NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

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

Názov	Národná certifikačná schéma európskej peňaženky digitálnej identity občana – EUDIW-SK, založená na verzii 0.4.614 kandidátskej schémy EÚ
Označenie	NCS-02
Verzia	v.1.0
Dátum vydania	25.05.2026
Dátum nadobudnutia účinnosti	22.06.2026
Schválil	JUDr. Roman Konečný

Národný bezpečnostný úrad | Budatínska 30 | 851 06 Bratislava | Slovenská republika
tel.: +421 2 6869 1111 | podatelna@nbu.gov.sk | www.nbu.gov.sk

História dokumentu

Dátum	Verzia	Zmena	Autor
3.03.2026	0.1	Vytvorenie na základe národných šablón	NBÚ
3.03.2026	0.2	Vytvorenie na základe národných šablón a schémy kandidátskych krajín EÚ v 03	NBÚ
20.04.2026	03	Aktualizácia zverejneného návrhu kandidátskej schémy EÚ	NBÚ
25.05.2026	1.0	Prvá verzia	NBÚ
8.06.2026	1.0	Preklad do slovenského jazyka	NBÚ

Obsah

ZHRNUTIE (EÚ A SLOVENSKÁ REPUBLIKA) 3

ZÁSADY SCHÉMY (INFORMATÍVNE) 5

PREDHOVOR 10

POČIATOČNÝ KONTEXT SLOVENSKEJ NÁRODNEJ CERTIFIKAČNEJ SCHÉMY PRE PEŇAŽENKY EUDI (INFORMATÍVNY) 11

Počiatočný kontext a pozadie 12

ODKAZY (PÔVODNÁ SCHÉMA EÚ) 28

1. VŠEOBECNÉ POŽIADAVKY (NORMATÍVNE) 31

1.1. Predmet a rozsah pôsobnosti 32
1.2. Vymedzenie pojmov 32
1.3. Úroveň záruky 33
1.4. Vlastné posúdenie zhody 33

2. HODNOTIACE KRITÉRIÁ A METÓDY (NORMATÍVNE) 33

2.1. Hodnotiace kritériá pre služby IKT EUDIW-SK 33
2.2. Metódy hodnotenia služieb IKT v rámci EUDIW-SK 34
2.3. Subdodávanie hodnotiacich činností 35

3. VYDÁVANIE, OBNOVENIE A ODŇATIE CERTIFIKÁTOV EUDIW -SK(NORMATÍVNE) 36

3.1. Informácie potrebné na certifikáciu 36
3.2. Podmienky na vydanie certifikátu EUDIW-SK 37
3.3. Vydanie certifikátu EUDIW-SK 38
3.4. Značka a označenie 39
3.5. Doba platnosti certifikátu EUDIW-SK 39
3.6. Údržba certifikátu EUDIW-SK 40
3.7. Zrušenie certifikátu EUDIW-SK 40

4. ORGÁNY POSUDZOVANIA ZHODY (NORMATÍVNE) 41

4.1. Požiadavky na akreditáciu orgánu posudzovania zhody 41
4.2. Dodatočné alebo osobitné požiadavky na orgán posudzovania zhody 41
4.3. Oznamovanie certifikačných orgánov 41
4.4. Ukončenie činnosti certifikačného orgánu 42

5. MONITOROVANIE DODRŽIAVANIA (NORMATÍVNE) 43

5.1. Monitorovacie činnosti vykonávané NCCA 43
5.2. Monitorovacie činnosti certifikačného orgánu 44
5.3. Monitorovacie činnosti držiteľa certifikátu 44
5.4. Sťažnosti a odvolania 45

6. NEZHODY A NEDODRŽIAVANIE POŽIADAVIEK (NORMATÍVNE) 46

6.1. Dôsledky nezhody certifikovanej služby 46
6.2. Dôsledky nedodržiavania predpisov držiteľom certifikátu 47
6.3. Pozastavenie platnosti certifikátu EUDIW-SK 47
6.4. Dôsledky nedodržiavania povinností certifikačným orgánom 48

7. RIADENIE ZRANITEĽNOSTÍ (NORMATÍVNA) 49

7.1. POSTUPY RIADENIA ZRANITEĽNOSTI 49
7.2. ANALÝZA VPLYVU ZRANITEĽNOSTI 49
7.3. SPRÁVA O ANALÝZE VPLYVU ZRANITEĽNOSTI 50
7.4. ODSTRÁNENIE ZRANITEĽNOSTÍ 51

8. ZVEREJŇOVANIE ZRANITEĽNOSTÍ (NORMATÍVNA) 52

8.1. KOORDINOVANÉ ZVEREJŇOVANIE ZRANITEĽNOSTÍ 52
8.2. INFORMÁCIE POSKYTOVANÉ DOZORNÝM ORGÁNOM 52
8.3. ZVEREJNENIE ZRANITEĽNOSTI 53

9. UCHOVÁVANIE, ZVEREJŇOVANIE A OCHRANA INFORMÁCIÍ (NORMATÍVNE) 53

9.1. UCHOVÁVANIE ZÁZNAMOV ORGÁNMI POSUDZOVANIA ZHODY 53
9.2. INFORMÁCIE DOSTUPNÉ DRŽITEĽOM CERTIFIKÁTU 53
9.3. INFORMÁCIE O DOSTUPNOSTI SPRÍSTUPNENÉ AGENTÚROU ENISA 54
9.4. OCHRANA INFORMÁCIÍ 54

10. VZÁJOMNÉ UZNÁVANIE 54

11. PARTNERSKÉ HODNOTENIE 54

12. POŽIADAVKY NA ÚDRŽBU A KONEČNÉ POŽIADAVKY 54

Zhrnutie (EÚ a Slovenská republika)

1. Tento dokument zavádza európsku certifikačnú schému pre peňaženky európskej digitálnej identity (EUDI). Vychádza z usmernení európskeho rámca certifikácie kybernetickej bezpečnosti, ako je definovaný v nariadení (EÚ) 2019/881 (akt o kybernetickej bezpečnosti).
2. Hoci je táto schéma prezentovaná ako jednotná, je dôležité poznamenať, že certifikácia peňaženky EUDI nebude monolitická. Najkritickejšie hardvérové a softvérové komponenty budú certifikované pomocou schémy EUCC, ostatné softvérové komponenty budú certifikované pomocou iných schém a skúšanie zhody môže vykonávať ešte iné laboratórium. Nakoľko na poskytovateľa peňaženky ako poskytovateľa dôveryhodných služieb sa vzťahuje Smernica NIS 2, tak na IT systémy sa môže využiť systém mananžérstva informačnej bezpečnosti (ISMS, ISO 27001). ISMS
3. Z tohto dôvodu sa certifikačná schéma musí považovať za certifikačný systém v zmysle normy ISO 17067, *t. j.* súbor pravidiel a postupov na riadenie podobných alebo súvisiacich systémov posudzovania zhody. To je zrejmé na národnej úrovni, kde bude certifikácia prispôsobená danej architektúre a presne definuje schémy, ktoré sa majú použiť pre každú zložku.
4. Na európskej úrovni je táto certifikačná schéma opísaná abstraktnejšie než na národnej úrovni. Jej vnútorná logika však zostáva prítomná a prejavuje sa v troch oblastiach.
5. Po prvé, schéma sa môže použiť na certifikáciu kompletného riešenia, ktoré kombinuje riešenie peňaženky a prostriedky elektronickej identifikácie, ale ponúka aj možnosť certifikovať samostatne riešenie peňaženky alebo služby poskytovateľa PID (angl. Person identification data, identifikačné údaje osoby), ktorý peňaženku podporuje.
6. Po druhé, schéma výslovne podporuje kombináciu s inými certifikačnými schémami, vrátane iných európskych schém, ale aj národných a súkromných schém, aspoň tých, ktoré sú založené na akreditáciiSchéma napokon podporuje aj opätovné využitie dôkazov z iných schém posudzovania zhody a vo všeobecnejšom zmysle aj opätovné využitie akýchkoľvek informácií o záruke, napríklad osvedčenia vydaného verejnými audítormi, a to prostredníctvom opätovného využitia analýzy závislostí, ktorá bola zavedená na účely certifikácie cloudových služieb.
7. Nižšie navrhnutá schéma bola koncipovaná ako koordinátor, ktorý poskytuje všeobecné návody pre hodnotenie a certifikáciu služieb poskytujúcich peňaženku EUDI, ale ponecháva certifikačným orgánom a uchádzačom o certifikáciu veľkú voľnosť pri organizovaní svojich činností posudzovania zhody spôsobom, ktorý im najviac vyhovuje. Na záver sa uvádza zaradenie európskeho systému do národnej certifikačnej schémy európskej peňaženky identity občana, pričom sa skúmajú možnosti, ktoré mu pripisujú viac či menej ústrednú úlohu.
8. Vzhľadom na počiatočné štádium zrelosti všetkých zložiek certifikačného ekosystému a variabilitu prístupu sa okolnosti slovenského certifikačného ekosystému príliš nelíšia, preto považujeme toto zhrnutie za relevantné aj pre slovenskú národnú certifikačnú schému. Odchýlky slovenského prístupu v porovnaní s pôvodnou šablónou v každej kapitole označujeme buď odlišnou farbou, alebo pod pôvodným textom návrhu schémy EÚ.

   Existujú rozdiely z nasledujúcich dôvodov, napr.:

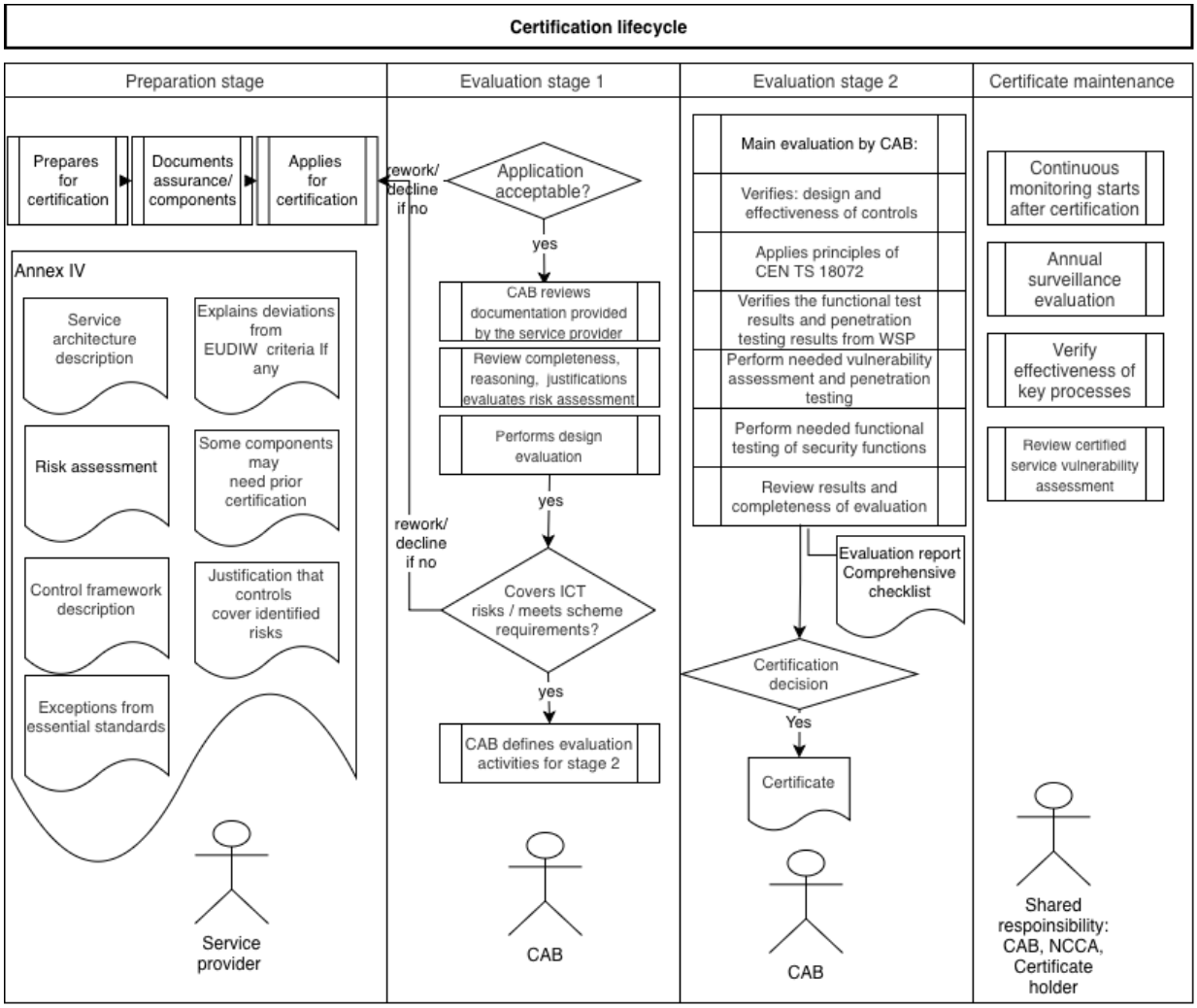
   a. chýbajúce informácie v šablóne,
   b. otvorené otázky v šablóne/kandidátskej schéme EÚ,
   c. odlišné národné pozadie a okolnosti,
   d. existujúca predchádzajúca certifikačná schéma pre nariadenie eIDAS na Slovensku,
   e. kapacita existujúceho certifikačného orgánu,
   f. konkrétne implementácie slovenského práva alebo iné obmedzenia vyplývajúce z náročného časového harmonogramu tohto projektu.

