektronického doručenia s potvrdením o doručení; (l) validácia údajov prenášaných prostredníctvom služieb elektronického doručenia s doručenkovým potvrdením a súvisiacich dôkazov; (m) elektronická archivácia elektronických údajov a elektronických dokumentov; (n) zaznamenávanie elektronických údajov do elektronickej knihy; [ZDROJ: Nariadenie (EÚ) č. 910/2014, článok 3 ods. 16]
poskytovateľ dôveryhodných služieb	fyzická alebo právnická osoba, ktorá poskytuje jednu alebo viaceré dôveryhodné služby buď ako kvalifikovaný, alebo ako nekvalifikovaný poskytovateľ dôveryhodných služieb [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 19]
tunel	dátová cesta medzi sieťovými zariadeniami, ktorá je vytvorená cez existujúcu sieťovú infraštruktúru Poznámka 1 k heslu: Tunely možno vytvoriť pomocou techník, ako je zapuzdrenie protokolu, prepínanie štítkov alebo virtuálne okruhy [ZDROJ: Z ISO/IEC 27033-1:2015(en), 3.40]
podnik	subjekty vykonávajúce hospodársku činnosť bez ohľadu na ich právny status a spôsob financovania, vrátane všetkých prepojených podnikov alebo pridružených podnikov, ktoré tvoria skupinu prostredníctvom priamej alebo nepriamej riaditeľskej činnosti jedného podniku alebo podniku nad druhým. [ZDROJ: Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/1925 zo 14. septembra 2022 o súťažných a spravodlivých trhoch v digitálnom sektore a o zmene a doplnení smerníc (EÚ) 2019/1937 a (EÚ) 2020/1828 (zákon o digitálnych trhoch), článok 2 ods. 27]]

užívateľ	fyzická alebo právnická osoba, alebo fyzická osoba zastupujúca inú fyzickú alebo právnickú osobu, ktorá využíva dôveryhodné služby alebo prostriedky elektronickej identifikácie poskytované v súlade s nariadením eIDAS [ZDROJ: Nariadenie (EÚ) č. 910/2014, článok 3 ods. 5a]
zariadenie používateľa	opatrenie na riadenie používateľa peňaženky, ktoré sa používa na podporu prevádzky jednotky peňaženky POZNÁMKA 1: Zariadením používateľa môže byť zariadenie, na ktorom beží aplikácia používateľského rozhrania peňaženky, a to ako samostatná aplikácia alebo ako prehliadač POZNÁMKA 2: Zariadenie používateľa sa môže používať ako základ overovania prostredníctvom dôkazu o vlastníctve POZNÁMKA 3: Používateľ peňaženky môže na podporu jednotky peňaženky používať jedno alebo viacero používateľských zariadení

Termín	Definícia
užívateľské prostredie	časť jednotky peňaženky, ktorá je umiestnená vo vzdialenom prostredí poskytovateľa peňaženky POZNÁMKA: Hoci sú všetky používateľské prostredia súčasťou toho istého vzdialeného prostredia, používateľ má prístup len k svojmu vlastnému používateľskému prostrediu
validácia	[posudzovanie zhody] potvrdenie pravdepodobnosti pre konkrétne zamýšľané použitie alebo aplikáciu prostredníctvom poskytnutia objektívnych dôkazov, že boli splnené určené požiadavky (5.1) Poznámka 1 k heslu: Validácia sa môže uplatniť na tvrdenia s cieľom potvrdiť informácie uvedené v tvrdení týkajúce sa zamýšľaného budúceho použitia. [ZDROJ: Z ISO/IEC 17000:2020(en), 6.5]
validácia	[eIDAS] proces validácie a potvrdzovania, že údaje v elektronickej forme sú platné v súlade s nariadením eIDAS [ZDROJ: Z nariadenia (EÚ) č. 910/2014, článok 3 ods. 41]
verifikácia	potvrdenie pravdivosti prostredníctvom poskytnutia objektívnych dôkazov, že boli splnené určené požiadavky (5.1) Poznámka 1 k heslu: Verifikácia sa môže uplatniť na tvrdenia s cieľom potvrdiť informácie uvedené v tvrdení týkajúce sa udalostí, ktoré sa už stali, alebo výsledkov, ktoré už boli dosiahnuté. [ZDROJ: Z ISO/IEC 17000:2020(en), 6.6]
kontrola verzií	vytvorenie a udržiavanie referenčných stavov a identifikácia a opatrenia na riadenie zmien referenčných stavov, ktoré umožňujú návrat k predchádzajúcemu referenčnému stavu [ZDROJ: Z ISO/IEC/IEEE 24765:2017(en), 3.4546]
zraniteľnosť	slabina aktíva alebo opatrenia, ktorú môže využiť jedna alebo viacero hrozieb [ZDROJ: Z ISO/IEC 27000:2018(en), 2018, 3.77]
inštancia peňaženky	aplikácia nainštalovaná a nakonfigurovaná na zariadení alebo v prostredí používateľa peňaženky, ktorá je súčasťou jednotky peňaženky a ktorú používateľ peňaženky používa na interakciu s jednotkou peňaženky POZNÁMKA: inštancia peňaženky je inštancia jednej alebo viacerých aplikácií používateľského rozhrania peňaženky, prípadne rozdelená medzi zariadenie používateľa peňaženky a vzdialené prostredie poskytovateľa peňaženky [ZDROJ: Z nariadenia CIR (EÚ) 2024/2981 (EUDIF IA), článok 2 ods. 5, doplnená poznámka]
poskytovateľ peňaženky	fyzická alebo právnická osoba, ktorá poskytuje riešenia peňaženky POZNÁMKA: Vzhľadom na zložitú povahu riešenia peňaženky poskytovateľ peňaženky vyrába alebo obstaráva hardvér a softvér pre riešenie peňaženky, spravuje ich konfigurácie alebo nastavenia a sprístupňuje ich používateľom peňaženky. Poskytovateľ peňaženky tiež poskytuje služby z riešenia peňaženky a prevádzkuje procesy potrebné na správu jednotiek peňaženky. [ZDROJ: Z nariadenia (EÚ) 2024/2981 (EUDIF IA), článok 2 ods. 8]
bezpečná kryptografická aplikácia peňaženky **WSCA**	aplikácia, ktorá spravuje kritické aktíva prostredníctvom prepojenia s kryptografickými a nekryptografickými funkciami poskytovanými zariadením zabezpečujúcim kryptografiu peňaženky a ich využívaním POZNÁMKA: Bezpečná kryptografická aplikácia peňaženky musí bežať v bezpečnom prostredí, ktorým môže byť bezpečné kryptografické zariadenie peňaženky, iné bezpečné prostredie na zariadení používateľa alebo bezpečné prostredie v backende poskytovateľa peňaženky. [ZDROJ: Z nariadenia (EÚ) 2024/2981 (EUDIF IA), článok 2 ods. 4, doplnená poznámka]
bezpečné kryptografické zariadenie peňaženky **WSCD**	zariadenie odolné proti manipulácii, ktoré poskytuje prostredie prepojené s kryptografickou aplikáciou zabezpečujúcou peňaženku a používané touto aplikáciou na ochranu kritických aktív a poskytovanie kryptografických funkcií na bezpečné vykonávanie kritických operácií [ZDROJ: Z nariadenia (EÚ) 2024/2981 (EUDIF IA), článok 2 ods. 6]