Zásady schémy (informatívne)

Nasledujúca tabuľka je zahrnutá ako informatívna pomôcka na zachovanie logiky životného cyklu certifikácie opísanej v nenormatívnej kapitole „Zásady schémy“ návrhu kandidátskej schémy EUDIW EÚ; keďže slovenská národná schéma je vypracovaná primárne na základe normatívnej štruktúry a príloh návrhu schémy EÚ, informatívne časti návrhu EÚ nie sú v plnom znení zopakované v hlavnej časti slovenskej národnej schémy, ale ich praktický význam je tu zohľadnený s cieľom vysvetliť, ako príloha I, príloha IV, príloha VIII, príloha X, príloha XI a ustanovenia o udržiavaní certifikátov fungujú spoločne v priebehu celého životného cyklu certifikácie.

Životný cyklus certifikácie sa má čítať spolu so slovenskými prílohami, ktoré nadväzujú na kandidátsku schému EUDIW EÚ prispôsobenú slovenskému národnému kontextu. Príloha I definuje certifikovaný objekt a hranice jeho modulov. Príloha II upravuje údržbu certifikátov a dohľad po ich vydaní. Príloha IV definuje súbor dôkazov pripravený poskytovateľom služby. Príloha VIII definuje akreditáciu, autorizáciu, spôsobilosť a povolené činnosti CAB (angl. Conformity assessment body, orgán posudzovania zhody). Príloha XI definuje metódy používané CAB. Príloha X definuje hodnotiace kritériá.

Tabuľka č.1 Životný cyklus certifikácie



Fáza životného cyklu	Prvok diagramu	Vysvetlenie
Prípravná fáza (preparation stage)	Príprava na certifikáciu	Poskytovateľ služieb začne s prípravou certifikačného balíka ešte pred podaním žiadosti. Nejde len o administratívnu prípravu, ale aj o prípravu architektúry, rizík, dôkazov, dokumentácie o záruke a odôvodnenia predmetu.
Prípravná fáza	Dokumenty o zárukách / komponenty	Poskytovateľ služieb identifikuje komponenty, podslužby, opakovane použiteľné informácie o záruke a dôkazy pre certifikovanú službu IKT. Zahŕňa to certifikáty komponentov, správy o záruke, dôkazy QTSP, dôkazy ISMS, dôkazy o funkčnom skúšaní a ďalšie výstupy posudzovania zhody.
Fáza prípravy	Podanie žiadosti o certifikáciu	Poskytovateľ predloží žiadosť a podpornú dokumentáciu CAB. Žiadosť musí identifikovaťpredmet certifikácie, modul(y), architektonický profil (profily), modifikátor(y) prípadov použitia, závislosti a požadované hranice certifikátu.
Prípravná fáza	Súbor dôkazov podľa prílohy IV	Rámček „Príloha IV“ v diagramu predstavuje minimálne informácie potrebné na certifikáciu. Mal by sa chápať ako štruktúrovaná dokumentácia, nie ako jediný dokument.
Prípravná fáza	Popis architektúry služby	Poskytovateľ opisuje architektúru certifikovanej služby, vrátane riešenia peňaženky, služby PID, služby validácie, backendových systémov, WSCA (angl. Wallet Secure Cryptographic Application, bezpečná kryptografická aplikácia peňazenky) /WSCD (angl. Wallet Secure Cryptographic Device, bezpečne kryptografické zariadenie peňaženky), rozhraní, tokov údajov, hraníc dôveryhodnosti, predpokladov a externých závislostí.
Prípravná fáza	Posúdenie rizík	Poskytovateľ pripraví posúdenie rizík špecifických pre implementáciu, vrátane rizík z registra rizík Únie a rizík špecifických pre implementáciu na Slovensku.
Prípravná fáza	Popis rámca opatrenia na riadenie	Poskytovateľ vysvetlí kontrolný rámec a spôsob, akým sa opatrenia implementujú v rámci komponentov, procesov a modulov.
Prípravná fáza	Výnimky zo základných noriem	Poskytovateľ identifikuje, kde sa normy, technické špecifikácie, základné normy, profily ochrany alebo rámcové požiadavky neuplatňujú v plnom rozsahu, nie sú uplatniteľné, stále sa vyvíjajú alebo sa uplatňujú odlišne.
Prípravná fáza	Vysvetlenie prípadných odchýlok od kritérií EUDIW	Poskytovateľ musí vysvetliť, prečo žiadna odchýlka neznižuje požadovaná úroveň záruky ani nezanecháva riziko nezakryté.
Prípravná fáza	Niektoré komponenty	Niektoré komponenty môžu vyžadovať predchádzajúcu certifikáciu, samostatné posúdenie alebo opätovnú záruku, aby

	môžu vyžadovať predchádzajúcu certifikáciu	mohli podporiť celkový záver certifikácie. To platí najmä pre WSCD, WSCA, inštanciu peňaženky, backend ISMS, služby QTSP alebo skúšanie funkčnej zhody.
Prípravná fáza	Odôvodnenie, že opatrenia riadia identifikované riziká	Poskytovateľ vysvetlí, prečo implementované opatrenia a informácie o opätovne použiteľnej záruke pokrývajú identifikované riziká, vrátane zvyškových rizík a kompenzačných opatrení.
Fáza hodnotenia (Evaluation stage) 1	Je žiadosť prijateľná?	Certifikačný orgán najprv skontroluje, či je žiadosť dostatočne kompletná a či spadá do predmetu schémy. Ide o kontrolu prijateľnosti, nie o úplné posudzovanie zhody.
Fáza hodnotenia 1	Prepracovanie / zamietnutie, ak nie	Ak je žiadosť neúplná, nespadá do predmetu konania, je nekonzistentná alebo nedostatočne podložená, CAB v konaní nepokračuje. Poskytovateľ musí žiadosť opraviť, inak bude žiadosť zamietnutá.
Fáza hodnotenia 1	CAB preskúma dokumentáciu poskytnutú poskytovateľom služieb	CAB preskúma predloženú dokumentáciu s cieľom porozumieť službe, predmetu, argumentácii týkajúcej sa rizík, súboru dôkazov, predpokladom a opätovne použiteľnej záruke.
Fáza hodnotenia 1	Preskúma úplnosť, odôvodnenie, zdôvodnenia a vyhodnotí posúdenie rizika	CAB overuje, či je súbor dôkazov kompletný, či je odôvodnenie poskytovateľa koherentné a či je posúdenie rizík dostatočne prepojené s opatreniami a komponentmi.
Fáza hodnotenia 1	Vykonáva hodnotenie návrhu	CAB hodnotí, či sú návrh služby, architektúra, závislosti, predpoklady a opatrenia vhodné na splnenie hodnotiacich kritérií.
Fáza hodnotenia 1	Zahŕňa riziká IKT / spĺňa požiadavky schémy?	CAB určí, či by služba v prípade implementácie a prevádzky podľa popisu pokrývala riziká v oblasti IKT a spĺňala požiadavky schémy. Toto je kľúčová rozhodovacia brána fázy 1.
Fáza hodnotenia 1	CAB definuje hodnotiace činnosti pre fázu 2	CAB pripraví plán hodnotenia pre hlavnú fázu hodnotenia. Tento plán identifikuje audity, inšpekcie, skúšanie, kontroly závislostí, odber vzoriek, posúdenie zraniteľnosti, funkčné skúšanie a zostávajúce činnosti.
Fáza hodnotenia (Evaluation stage) 2	Hlavné hodnotenie CAB	CAB vykonáva hlavné hodnotiace činnosti v súlade s hodnotiacim plánom. Ide o fázu zhromažďovania dôkazov a verifikácie.

Fáza hodnotenia 2	Overuje návrh a účinnosť opatrení na riadenie	CAB overuje, či sú opatrenia správne navrhnuté a či fungujú efektívne, alebo v prípade počiatočnej certifikácie, či je možné preukázať ich prevádzkovú účinnosť prostredníctvom pilotných projektov, testov alebo kontrolovanej prevádzky.
Fáza hodnotenia 2	Uplatňuje zásady normy CEN TS 18072	Hodnotenie presahuje rámec jednoduchého auditu dokumentácie. CAB používa audit, inšpekciu a v prípade potreby skúšanie vhodné pre služby IKT s vysokou úrovňou záruky a komplexné hodnotenie.
Fáza hodnotenia 2	Overuje výsledky funkčných skúšaní a výsledky penetračných skúšaní od WSP	CAB preskúma skúšanie, ktoré už vykonal alebo poskytol poskytovateľ riešení peňaženiek, vrátane skúšania funkčnej zhody a penetračných testov. CAB výsledky slepo neprijíma, ale overuje ich vhodnosť, predmet a spoľahlivosť.
Fáza hodnotenia 2	Vykonanie potrebného posúdenia zraniteľnosti a penetračného skúšania	Ak sú existujúce dôkazy nedostatočné alebo ak riziko vyžaduje priame overenie, CAB vykoná alebo vyžaduje dodatočné posúdenie zraniteľnosti a penetračné skúšanie.
Fáza hodnotenia 2	Vykonanie potrebného funkčného skúšania bezpečnostných funkcií	CAB vykoná alebo vyžaduje funkčné skúšanie funkcií relevantných pre bezpečnosť, najmä ak je funkčná zhoda potrebná na preukázanie, že bezpečnostné funkcie sú správne implementované.
Fáza hodnotenia 2	Preskúmanie výsledkov a úplnosti hodnotenia	CAB preskúma, či boli vykonané všetky požiadavky, či sú dôkazy dostatočné a či boli zistenia vyriešené.
Fáza hodnotenia 2	Hodnotiaca správa / komplexný kontrolný zoznam	CAB vypracuje hodnotiacu správu a komplexný kontrolný zoznam, v ktorom sa uvádza, ako súvisia dôkazy, kritériá, metódy a závery.
Fáza hodnotenia 2	Rozhodnutie o certifikácii	Rozhodnutie o certifikácii sa prijíma na základe výsledkov hodnotenia, preskúmania a záveru, že požiadavky sú splnené bez nevyriešených blokujúcich nezhôd.
Fáza hodnotenia 2	Certifikát	Certifikát zaznamenáva predmet certifikácie, moduly, profily, predpoklady, závislosti, úroveň záruky, držiteľa certifikátu a platnosť.

Udržiavanie certifikátu	Po certifikácii začína nepretržité monitorovanie	Po certifikácii musí certifikovaná služba zostať pod dohľadom. Ide o spoločnú zodpovednosť držiteľa certifikátu, CAB a NCCA.
Udržiavanie certifikátu	Ročné hodnotenie dohľadu	Certifikovaná služba sa pravidelne, zvyčajne raz ročne, opätovne posudzuje s cieľom potvrdiť jej trvalú zhodu.
Udržiavanie certifikátu	Overenie účinnosti kľúčových procesov	Pri údržiavaní sa overuje, či kľúčové procesy, ako je riadenie zraniteľností, riadenie zmien, riadenie incidentov, riadenie podvodov a kontrola certifikovaných verzií, zostávajú v plnej miere účinné.
Udržiavanie certifikátu	Preskúmanie posúdenia zraniteľnosti certifikovanej služby	CAB preskúma, či posúdenie zraniteľnosti zostáva aktuálne vzhľadom na nové zraniteľnosti, zmeny komponentov, vývoj hrozieb a zmeny závislostí.
Priečne	Účastník poskytovateľa služieb	Poskytovateľ služby je zodpovedný za prípravu, dokumentáciu, posúdenie rizík, zhromažďovanie dôkazov a údržbu certifikovanej služby.
Priečne	Úloha CAB	Subjekt CAB overuje prijateľnosť, hodnotí dokumentáciu, vykonáva alebo koordinuje hodnotiace činnosti, posudzuje výsledky a podporuje rozhodnutie o certifikácii.
Priečne	Spoločná zodpovednosť: CAB, NCCA, držiteľ certifikátu	Udržovanie nie je len činnosťou CAB. Držiteľ certifikátu monitoruje zmeny a zraniteľnosti, CAB vykonáva dohľad a špeciálne hodnotenia a NCCA vykonáva dozor.

Predhovor

(EÚ, informatívne)

1. OBMEDZENIA

a) Ekosystém peňaženiek EUDI je stále v počiatočnom štádiu. Začiatkom roka 2026 nebola nasadená ani certifikovaná žiadna peňaženka EUDI a na špecifikácii sa stále pracuje. Okrem toho, pokiaľ ide o bezpečnosť, nie je k dispozícii žiadna norma ani technická špecifikácia a do konca roka sa ich zavedenie ani neočakáva. Táto kandidátska schéma preto obsahuje v prílohách technické špecifikácie vypracované agentúrou ENISA, ktoré sa majú použiť v prvej verzii schémy a ktoré môžu byť predložené európskym normalizačným organizáciám (ESO) na ich následnú údržbu.

b) Väčšina implementácií peňaženiek je navrhnutá tak, aby fungovala na osobných mobilných zariadeniach, ktoré do roku 2026 zriedka prešli akoukoľvek formálnou certifikáciou. Keďže tieto zariadenia poskytujú používatelia a preto nie sú zahrnuté do predmetu certifikácie, je veľmi ťažké spoliehať sa na ich bezpečnostné vlastnosti. Jedným z riešení je zahrnúť špecifické bezpečnostné opatrenia do mobilných aplikácií, ktoré sú dostupné a spustené na týchto zariadeniach, ale tento prístup je v niektorých aspektoch obmedzený, napríklad pri overovaní používateľov. Návrh kandidátskej schémy preto zavádza proces riadenia podvodov, ktorý dopĺňa riadenie zraniteľností o riadenie podvodov, s cieľom identifikovať potenciálne problémy čo najskôr.

2. ODKAZY NA LEGISLATÍVU

a) Schéma obsahuje len málo priamych odkazov na nariadenie (EÚ) 2024/1183, bežne označované ako Európsky rámec pre digitálnu identitu (eIDAS), pretože vychádza z predpokladu, že na jeho certifikáty sa bude odkazovať v národnej schéme pre peňaženky EUDI, takže povinnosti vyplývajúce z eIDAS, najmä z článku 5c, sa vzťahujú skôr na túto národnú schému ako na súčasnú schému. Môže však existovať možnosť využiť túto schému EÚ na splnenie požiadaviek článku 5c, čo sa skúma v prílohe XIV.

b) Nariadenie (EÚ) 2024/2847, bežne označované ako akt o kybernetickej odolnosti (CRA), sa priamo nevzťahuje na peňaženky EUDI, keďže sú v kontexte tejto schémy certifikované ako služby IKT, nie ako produkty IKT. Avšak najmä v prípade, ak je inštancia peňaženky mobilnou aplikáciou, nariadenie by sa vzťahovalo na inštanciu peňaženky, ak ju na trh uvádza komerčný subjekt. Keďže uplatňovanie CRA sa bude líšiť v závislosti od architektúry peňaženky EUDI a ďalších parametrov, v rámci schémy sa rozhodlo o použití požiadaviek CRA tam, kde je to relevantné, avšak nie systematicky, keďže certifikáty EUDIW-SK (uplatňujúce sa na službu IKT, nie na produkt IKT) nebudú vhodné na predpoklad zhody.

c) Smernica (EÚ) 2022/2555 o sieťových a informačných systémoch (NIS2) sa priamo nevzťahuje na peňaženky EUDI, hoci niektoré členské štáty rozšírili rozsah pôsobnosti pri vnútroštátnej transponovazícii smernice tak, aby zahŕňal poskytovateľov peňaženiek EUDI, a existuje prebiehajúci návrh na ich zaradenie do predmetu pôsobnosti pri najbližšej revízii smernice. Obmedzenia v oblasti kybernetickej bezpečnosti sa však väčšinou uplatňujú, keďže norma, ktorú sme navrhli použiť ako základ pre hodnotenie peňaženiek EUDI (ETSI EN 319 401), obsahuje vo svojej najnovšej verzii v2.3.1 požiadavky navrhnuté tak, aby spĺňali požiadavky vykonávacieho nariadenia Komisie (CIR) (EÚ) 2024/2690.

Počiatočný kontext slovenskej národnej certifikačnej schémy pre peňaženky EUDI (informatívny)

Počiatočný kontext a pozadie

1. V čase finalizácie tohto návrhu slovenskej národnej certifikačnej schémy boli k dispozícii usmernenia pre národnú implementáciu certifikačnej schémy peňaženiek EUDI. Tieto usmernenia boli vypracované s cieľom vytvoriť dôveryhodný, opakovateľný a vzájomne kompatibilný certifikačný rámec na úrovni EÚ s ambíciou, aby sa národné schémy mohli čo najhladšie transformovať na budúcu kandidátsku schému na úrovni EÚ.
2. Tento vývoj potvrdil pôvodný strategický zámer odvodiť národnú schému v čo najväčšej miere z existujúcich materiálov, rámcov a noriem a čo najviac ho zosúladiť s budúcou spoločnou európskou certifikačnou schémou.
3. **Slovenská národná certifikačná schéma preto:**
   a) vo veľkej miere vychádza z existujúcich dokumentov EÚ a referenčných materiálov,
   b) sa opiera o platné medzinárodné normy, z ktorých niektoré sú ešte v štádiu návrhu
   c) predpokladá budúce zosúladenie s vyvíjajúcou sa kandidátskou schémou EÚ,
   d) minimalizuje národné odchýlky od kandidátskej schémy EÚ, pokiaľ to nie je absolútne nevyhnutné.
   e) Tento prístup má za cieľ zabezpečiť dlhodobú kompatibilitu, znížiť potrebu dodatočných úprav a uľahčiť potenciálny prechod na certifikačnú schému na úrovni EÚ.

4. **Neistota a meniace sa prostredie**
   - Projekt národnej certifikačnej schémy EUDIW-SK je svojou povahou komplexný z dôvodu:
     1) nejednoznačnosti určitých regulačných a technických požiadaviek,
     2) neustáleho vývoja príslušných noriem,
     3) vyvíjajúcej sa architektúry národného riešenia EUDI Wallet,
     4) vyvíjajúceho sa referenčného rámca architektúry (ARF)
     5) neúplných alebo na úrovni predbežných rámcov funkčnej zhody,
     6) Dynamický vývoj koncepcií certifikácie na úrovni EÚ,
     7) Nedostatok skúseností a odborníkov na audit, certifikáciu a prípravu schémy v oblasti EUDIW, čo je komplex certifikácie produktov, služieb a procesov
     8) Náročný časový harmonogram certifikácie národného riešenia v rámci schémy, ktorá sa práve vyvíja
   - Okrem toho zostáva harmonogram certifikácie národného riešenia neistý, keďže riešenie sa stále vyvíja a prispôsobuje sa meniacemu sa ARF. V dôsledku toho môžu byť niektoré referenčné normy a rámce v čase posudzovania zhody stále vo vývoji a audítor bude musieť počas certifikačného auditu prijímať rozhodnutia a odôvodňovať odchýlky od návrhov noriem.
5. **Prístup zameraný na budovanie mostov:**

   - Slovenská národná certifikačná schéma nemá za cieľ vytvárať pridanú hodnotu opakovaním regulačných požiadaviek alebo preberaním odsekov z existujúcich noriem.

Cieľom schémy je skôr predstaviť štruktúrovaný spôsob uvažovania o požiadavkách, prepojiť súvisiace požiadavky v rôznych rámcoch, identifikovať prekrývania a nedostatky v rámci schémy certifikácie elektronických identít eIDAS a vysvetliť, ako sa majú nedostatky dočasne zmierniť, kým nebude plne dostupná európska certifikačná schéma. Schéma je preto zámerne navrhnutá ako most medzi súčasnou fázou národnej implementácie a budúcim európskym certifikačným rámcom.

- Táto prepojovacia úloha je motivovaná praktickými obmedzeniami. Existuje výrazný nedostatok kvalifikovaných odborníkov a tí istí odborníci sú už potrební v rámci viacerých certifikačných schém a prekrývajúcich sa oblastí, vrátane nariadenia eIDAS, národnej regulácie kybernetickej bezpečnosti, hodnotení QTSP založených na ETSI, budúcich činností súvisiacich s EUCC a začínajúcej práce v oblasti posudzovania zhody EUDI Wallet. Slovenská schéma sa preto snaží minimalizovať zdvojovanie úsilia, maximalizovať opätovné využitie výstupov hodnotenia a vyhnúť sa štruktúre, ktorá by nútila opakovať tú istú prácu počas neskoršieho prechodu na schému EÚ.

6. **Za týchto okolností:**

a) Od audítorov sa očakáva, že pri posudzovaní požiadaviek odvodených z návrhov alebo vyvíjajúcich sa noriem budú uplatňovať odborný úsudok a náležitú starostlivosť.

b) Certifikačné orgány budú musieť jasne zdokumentovať, ktoré ustanovenia sa uplatňujú v plnom rozsahu a ktoré sú podmienené alebo prechodné.

c) Od poskytovateľov riešení sa očakáva, že identifikujú a vyriešia nedostatky v prípadoch, keď sú normy neúplné alebo sa vyvíjajú, najmä v súvislosti s požiadavkami na vysokú úroveň záruky, a poskytnú odôvodnenie, ako certifikovaný ekosystém EUDIW spĺňa požiadavky právnych predpisov a certifikačné požiadavky na úrovni záruky vysoká.

d) Vydanie tohto návrhu v tejto fáze slúži dôležitému účelu: stanovuje smer pre všetky zainteresované strany a poskytuje transparentné očakávania týkajúce sa certifikačných procesov, dokumentácie, vstupných materiálov a predpokladaných časových harmonogramov pre súčasných a budúcich poskytovateľov riešení peňaženiek.

7. **Štyri praktické piliere slovenského prístupu**

Slovenská schéma je postavená na štyroch praktických pilieroch.

(a) Prvým pilierom je už zavedený ekosystém auditov kybernetickej bezpečnosti podľa vnútroštátnych právnych predpisov, vrátane povinných požiadaviek na audit kybernetickej bezpečnosti a regulovaného kvalifikačného rámca pre audítorov kybernetickej bezpečnosti.

(b) Druhým pilierom sú dlhoročné skúsenosti z auditu nariadenia eIDAS a poskytovateľov dôveryhodných služieb, kde spoľahlivé výsledky v minulosti záviseli nielen od normatívneho textu, ale aj od spôsobilosti a odborného úsudku audítorov pôsobiacich v rámci rámcov založených na ETSI a predtým ovplyvnených ISACA.

(c) Tretím pilierom je zámerne audítorsky orientovaný prístup, ktorý akceptuje, že v prechodnom a na princípoch založenom prostredí musia odborní audítori preklenúť nedostatok medzi zákonnými povinnosťami, technickými normami, architektonickými realitami a dostupnými dôkazmi.

(d) Štvrtým pilierom je systematické opätovné využitie existujúcich európskych a medzinárodných výstupov, vrátane materiálov ENISA, noriem ETSI, noriem ISO, rámca funkčného posudzovania zhody, prvkov referenčného rámca architektúry a

ďalších základných noriem a technických špecifikácií.

To znamená, že slovenská schéma nedefinuje ani nekopíruje dostupné požiadavky. Skôr považuje dostupné materiály za autoritatívne vstupy a integruje ich do procesu hodnotenia štruktúrovaným a sledovateľným spôsobom. Referenčný rámec architektúry sa nepovažuje za samostatný zdroj povinností, ale za štruktúrované a vyjadrenie právnych a technických požiadaviek, ktoré je potrebné interpretovať a premietnuť do hodnotiacich kritérií, opatrení a dôkazov.