riešenie peňaženky	kombinácia softvéru, hardvéru, služieb, nastavení a konfigurácií, vrátane inštancií peňaženky, jednej alebo viacerých zabezpečených kryptografických aplikácií peňaženky a jedného alebo viacerých zabezpečených kryptografických zariadení peňaženky POZNÁMKA 1: Riešenie peňaženky zahŕňa všetky komponenty peňaženky EUDI, ktoré musia byť certifikované a ktoré môžu byť inštanciované do prostriedku elektronickej identifikácie. POZNÁMKA 2: Riešenie peňaženky bude pravdepodobne zahŕňať niekoľko variantov aplikácií inštancií peňaženky a prípadne aj bezpečných kryptografických aplikácií peňaženky, ktoré budú určené pre rôzne typy užívateľských zariadení. [ZDROJ: Z nariadenia CIR (EÚ) 2024/2981 (EUDIF IA), článok 2 ods. 1, doplnené poznámky]

Termín	Vymedzenie
jednotka peňaženky	jedinečná konfigurácia riešenia peňaženky, ktorá zahŕňa inštancie peňaženky, zabezpečené kryptografické aplikácie peňaženky a zabezpečené kryptografické zariadenia peňaženky poskytované poskytovateľom peňaženky jednotlivému používateľovi peňaženky POZNÁMKA 1: Jednotka peňaženky nezahŕňa časti riešenia peňaženky, ktoré priamo nepodporujú používateľa, a to najmä väčšinu služieb poskytovaných backendom poskytovateľa peňaženky. POZNÁMKA 2: Zabezpečené kryptografické zariadenia peňaženky nemusia byť skutočne poskytnuté používateľovi, keďže môžu byť zahrnuté v zariadení poskytnutom používateľom peňaženky, alebo poskytovateľ peňaženky môže poskytovať iba prístup k vzdialenému zabezpečenému kryptografickému zariadeniu peňaženky zdieľanému s mnohými inými používateľmi. POZNÁMKA 3: Typická jednotka peňaženky bude obsahovať jednu inštanciu peňaženky a bezpečnú kryptografickú aplikáciu peňaženky, vhodnú pre zariadenie používateľa peňaženky. [ZDROJ: Z nariadenia CIR (EÚ) 2024/2981 (EUDIF IA), článok 2 ods. 10, doplnené poznámky]
používateľ peňaženky	užívateľ, ktorý riadi jednotku peňaženky [ZDROJ: Z nariadenia (EÚ) 2024/2981 (EUDIF IA), článok 2 ods. 12]
aplikácia používateľského rozhrania peňaženky, WUIA	aplikácia, ktorá definuje používateľské rozhranie riešenia peňaženky POZNÁMKA 1: Inštancia peňaženky zahŕňa inštanciáciu aplikácie používateľského rozhrania peňaženky. Môže tiež zahŕňať kód na strane servera, ktorý je súčasťou backendu poskytovateľa peňaženky. POZNÁMKA 2: Aplikácia používateľského rozhrania peňaženky môže zahŕňať niekoľko modulov, napríklad modul bežiaci v dôveryhodnom prostredí mobilného zariadenia. PRÍKLADY: Aplikácia používateľského rozhrania peňaženky môže byť natívna mobilná aplikácia bežiaca na mobilnom zariadení alebo webová aplikácia bežiaca v prehliadači.
zrušenie výberu	zrušenie vyhlásenia o zhode orgánom, ktorý vyhlásenie vydal [ZDROJ: Z ISO/IEC 17000:2020(en), 8.3]