8. **Zosúladenie s národným orgánom pre akreditáciu**

   a) Vývoj slovenskej národnej certifikačnej schémy pre peňaženku EUDI prebiehal v úzkej spolupráci so slovenským NAB SNAS (Slovenská národná akreditačná služba). Počas série analytických workshopov a konzultácií boli vyhodnotené potenciálne štrukturálne prístupy.

   b) V spolupráci so SNAS sme analyzovali existujúce potenciálne inšpiratívne zdroje pre výber prístupu k národnému schému, napr.:

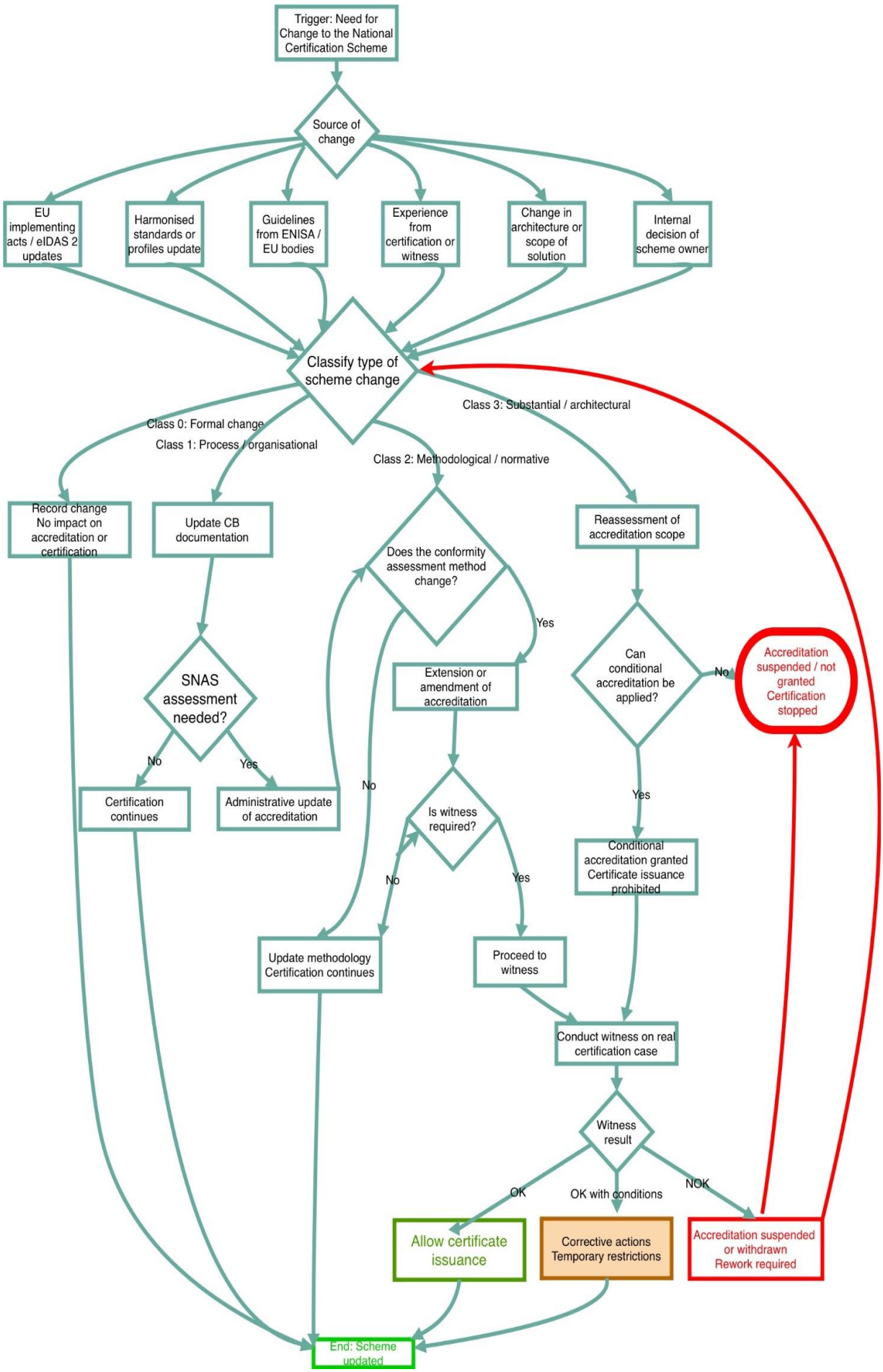
      1) **nástrojová sada CASCO** https://www.iso.org/committee/54998/x/catalogue/p/1/u/0/w/0/d/0.
      2) **ISO/IEC 17011: 2017** Posudzovanie zhody — Požiadavky na orgány akreditácie akreditujúce orgány posudzovania zhody
      3) **ISO/IEC 17029:2019** Posudzovanie zhody – Všeobecné zásady a požiadavky na validačné a verifikačné orgány
      4) **ISO/IEC DIS 17007:2026**
      5) Posudzovanie zhody — Usmernenia pre vypracovanie normatívnych dokumentov vhodných na použitie pri posudzovaní zhody
      6) **ISO/IEC DRT 17032:2019**
      7) **Posudzovanie zhody** — Návody a príklady certifikačnej schémy pre procesy

   c) Kľúčovým míľnikom pri príprave tohto návrhu bolo dosiahnutie dohody so SNAS o tom, ako riešiť:

      1) nejednoznačnosť v regulačných a technických požiadavkách,
      2) zmenami vyplývajúcimi z nedokončených alebo vyvíjajúcich sa noriem,
      3) úpravami architektúry výrobkov,
      4) budúcich aktualizácií kandidátskych schém na úrovni EÚ,
      5) vyvíjajúci sa koncept posudzovania zhody.

9. **Táto dohoda stanovila štruktúrovaný prístup k:**

   a) aktualizácii a udržiavaniu národného schému,
   b) riadenie zmien v rámci ekosystému akreditácie a certifikácie,
   c) predchádzaniu regulačnej paralýze spôsobenej neistotou,
   d) zabezpečenie pokroku napriek meniacim sa vonkajším vplyvom.
   e) schéma preto zahŕňa definovanú logiku riadenia zmien pre akreditáciu a certifikačné pracovné postupy – pozri diagram.


Trigger: Need for Change to the National Certification Scheme
Source of change
EU implementing acts / eIDAS 2 updates
Harmonised standards or profiles update
Guidelines from ENISA / EU bodies
Experience from certification or witness
Change in architecture or scope of solution
Internal decision of scheme owner
Classify type of scheme change
Class 0: Formal change
Class 1: Process / organisational
Class 2: Methodological / normative
Class 3: Substantial / architectural
Record change No impact on accreditation or certification
Update CB documentation
Does the conformity assessment method change?
Reassessment of accreditation scope
SNAS assessment needed?
Yes
No
Extension or amendment of accreditation
Can conditional accreditation be applied?
No
Accreditation suspended / not granted Certification stopped
Yes
No
Certification continues
Administrative update of accreditation
Is witness required?
No
Yes
Conditional accreditation granted Certificate issuance prohibited
Update methodology Certification continues
Proceed to witness
Conduct witness on real certification case
Witness result
OK
OK with conditions
NOK
Allow certificate issuance
Corrective actions Temporary restrictions
Accreditation suspended or withdrawn Rework required
End: Scheme updated

Krok diagramu	Vysvetlenie	Odôvodnenie v kontexte schéma
Spúšťač: potreba zmeny v národnej certifikačnej schéme	Je identifikovaná potreba zmeny.	Slovenská schéma je koncipovaná ako kontrolovaná, perspektívna základná línia, ktorá sa musí vyvíjať v súlade s usmerneniami, normami, architektúrou a praxou akreditácie EÚ.
Zdroj zmeny	Zistiť, prečo je potrebné schéma zmeniť.	Zmena musí byť sledovateľná s konkrétnym dôvodom a nesmie sa riešiť neformálne.
Vykonávacie akty EÚ / aktualizácie nariadenia eIDAS 2	Zmeny právnych predpisov alebo regulácie na úrovni EÚ.	Môže si vyžiadať povinné prispôsobenie národnej schémy s cieľom zachovať zhodu s právnymi predpismi.
Aktualizácia harmonizovaných noriem alebo profilov	Nové alebo revidované technické normy, profily ochrany alebo harmonizované dokumenty.	Schéma sa opiera o výstupy EÚ a medzinárodné výstupy a mala by ich v prípade potreby integrovať.
Návod od agentúry ENISA / orgánov EÚ	Nové interpretačné alebo technické usmernenia.	Takéto usmernenia môžu ovplyvniť hodnotiace kritériá, metódy alebo očakávania v oblasti záruky.
Skúsenosti z certifikácie alebo svedectva	Poučenia z reálnej certifikácie, pilotného hodnotenia alebo akreditácie.	Akreditácia a certifikácia sú vzájomne závislé; skúsenosti zo svedectva môžu odhaliť praktické nedostatky.
Zmena architektúry alebo predmetu riešenia	Zmeny v architektúre peňaženky, moduloch, profiloch alebo predmete certifikácie.	Zmeny architektúry/profilu môžu ovplyvniť riziko, závislosti, plán hodnotenia a predmet akreditácie.
Vnútorné rozhodnutie vlastníka schémy	NBÚ/vlastník schémy sa rozhodne schému vylepšiť.	Vlastník schémy pravidelne prehodnocuje potrebu aktualizácií.
Klasifikácia typu zmeny schémy	Určite kategóriu vplyvu zmeny.	Toto je kľúčové opatrenie: reakcia musí byť úmerná závažnosti zmeny.
Trieda 0: Formálna zmena	Redakčné, formátovacie, číslovacie, terminologické alebo nepodstatné opravy.	Žiadny vplyv na certifikáciu alebo akreditáciu, pretože požiadavky a metódy zostávajú nezmenené.
Zaznamenať zmenu – žiadny vplyv na akreditáciu alebo certifikáciu	Zaznamenajte zmenu a zachovajte účinnosť existujúceej schémy.	Zachováva sa sledovateľnosť bez spustenia zbytočného opätovného posudzovania.
Trieda 1: Zmena procesu / organizačná zmena	Zmena ovplyvňuje postupy, zodpovednosti, dokumentáciu, podávanie správ alebo administratívne pracovné toky.	Môže ovplyvniť dokumentáciu CAB alebo záznamy o akreditácii, ale nemusí nutne meniť technické požiadavky.
Aktualizácia dokumentácie certifikačného orgánu	Certifikačný orgán aktualizuje postupy, šablóny, kontrolné zoznamy, záznamy o spôsobilostiach alebo prevádzkové dokumenty.	Je potrebné zabezpečiť, aby CAB naďalej fungoval v súlade s aktualizovanou schémou.

Je potrebné posúdenie SNAS?	Rozhodnite, či zmena ovplyvňuje činnosti spojené s akreditáciou alebo predpoklady o spôsobilostiach.	Predmet akreditácie a schopnosti CAB musia zostať v súlade so schémou.
Nie → certifikácia pokračuje	Ak predmet akreditácie nie je ovplyvnený, certifikácia môže pokračovať.	Zabráni sa tak regulačnej paralýze, ak je zmena iba administratívna.
Áno → administratívna aktualizácia akreditácie prostredníctvom	SNAS aktualizuje alebo potvrdzuje dokumentáciu týkajúcu sa akreditácie.	Udržiava záznamy o akreditácii v súlade bez nutnosti úplného technického prehodnotenia.
Trieda 2: Metodická/normatívna zmena	Zmena ovplyvňuje hodnotiace kritériá, metódy, normy, normatívne odkazy, očakávania týkajúce sa dôkazov alebo logiku posudzovania.	Tieto zmeny môžu ovplyvniť spôsob preukazovania zhody, ale nie nevyhnutne architektúru alebo predmet akreditácie.
Mení sa metóda posudzovania zhody?	Rozhodnite, či sa mení skutočná metóda hodnotenia, spôsobilosť, skúšanie, inšpekcia alebo prístup k auditu.	Dokument rozlišuje medzi auditom, inšpekciou a skúšaním; zmeny metódy môžu ovplyvniť akreditáciu.
Nie → aktualizujte metodiku, certifikácia pokračuje	Aktualizujte interpretáciu, usmernenia, kontrolné zoznamy alebo hodnotiace matice bez prerušenia certifikácie.	Primeraný v prípade, ak zmena objasňuje existujúce požiadavky, ale nemení metódu ani základ záruky.
Áno → rozšírenie alebo zmena akreditácie	Predmet akreditácie alebo metódy môžu vyžadovať zmenu, kým sa certifikáty budú môcť opierať o aktualizovanú metódu.	Požiadavka platí v prípade, ak CAB potrebuje nové spôsobilosti, metódu, kapacity pre skúšanie alebo inšpekciu.
Je potrebný svedok?	Rozhodnite, či SNAS musí sledovať skutočný certifikačný prípad.	V dokumente sa uvádza, že akreditácia môže vyžadovať audit svedka počas skutočného certifikačného procesu.
Nie → aktualizácia metodiky, certifikácia pokračuje	Aktualizácia akreditácie sa môže vykonať administratívne alebo prostredníctvom preskúmania dokumentov.	Používa sa v prípadoch, keď už bola preukázaná spôsobilosť.
Áno → pokračovať k svedkovi	SNAS pozoruje CAB v skutočnom certifikačnom prípade.	Je to potrebné v prípadoch, keď sa spôsobilosť musí preukázať v praxi.
Vykonajte svedectvo v reálnom certifikačnom prípade	Svedectvo o akreditácii sa vykonáva počas skutočnej certifikačnej činnosti.	To odráža paralelný model akreditácie/certifikácie schémy.
Výsledok svedectva: OK	Spôsobilosť CAB a uplatňovanie metódy sú potvrdené.	Môže sa pristúpiť k vydaniu certifikátu.
Povoliť vydanie certifikátu	Certifikácia môže pokračovať podľa	Záruka zostáva platná a základ akreditácie je potvrdený.

	aktualizovanej schémy/metódy.	
Výsledok posúdenia: V poriadku s podmienkami	Zistili sa menšie problémy alebo obmedzenia.	Certifikácia môže pokračovať len s nápravnými opatreniami alebo dočasnými obmedzeniami.
Nápravné opatrenia / dočasné obmedzenia	CAB musí problémy odstrániť; predmet alebo vydanie môže byť dočasne obmedzené.	Proporcionálna reakcia na nekritické zistenia.
Výsledok svedectva: NOK	CAB nedokáže preukázať požadovanú spôsobilosť alebo uplatňovanie metódy.	Certifikácia nemôže bezpečne pokračovať podľa zmenenej metódy.
Akreditácia pozastavená alebo odňatá / vyžaduje sa prepracovanie	Akreditácia je pozastavená/odňatá alebo CAB musí zopakovať prípravu.	Zabraňuje vydávaniu certifikátov bez preukázanej spôsobilosti.
Trieda 3: Významná/architektonická zmena	Zmena ovplyvňuje základnú architektúru, predmet certifikácie, model záruky, hranice modulov, kritické komponenty alebo pokrytie rizík.	Dokument považuje zmeny architektúry a kritických komponentov za podstatné.
Prehodnotenie predmetu akreditácie	SNAS/NBÚ opätovne posúdia, či súčasná akreditácia stále pokrýva dané schéma.	Je to potrebné, pretože zmena môže vyžadovať odlišnú spôsobilosť, metódy alebo predmet.
Je možné uplatniť podmienenú akreditáciu?	Určite, či certifikácia môže pokračovať za kontrolovaných podmienok.	Podporuje pokrok napriek meniacim sa požiadavkám, pričom zachováva záruku.
Nie → akreditácia pozastavená / neudelená / certifikácia zastavená	Ak podmienky nemôžu zabezpečiť spoľahlivé posúdenie, certifikácia sa zastaví.	Chráni dôveryhodnosť schémy a zabraňuje vydávaniu neplatných certifikátov.
Áno → udelená podmienečná akreditácia; vydávanie certifikátov zakázané	CAB môže pokračovať v prípravných a hodnotiacich prácach, zatiaľ však nesmie vydávať certifikáty.	Je to užitočné v prípadoch, keď je pred konečnou akreditáciou potrebný svedok alebo dodatočné dôkazy.
Vykonanie svedectva na skutočnom certifikačnom prípade	Skutočný prípad sa používa na potvrdenie spôsobilostí v rámci zmenenej architektúry alebo predmetu.	Je to v súlade s požiadavkou dokumentu, že akreditácia a certifikácia môžu prebiehať paralelne.
Koniec: aktualizované schéma	Aktualizovaná schéma, dokumentácia, stav akreditácie a logika certifikácie sú zosúladené.	Konečný stav: schéma zostáva aktuálna, sledovateľná a použiteľná bez ohrozenia záruky.

10. **Vzájomná závislosť certifikácie a akreditácie a vývoj WS (ang. wallet solution, riešenie peňaženky)**

    a) Podľa pravidiel akreditácie vyžaduje akreditácia certifikačného orgánu vykonanie „svedeckého auditu“. Svedecký audit sa musí vykonať počas skutočného certifikačného procesu. Z toho vyplýva:

1) Akreditáciu nie je možné finalizovať bez aktívneho certifikačného prípadu.
2) Certifikačnú schému nemožno považovať za funkčnú bez zosúladenia s požiadavkami akreditácie.
3) Je potrebný aspoň jeden pilotný alebo skutočný certifikačný klient.
4) Zároveň sa WS nemôže používať vo výrobe bez certifikácie, preto je zrejmé, že certifikácia sa musí vykonávať vo fáze prototypu a v testovacom prostredí.

b) Vzhľadom na špecifický predmet certifikácie validácie peňaženky EUDI na Slovensku sa predpokladá, že bude existovať iba jedno národné riešenie peňaženky, ktoré bude podliehať certifikácii s postupným prístupom pri certifikácii konkrétnych profilov. Preto sa procesy akreditácie a certifikácie musia vykonávať paralelne, pričom certifikačný proces tvorí neoddeliteľnú súčasť akreditačného auditu za prítomnosti svedka.

c) Očakáva sa, že oba procesy budú prebiehať súbežne a budú koordinovane ukončené spolu s prvými fázami vývoja WS .

11. **Odôvodnenie použitia šablóny EÚ**

a) Usmernenia EÚ odporúčajú postupný a evolučný prístup k vývoju národného ekosystému peňaženky EUDI. Očakáva sa, že celý rozsah prípadov použitia, funkcií a vrstiev interoperability dozrie v priebehu niekoľkých rokov.

b) Zároveň sa môže stať, že európsky certifikačný rámec dosiahne prevádzkovú jasnosť skôr, ako sa dokončí úplný národný funkčný vývoj riešenia peňaženky.

c) Predpokladaná platnosť národného certifikátu (napr. päť rokov) sa musí posudzovať s ohľadom na očakávaný vývoj národnej certifikačnej schémy na európskej úrovni.

d) Je vysoko pravdepodobné, že prechod na certifikačný rámec EÚ nastane pred uplynutím platnosti prvého národného certifikátu. V dôsledku toho:
1) Očakáva sa, že slovenské národné schéma bude fungovať v rámci prechodného obdobia.
2) Plne nezávislý národný štrukturálny model by pravdepodobne spôsobil zbytočné náklady na budúcu transformáciu.

e) Na základe uvedených úvah slovenský národný systém prijíma schému kandidátskeho systému EÚ ako svoj štrukturálny základ s cieľom:
1) zabezpečiť maximálnu zhodu s budúcimi certifikačnými požiadavkami EÚ,
2) umožniť hladké a jednoduché posudzovanie zo strany EDICG
3) minimalizovať štrukturálne odchýlky a transformačné úsilie,
4) vyhnúť sa duplicite a zbytočným národným špecifikám,
5) uľahčiť hladšie neskoršie vzájomné hodnotenie a porovnateľnosť na úrovni EÚ,
6) zabezpečiť predvídateľnosť pre orgány akreditácie a certifikačný personál,
7) jasne odlíšiť skutočne špecifické slovenské prvky od spoločných základných požiadaviek EÚ.

f) Slovenská národná schéma preto slúži ako:
1) národný operačný certifikačný rámec a
2) štruktúrovaný most smerom k budúcej európskej certifikačnej schéme.

g) Tento prístup zabezpečuje regulačnú kontinuitu, proporcionalitu úsilia a strategickú súdržnosť v rámci sa vyvíjajúceho európskeho ekosystému digitálnej identity.

12. **Paralelný vývoj noriem a architektúry**

a) Očakáva sa, že procesy akreditácie a certifikácie budú trvať niekoľko mesiacov (odhadom 6–9 mesiacov alebo dlhšie – v závislosti od komponentov architektúry). Počas

tohto obdobia:

1) Príslušné medzinárodné normy môžu dosiahnuť vyspelejšie štádiá.
2) Môžu byť dostupné profily ochrany a certifikované komponenty podľa EUCC.
3) Môžu byť vydané ďalšie usmernenia a dokumenty EÚ.
4) Národná architektúra peňaženky sa bude vyvíjať a bude presnejšie definovaná.

b) Schéma preto musí byť dostatočne flexibilná, aby zohľadňovalo meniace sa technické a regulačné požiadavky bez nutnosti štrukturálnej úpravy.

13. **Sprievodný diagram procesu opisuje, ako:**

a) sa vyhodnocujú vonkajšie zmeny (napr. nové normy, usmernenia EÚ, aktualizácie architektúry), posudzuje sa ich vplyv na národnú schému a potrebné úpravy sa implementujú kontrolovaným a transparentným spôsobom.

b) tento prístup zabezpečuje pokrok bez vytvárania kruhových závislostí alebo patových situácií spôsobených regulačnou neistotou v rámci časového tlaku.

14. **Použitie šablón EÚ a zosúladenie verzií**

a) Návrh slovenskej národnej schémy bol pôvodne vypracovaný s použitím šablóny pre národné schémy verzie 0.2 z 08/2025. Krátko pred finalizáciou bola dostupná šablóna kandidátskej schémy EÚ verzie 0.3.609 a aktualizovaný návod EÚ a začala sa verejná konzultácia k verzii 0.4.614.

b) V reakcii na to sa proces vypracovávania návrhu zosúladil s kandidátskou schémou EÚ verzie č. 04.614 s nasledujúcimi cieľmi:

1) využiť najnovšiu dostupnú základnú líniu zosúladenia,
2) uľahčiť hladký prechod na budúcu schému kandidátskej krajiny EÚ,
3) minimalizovať národné odchýlky,
4) zjednodušiť vzájomné hodnotenie a posudzovanie na úrovni EÚ,
5) vyhnúť sa zbytočnému prebudovávaniu existujúcich štruktúr,
6) jasne identifikovať a odôvodniť akékoľvek špecifické rozdiely pre Slovensko.

c) Táto premyslená stratégia zosúlaďovania znižuje dlhodobé regulačné trenice a podporuje interoperabilitu na úrovni EÚ. Neskoršie aktualizácie kandidátskej schémy sa budú posudzovať podľa logiky opísanej v diagramu.

15. **Rámec posudzovania funkčnej zhody**

a) Ďalším faktorom, ktorý prispel k pokroku pri príprave tohto návrhu, bolo zverejnenie verzie 0.1 rámca pre posudzovanie funkčnej zhody.

b) Hoci ide o predbežnú verziu, tento rámec poskytol:

1) štruktúrovanú metodiku prístupu k funkčnému skúšaniu,
2) usmernenie pre výber primeraných testovacích postupov,
3) interpretačný rámec na posudzovanie funkčných požiadaviek riešení digitálnej identity,
4) referenčný bod v situáciách, keď architektonické profily ešte neboli úplne definované.

c) Vzhľadom na vyvíjajúcu sa povahu tohto rámca:

1) Audítori môžu potrebovať určiť, ktoré časti sú v čase hodnotenia uplatniteľné.
2) Na funkčné skúšanie by sa mala použiť najnovšia dostupná verzia rámca, pokiaľ nie je výslovne odôvodnené inak.

3) Odchýlky alebo neaplikovateľné časti musia byť jasne zdokumentované a odôvodnené v správach o posudzovaní zhody.

16. **Účel vydania tohto návrhu**

a) Napriek meniacej sa regulačnej a technickej situácii sa tento návrh vydáva s cieľom:
   1) stanovenie jasných očakávaní v oblasti certifikácie,
   2) umožniť akreditačným orgánom a certifikačnému personálu pripraviť kvalifikačné rámce,
   3) poskytnúť predvídateľnosť súčasným a budúcim poskytovateľom riešení,
   4) definovať štruktúrovanú cestu k certifikácii úrovne záruky vysoká,
   5) predchádzalo stagnácii spôsobenou regulačnou neistotou.

b) Tento dokument preto predstavuje kontrolovanú, do budúcnosti orientovanú základnú líniu, ktorá je navrhnutá tak, aby sa vyvíjala riadeným a transparentným spôsobom súbežne s vývojom v EÚ.

17. **Regulačný a strategický kontext slovenskej schémy národného systému**

Slovenský rámec pre európsku peňaženku digitálnej identity je postavený na zákone č. 272/2016 Z. z. o dôveryhodných službách v znení neskorších predpisov, ktorý implementuje požiadavky nariadenia eIDAS do slovenského práva, a na súvisiacom právnom rámci EÚ, ktorý upravuje požiadavky na certifikáciu, akreditáciu, dohľad a úroveň záruky peňaženky EUDI.

Národný systém funguje na križovatke viacerých úrovní povinností: nariadenie eIDAS a jeho vykonávacích aktov pre ekosystém peňaženky EUDI; zákona o kybernetickej bezpečnosti a jeho vykonávacích predpisov pre národné riadenie kybernetickej bezpečnosti a povinné audítorské povinnosti; požiadaviek na posudzovanie zhody a systémy manažérstva založené na ETSI a ISO; a v prípade potreby produktovo orientovaných schém a technických požiadaviek, ako sú EUCC, záruka odvodená od spoločných kritérií, rámce funkčnej zhody a vznikajúce technické profily.

18. **Vnútroštátny právny základ a úlohy zainteresovaných strán**

V rámci slovenského ekosystému pôsobí NBÚ ako vlastník schémy a kľúčový dozorný orgán v oblasti dôveryhodných služieb a národnej certifikačnej schémy, zatiaľ čo Ministerstvo vnútra by malo pôsobiť ako verejný orgán zodpovedný za zabezpečenie poskytovania európskej peňaženky a súvisiacej schémy eID a funkcií prepojenia PID. SNAS pôsobí ako národný akreditačný orgán a orgán posudzovania zhody musí pôsobiť v rámci logiky akreditácie a autorizácie stanovenej schémou.

Z hľadiska vnútroštátneho práva musí byť poskytovateľ riešenia peňaženky kvalifikovaným poskytovateľom dôveryhodných služieb alebo preukázať, že na tento účel uzavrel platnú zmluvu s kvalifikovaným poskytovateľom dôveryhodných služieb. Táto právna podmienka nie je iba administratívna; ide o štrukturálny predpoklad, ktorý priamo ovplyvňuje prípustnosť

poskytovateľa, opätovné použitie existujúcej záruky dôveryhodných služieb, analýzu závislosti od CAB a predmet dohľadu zo strany NBÚ.

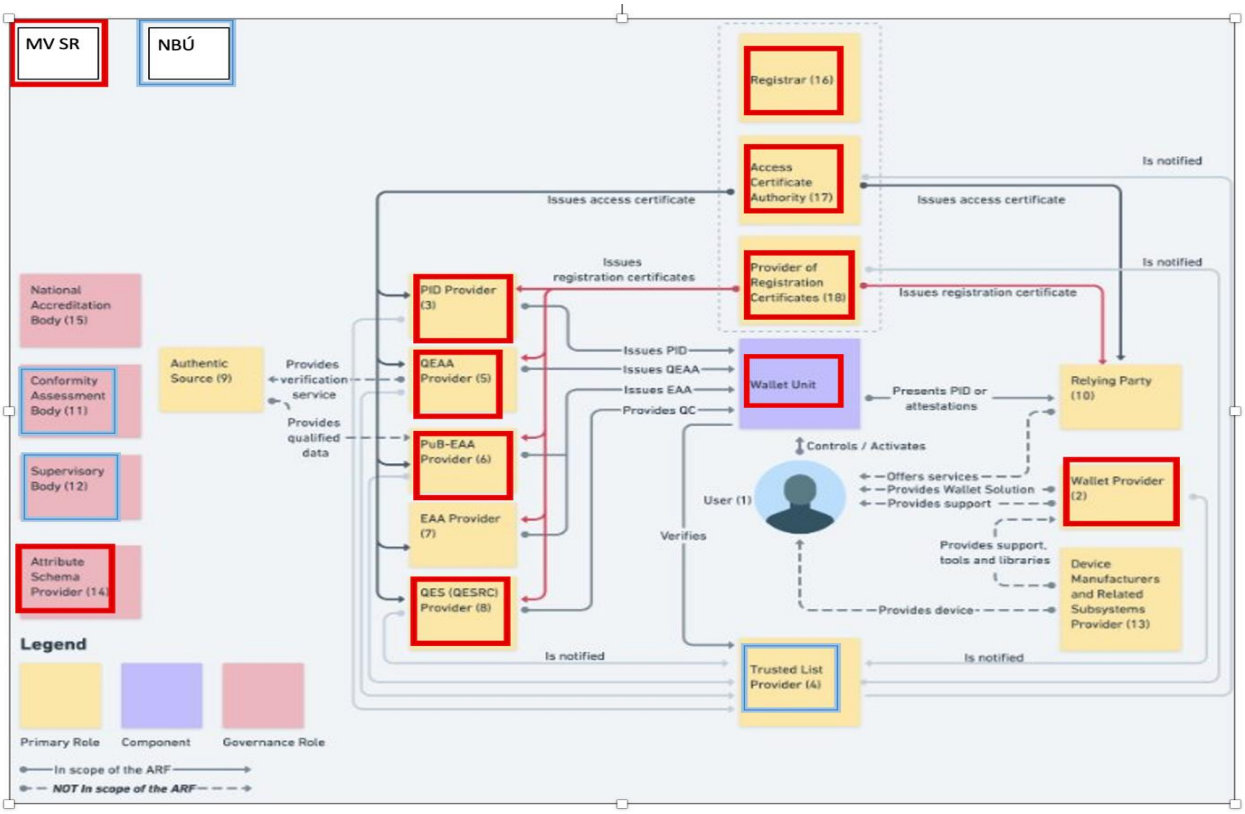
V rámci slovenskej národnej certifikačnej schémy musí riešenie peňaženky a jej prevádzkové prostredie spĺňať nielen požiadavky nariadenia eIDAS a vykonávacích aktov, ale aj všetky príslušné povinnosti vyplývajúce zo slovenskej legislatívy v oblasti kybernetickej bezpečnosti. To zahŕňa informačné systémy, siete, podpornú infraštruktúru a organizačné opatrenia používané na poskytovanie a prevádzku riešenia peňaženky.

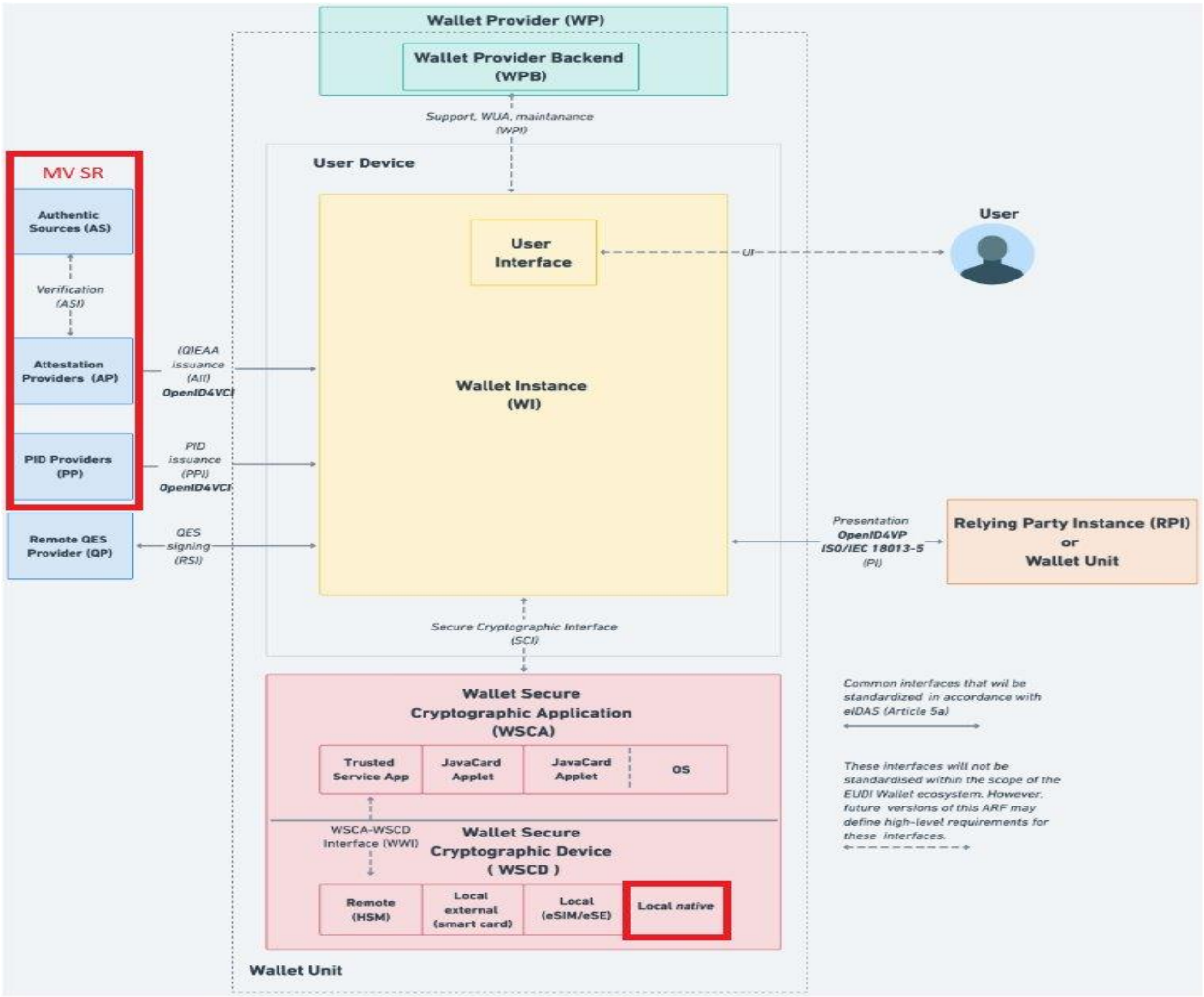
Poskytovateľ musí zabezpečiť, aby bolo riešenie peňaženky navrhnuté, implementované a prevádzkované v súlade s bezpečnostnými opatreniami predpísanými pre príslušné kategórie podľa Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a jeho vykonávacieho nariadenia, vrátane zavedenia rámca riadenia informačnej bezpečnosti, analýzy a riešenia rizík, implementácie technických a organizačných opatrení, detekcie a riešenia incidentov, plánovania kontinuity, monitorovania bezpečnosti a v prípade potreby povinného auditu kybernetickej bezpečnosti. Dodržiavanie vnútroštátnych právnych predpisov v oblasti kybernetickej bezpečnosti tvorí neoddeliteľnú súčasť celkového hodnotenia certifikácie a môže poskytovať opätovne použiteľné informácie o zárukách, avšak až po tom, čo CAB posúdi ich vhodnosť a relevantnosť prostredníctvom analýzy závislostí.

1. Slovenský rámec pre európsku peňaženku digitálnej identity (EUDIW-SK) je postavený na slovenskom **zákone o dôveryhodných službách** (v znení neskorších predpisov), ktorý implementuje nariadenie eIDAS do slovenského práva s povinným dodržiavaním úrovne záruky vysoká.
2. **Kľúčové zainteresované strany a ich úlohy**

   Hlavní slovenskí aktéri v rámci certifikačného ekosystému:

Členský štát	Slovensko (SK)
Vlastník schémy	NBÚ (NOKC)
Dozorný orgán	NBÚ (SRD)
Národný orgán pre akreditáciu	SNAS
CAB	NBÚ (SAC)
Poskytovateľ peňaženky	MV SR (Ministerstvo vnútra)
Poskytovateľ systému eID	MV SR (Ministerstvo vnútra)


MV SR
NBÚ
Registrar (16)
Access Certificate Authority (17)
Provider of Registration Certificates (18)
Is notified
Issues access certificate
Issues access certificate
Issues registration certificates
Is notified
Issues registration certificate
National Accreditation Body (15)
Conformity Assessment Body (11)
Supervisory Body (12)
Attribute Schema Provider (14)
Authentic Source (9)
Provides verification service
Provides qualified data
PID Provider (3)
QEAA Provider (5)
PuB-EAA Provider (6)
EAA Provider (7)
QES (QESRC) Provider (8)
Issues PID
Issues QEAA
Issues EAA
Provides QC
Wallet Unit
Presents PID or attestations
Relying Party (10)
Controls / Activates
User (1)
Offers services
Provides Wallet Solution
Provides support
Wallet Provider (2)
Verifies
Provides support, tools and libraries
Device Manufacturers and Related Subsystems Provider (13)
Provides device
Is notified
Trusted List Provider (4)
Is notified
Legend
Primary Role
Component
Governance Role
In scope of the ARF
NOT In scope of the ARF


Wallet Provider (WP)
Wallet Provider Backend (WPB)
Support, WUA, maintanance (WPI)
User Device
MV SR
Authentic Sources (AS)
Verification (ASI)
Attestation Providers (AP)
PID Providers (PP)
Remote QES Provider (QP)
(Q)EAA issuance (AII) OpenID4VCI
PID issuance (PPI) OpenID4VCI
QES signing (RSI)
User Interface
UI
User
Wallet Instance (WI)
Secure Cryptographic Interface (SCI)
Presentation OpenID4VP ISO/IEC 18013-5 (PI)
Relying Party Instance (RPI) or Wallet Unit
Wallet Secure Cryptographic Application (WSCA)
Trusted Service App
JavaCard Applet
JavaCard Applet
OS
WSCA-WSCD Interface (WWI)
Wallet Secure Cryptographic Device (WSCD)
Remote (HSM)
Local external (smart card)
Local (eSIM/eSE)
Local native
Wallet Unit
Common interfaces that wil be standardized in accordance with eIDAS (Article 5a)
These interfaces will not be standardised within the scope of the EUDI Wallet ecosystem. However, future versions of this ARF may define high-level requirements for these interfaces.

3. **NBÚ (Národný bezpečnostný úrad):**
   a) Pôsobí ako **dozorný orgán** pre **dôveryhodné služby a rámec európskej peňaženky [slovenský zákon o dôveryhodnyých služách** č. 272/2016, § 11 písm. a), § 12 ods. 3].
   b) Pôsobí ako **jednotné kontaktné miesto** pre služby dôveryhodnosti, európske peňaženky a schémy elektronickej identifikácie [slovenský **zákon o službách dôveryhodnosti** č. 272/2016, § 11 písm. b)].
   c) Zodpovedá za **certifikáciu** kybernetickej bezpečnosti informačných a komunikačných technológií podľa zákona o kybernetickej bezpečnosti [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 11 písm. d)].
   d) Vedie **zoznam dôveryhodných subjektov** a národnú infraštruktúru na validáciu certifikátov [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 11 písm. i), § 11 písm. g)].
4. **Ministerstvo vnútra Slovenskej republiky:**
   a) Verejný orgán zodpovedný za **zabezpečenie** poskytovania európskej peňaženky [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 10a ods. 1 písm. b)].
   b) Zostavuje a vedie zoznam **dôverujúcich strán** [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 10a ods. 1 písm. a)].
   c) Zabezpečuje prepojenie **identifikačných údajov osoby (PID)** s peňaženkou [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 10a ods. 1 písm. c)].
   d) Pôsobí ako vydavateľ orgánu verejného sektora zodpovedný za **elektronické osvedčenie atribútov z** autentického zdroja **(PubEAA)** na základe údajov z národných **autentických zdrojov** [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 10a ods. 2, eIDAS čl. 3 ods. 46].
5. **Poskytovateľ európskej peňaženky:**
   a) Musí byť **kvalifikovaným poskytovateľom dôveryhodných služieb (QTSP)** alebo preukázať, že má na tento účel uzatvorenú zmluvu s takýmto poskytovateľom [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 10 ods. 1].
   b) Je požiadavka predložiť NBÚ **oznámenie o zámere** poskytovať peňaženku a platný **certifikát peňaženky** [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 10 ods. 2].
   c) Musí zaregistrovať **dôverujúce strany** po overení ich totožnosti a zabezpečení ich súhlasu s pravidlami peňaženky [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 10 ods. 5].
   d) Je povinný bezodkladne nahlásiť akékoľvek podozrenie z **nezákonného alebo podvodného použitia** NBÚ [slovenský **zákon** č. 272/2016 , § 10 ods. 6 písm. e)].

19. **Certifikačný rámec v slovenskom práve**
    1. **Predmet certifikácie:** Certifikácia sa musí vzťahovať na integrované poskytovanie a prevádzku **riešenia peňaženky** aj **schémy eID**, v rámci ktorého sa poskytuje [IA 2024/2981, čl. 3 ods. 2].
    2. **Udelenie kvalifikovaného statusu:** NBÚ udeľuje „kvalifikovaný status“ na základe **správy o posudzovaní zhody** vydanej akreditovaným **orgánom posudzovania zhody**

(CAB) [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 3 ods. 1 a § 11 písm. a)].

3. **Oznamovanie informácií Komisii:** NBÚ oznamuje Komisii na základe **správy o posudzovaní zhody** vydanej akreditovaným **orgánom posudzovania zhody (CAB)** [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 11 písm. e), eIDAS čl. 5a ods. 18 písm. a), b) a c) a čl. 5c ods. 3; IA 2024/2981, článok 14 ods. 2)].
4. **Akreditácia:** Certifikačné orgány musia byť akreditované v súlade s **normou EN ISO/IEC 17065:2012** [IA 2024/2981, čl. 9 ods. 1].
5. **Audity kybernetickej bezpečnosti:** Poskytovatelia peňaženiek musia predložiť NBÚ záverečnú správu o výsledkoch **auditu kybernetickej bezpečnosti** [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 3 ods. 1 písm. c)].
6. **Úroveň záruky vysoká:** Národná schéma vyžaduje, aby riešenia peňaženiek boli odolné voči útočníkom s **vysokým útočným potenciálom**, pričom sa overuje dodržiavanie úrovne záruky vysoká stanoveného v **nariadení (EÚ) 2015/1502** [IA 2024/2981, čl. 8 ods. 2].

20. **Proces verifikácie a dohľadu**

1. **Podanie:** Poskytovateľ predloží svoj zámer a technické certifikáty NBÚ [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 10 ods. 2].
2. **Verifikácia:** NBÚ verifikuje, či poskytovateľ spĺňa požiadavky **zákona o dôveryhodných službách** a nariadenia eIDAS [slovenský **zákon o dôveryhodných službách** č. 272/2016, § 10 ods. 3].
3. **Odstránenie** nedostatkov**:** Ak sa zistia nedostatky, NBÚ pozastaví konanie a vyzve poskytovateľa, aby ich odstránil v stanovenej lehote [slovenský **zákon o službách dôvery** č. 272/2016, § 10 ods. 3].
4. **Dohľad:** Po začatí prevádzky NBÚ vykonáva priebežné **inšpekcie** a monitorovanie s cieľom zabezpečiť trvalé dodržiavanie predpisov [slovenský **zákon** č. 272/2016 , § 12 ods. 1].
5. Z hľadiska certifikácie NBÚ:
   a) udeľuje kvalifikovaný status na základe správy o posudzovaní zhody,
   b) overuje dodržiavanie vnútroštátnych požiadaviek a požiadaviek nariadenia eIDAS,
   c) vykonáva priebežný dohľad a inšpekcie.

21. **Posudzovanie zhody a kvalifikovaný status pre QTSP**

1. Proces prebieha podľa štruktúrovaného postupu:
   a) Posudzovanie zhody vykonáva orgán posudzovania zhody (CAB) s akreditáciou podľa normy EN ISO/IEC 17065:2012.
   b) CAB vydáva správu o posudzovaní zhody.
   c) NBÚ udeľuje kvalifikovaný status na základe tejto správy.
   d) Poskytovateľ musí predložiť aj záverečnú správu z auditu kybernetickej bezpečnosti.

2. Podľa § 10 ods. 1 slovenského **zákona o dôveryhodných službách** č. 272/2016 musí poskytovateľ riešenia peňaženky spĺňať požiadavku:

3. „Poskytovateľom európskej peňaženky je osoba, ktorá je kvalifikovaným poskytovateľom dôveryhodných služieb alebo preukáže, že na tento účel uzavrela zmluvu s kvalifikovaným poskytovateľom dôveryhodných služieb a spĺňa požiadavky stanovené v článku 5a nariadenia (EÚ) č. 910/2014 v znení neskorších zmien a doplnení."

4. Podľa **slovenského zákona o dôveryhodných službách** č. 272/2016 je certifikačné rozhodnutie CAB kľúčovým podkladom pre NBÚ. Poskytovateľ dôveryhodných služieb bez kvalifikovaného statusu musí predložiť certifikát a záverečnú správu NBÚ, aby mu bol udelený kvalifikovaný status a bol zaradený do zoznamu dôveryhodných subjektov. Akákoľvek CAB, ktorá si neudrží akreditáciu alebo u ktorej sa zistia nezhody, musí o tom bezodkladne informovať NBÚ.

22. **Slovenská regulácia Integrácia NIS2 do zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.**

1. **Zhoda s implementáciou NIS2 – povinný audit a bezpečnostné požiadavky pre verejný sektor.**

a) V rámci slovenskej národnej certifikačnej schémy pre európsku peňaženku digitálnej identity je Ministerstvo vnútra ako poskytovateľ riešenia pre peňaženku verejného sektora povinné zabezpečiť plné dodržiavanie nielen požiadaviek nariadenia eIDAS a vykonávacích aktov, ale aj všetkých platných povinností vyplývajúcich zo slovenskej legislatívy v oblasti kybernetickej bezpečnosti.

b) Riešenie peňaženky a jej prevádzkové prostredie musia byť v súlade s požiadavkami zákona č. 69/2018 Z. **z**. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len **„zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti")**, vrátane všetkých vykonávacích predpisov vydaných na jeho základe. Táto povinnosť sa vzťahuje na informačné systémy, siete, podpornú infraštruktúru a organizačné opatrenia používané na poskytovanie a prevádzku riešenia peňaženky.

c) Ministerstvo vnútra zabezpečí, aby bolo riešenie peňaženky navrhnuté, implementované a prevádzkované v súlade s bezpečnostnými opatreniami stanovenými pre prevádzkovateľov základných služieb alebo iných príslušných kategórií podľa zákona o kybernetickej bezpečnosti, podľa toho, čo sa uplatňuje. To zahŕňa vytvorenie rámca riadenia informačnej bezpečnosti, procesy analýzy rizík a ošetrenia rizík informačnej bezpečnosti, implementáciu technických a organizačných bezpečnostných opatrení, schopnosti detekcie a riešenia incidentov, plánovanie kontinuity a pravidelné monitorovanie bezpečnosti.

d) Ak je to vyžadované zákonom, ministerstvo sa podrobí auditom kybernetickej bezpečnosti vykonávaným autorizovanými audítormi a predloží záverečnú audítorskú správu Národnému bezpečnostnému úradu. Zistené nezhody sa odstránia v predpísaných lehotách a nápravné opatrenia sa preukázateľne vykonajú a zdokumentujú.

e) Dodržiavanie zákona o kybernetickej bezpečnosti tvorí neoddeliteľnú súčasť celkového posudzovania certifikácie. Orgán posudzovania zhody a Národný bezpečnostný úrad zohľadnia výsledky dohľadu a auditov v oblasti kybernetickej bezpečnosti pri hodnotení, či riešenie peňaženky spĺňa požiadavky na certifikáciu EUDIW-SK na úrovni záruky vysoká.

f) Zahrnutím úplného súboru vnútroštátnych povinností v oblasti kybernetickej bezpečnosti do certifikačného rámca slovenský systém zabezpečuje, že európska peňaženka digitálnej identity nie je posudzovaná izolovane ako technický produkt,

ale ako kritická verejná digitálna infraštruktúra fungujúca v rámci komplexného a vynútiteľného bezpečnostného režimu.

23. **Vzťah k iným európskym rámcom a normám**

a) Súčasná slovenská schéma čerpá inšpiráciu z nasledujúcich právnych predpisov a v prípade potreby ich využíva: nariadenie (EÚ) 2019/881, vykonávacie nariadenie Komisie (EÚ) 2024/2981, vykonávacie nariadenie Komisie (EÚ) 2025/2162, nariadenia eIDAS v znení neskorších zmien a doplnení, smernica (EÚ) 2022/2555, národnej transpozícii smernice NIS2, noriem ETSI EN 319 401, ETSI EN 319 403-1, ISO/IEC 17065, ISO/IEC 17000, ISO/IEC 17029, ISO/IEC 15408 a súvisiacich technických materiálov. Tieto odkazy neznamenajú, že každý uvedený dokument sa automaticky stáva priamou normatívnou požiadavkou pre každý certifikát. Skôr tvoria hodnotený korpus, z ktorého sa odvodzuje štruktúra schémy, očakávania týkajúce sa spôsobilostí CAB, logika hodnotenia a pravidlá opätovného použitia dôkazov.

b) Schéma sa zámerne vyhýba nadmernému predpisovaniu noriem spôsobom, ktorý by zbytočne obmedzoval akreditáciu alebo vynucoval predčasný záväzok voči technickým rámcom, ktoré sa stále vyvíjajú. Preferovaným prístupom je využitie nariadenia eIDAS, vykonávacích aktov, štruktúry referenčného rámca architektúry a konceptu základných noriem ako normatívneho základu, pričom sa ponecháva priestor na odôvodnený a dobre zdokumentovaný výber najvhodnejších technických noriem a zdrojov dôkazov v každom profile alebo module.

24. **Uplatniteľnosť CRA a dôkazov zameraných na produkt**

Ak sa Nariadenie o kybernetickej odolnosti alebo iné povinnosti zamerané na produkt vzťahujú na jeden alebo viacero produktov integrovaných do ekosystému peňaženky, poskytovateľ peňaženky, ktorý vystupuje ako globálny správca riešení, by mal poskytnúť zdokumentované mapovanie, ktoré ukazuje, ako existujúce certifikáty alebo technické dôkazy zodpovedajú platným požiadavkám na produkt a kde zostávajú zvyškové nedostatky. Ak existujúce certifikáty úplne nepokrývajú platné požiadavky, poskytovateľ musí poskytnúť dodatočné dôkazy, aby CAB mohla posúdiť zhodu integrovaného riešenia bez toho, aby boli dotknuté povinnosti skutočného výrobcu alebo dodávateľa.

25. **Strategické postavenie slovenskej schémy**

Zo strategického hľadiska sa slovenská schéma profiluje ako prechodná, ale obhajiteľná národná schéma, ktorá maximalizuje opätovné využitie existujúcich vyspelých ekosystémov záruky, namiesto toho, aby sa pokúšala o ich prestavbu. Jej cieľom nie je preformulovať všetky pravidlá, ktoré už sú obsiahnuté v európskom práve alebo podrobných normách, ale prepojiť ich do auditovateľnej a na národnej úrovni funkčnej schémy. Toto postavenie je obzvlášť dôležité pre budúce vzájomné hodnotenie, budúcu európsku porovnateľnosť a dlhodobú udržateľnosť certifikátov, správ a opätovne použitých dôkazov.

ODKAZY (pôvodná schéma EÚ)

a) Táto schéma odkazuje na tieto nariadenia:

1) 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 (zákon o kybernetickej bezpečnosti)

2) Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskej certifikačnej schémy kybernetickej bezpečnosti založenej na spoločných kritériách (EUCC)

3) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183 z 11. apríla 2024, ktorým sa mení a dopĺňa nariadenie (EÚ) č. 910/2014, pokiaľ ide o vytvorenie európskeho rámca pre digitálnu identitu

4) Vykonávacie nariadenie Komisie (EÚ) 2024/2981 z 28. novembra 2024, ktorým sa stanovujú pravidlá na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o certifikáciu európskych peňaženiek digitálnej identity

5) Vykonávacie nariadenie Komisie (EÚ) 2025/2162 z 27. októbra 2025, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014, pokiaľ ide o akreditáciu orgánov posudzovania zhody vykonávajúcich posudzovanie kvalifikovaných poskytovateľov dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, ktoré poskytujú, správu o posudzovaní zhody a schému posudzovania zhody

6) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Únii, ktorou sa mení a dopĺňa nariadenie (EÚ) č. 910/2014 a smernicu (EÚ) 2018/1972 a ktorou sa zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

7) Vykonávacie nariadenie Komisie (EÚ) 2024/2690 zo 17. októbra 2024, ktorým sa stanovujú pravidlá na uplatňovanie smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia riadenia rizík v oblasti kybernetickej bezpečnosti a ďalšie špecifikácie prípadov, v ktorých sa incident považuje za významný, pokiaľ ide o poskytovateľov služieb DNS, registrov názvov TLD, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátových centier, poskytovateľov sietí na doručovanie obsahu, poskytovateľov spravovaných služieb, poskytovateľov spravovaných bezpečnostných služieb, poskytovateľov online trhovísk, online vyhľadávačov a platforiem sociálnych sietí a poskytovateľov dôveryhodných služieb

8) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách na kybernetickú bezpečnosť pre výrobky s digitálnymi prvkami a o zmene a doplnení nariadení (EÚ) č. 168/2013 a (EÚ) č. 2019/1020 a smernice (EÚ) 2020/1828 (zákon o kybernetickej odolnosti)

b) Odvoláva sa tiež na tieto normy a technické špecifikácie:

1) ISO/IEC 17000:2020 – Posudzovanie zhody – Slovník a všeobecné zásady,

2) ISO/IEC 17065:2012 – Posudzovanie zhody – Požiadavky na orgány certifikujúce výrobky, procesy a služby,

3) ISO/IEC 17021-1:2015 – Posudzovanie zhody – Požiadavky na orgány poskytujúce audit a certifikáciu systémov manažérstva – Časť 1: Požiadavky,

4) ISO/IEC 17025:2017 – Posudzovanie zhody – Všeobecné požiadavky na spôsobilosť skúšobných a kalibračných laboratórií,

5) ISO/IEC 17029:2019 – Posudzovanie zhody – Všeobecné zásady a požiadavky na validačné a verifikačné orgány,

6) ISO/IEC 15408:2022, časti 1 až 5 – Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia – Hodnotiace kritériá pre bezpečnosť IT (spoločné kritériá),

7) CEN TS 18072 – Požiadavky na orgány posudzovania zhody certifikujúce služby IKT,

8) EN 17640:2022, „Metodika hodnotenia kybernetickej bezpečnosti s pevne stanoveným časovým rámcom pre produkty IKT“

9) ETSI EN 319 401 – Elektronické podpisy a infraštruktúry dôvery (ESI); Všeobecné požiadavky na politiku poskytovateľov dôveryhodných služieb. Použije sa najnovšia platná uverejnená verzia, pričom verzia 3.2.1 / január 2026 sa považuje za základnú verziu zohľadnenú pri príprave tejto schémy, pokiaľ nebude aktualizovaná prostredníctvom procesu údržby schémy.

10) EN ETSI 319 403-1: „Elektronické podpisy a infraštruktúry (ESI); Posudzovanie zhody poskytovateľov dôveryhodných služieb; Časť 1: Požiadavky na orgány posudzovania zhody posudzujúce poskytovateľov dôveryhodných služieb“.

c) Súvisiace slovenské právne predpisy:

1) **Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti**

2) Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (**Zákon o dôveryhodných službách**)

3) **Nariadenie vlády č. 227/2025 Z. z**. k **zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti** (bezpečnostné požiadavky – implementácia smernice NIS 2)

4) **Zákon č. 71/1967 Z. z. o správnom konaní v znení neskorších predpisov.**

5) **Zákon č. 9/2010 Z. z. o sťažnostiach, v znení neskorších predpisov.**

6) **Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.**

7) **Zákon č. 215/2004 Z. z. o ochrane utajovaných informácií a o zmenách a doplneniach niektorých zákonov.**

8) Ďalšie posudzované zdroje:

   a. ISO/IEC 17011: 2017 Posudzovanie zhody – Požiadavky na orgány akreditácie akreditujúce orgány posudzovania zhody

   b. ISO/IEC 17029: 2019 Posudzovanie zhody – Všeobecné zásady a požiadavky na validácia a verifikácia orgány

   c. ISO/IEC DIS 17007: 2026 – Posudzovanie zhody – Usmernenia pre vypracovanie normatívnych dokumentov vhodných na použitie pri posudzovaní zhody

   d. ISO/IEC DRT 17032:2019 – Posudzovanie zhody – Návody a príklady certifikačnej schémy pre procesy

9) ENISA, *Bezpečnostné požiadavky na poskytovateľov služieb súvisiacich s peňaženkami, verzia 0.5.614, marec 2026, na základe EN 319 401*. Používa sa ako externý technický referenčný dokument na interpretáciu bezpečnostných požiadaviek súvisiacich s peňaženkami, priradenia v registri rizík, priradenia noriem a priradenia podľa nariadenia (EÚ) 2015/1502. Tento dokument nie je reprodukovaný

v slovenskej národnej schéme a má sa používať v pôvodnej verzii, pričom jeho použiteľnosť posudzuje CAB.

10) FCAF je dostupný na Github (https://github.com/eu-digital-identity-wallet/eudi-doc-functional-conformance-assessment) alebo https://conformance.eudi.dev/latest-draft/

1. Všeobecné požiadavky (normatívne)

1.1. Predmet a rozsah pôsobnosti

1. Tento dokument stanovuje slovenskú národnú certifikačnú schému (EUDIW-SK) založenú na európskej kandidátskej schéme certifikačnej schémy kybernetickej bezpečnosti pre európske digitálne peňaženky (EUDIW), ako sa uvádza v článku 5c ods. 2 nariadenia (EÚ) č. 910/2014.
2. Táto schéma sa vzťahuje na všetky služby informačných a komunikačných technológií („IKT“), vrátane ich dokumentácie, ktoré sa predkladajú na certifikáciu v rámci EUDIW, a podporuje vydávanie certifikátov pre kyberbezpečnosť nasledujúcich typov služieb IKT:
    a) služby na poskytovanie a prevádzku riešení peňaženiek a schém elektronickej identifikácie („eID“), v rámci ktorých sa poskytujú;
    b) služby na poskytovanie a prevádzku riešení peňaženiek;
    c) služby na poskytovanie identifikačných údajov osoby (PID) na účely poskytovania schémy eID, v rámci ktorej sa poskytuje peňaženka európskej digitálnej identity;
    d) služby používané na validáciu platnosti jednotiek peňaženiek a dôverujúcich strán;
    e) požiadavky slovenských vnútroštátnych právnych predpisov na prevádzku poskytovateľov riešení EUDIW (SP).
3. Systém zahŕňa certifikáciu kybernetickej bezpečnosti peňaženiek európskej digitálnej identity (EUDI), ako sa vyžaduje v článku 5c ods. 2 nariadenia (EÚ) č. 910/2014 a v súlade s európskym rámcom certifikácie kybernetickej bezpečnosti stanoveným v nariadení (EÚ) 2019/881, konkrétne v európskom nariadení o kybernetickej bezpečnosti (CSA).

1.2. Vymedzenie pojmov

1. Na účely tejto schému sa uplatňujú definície uvedené v nariadení (EÚ) 2019/881, nariadení (EÚ) č. 910/2014, vykonávacom nariadení Komisie (EÚ) 2024/2981 a v prílohe XV k tomuto schému.
2. Na účely jednotného výkladu v slovenskej národnej schéme sa zdôrazňujú tieto pojmy:
    - riešenie peňaženky, inštancia peňaženky, jednotka peňaženky, bezpečná kryptografická aplikácia peňaženky (WSCA), bezpečné kryptografické zariadenie peňaženky (WSCD), kritické aktíva, používateľ peňaženky a poskytovateľ peňaženky majú význam, ktorý im priraďuje vykonávacie nariadenie Komisie (EÚ) 2024/2981;
    - vlastník schémy znamená slovenský orgán zodpovedný za udržiavanie tejto národnej certifikačnej schémy a koordináciu jej budúcich aktualizácií;
    - národný certifikačný orgán pre kybernetickú bezpečnosť / NCCA znamená NBÚ, keď koná v úlohe pridelené nariadením (EÚ) 2019/881 a slovenským zákonom o kybernetickej bezpečnosti;
    - certifikačný orgán alebo CAB znamená orgán posudzovania zhody akreditovaný a, ak je to vhodné, oprávnený vykonávať certifikačné činnosti v

rámci tejto schémy;

- držiteľ certifikátu znamená právnickú osobu zodpovednú za certifikovanú službu IKT a za udržanie certifikovaného stavu počas platnosti certifikátu;
- incident, zraniteľnosť, nezhoda, podstatná zmena, opakovane použiteľné informácie o záruke, závislosť a predpoklad prevádzkového prostredia sa vykladajú v súlade s kapitolami 5 až 8 a prílohami II, IX, X a XI;
- požiadavka na kvalifikovaného poskytovateľa dôveryhodných služieb (QTSP) znamená slovenský právny predpis, podľa ktorého musí byť poskytovateľ riešenia peňaženky kvalifikovaným poskytovateľom dôveryhodných služieb (QTSP) alebo musí preukázať platnú zmluvnú dohodu s kvalifikovaným poskytovateľom dôveryhodných služieb (QTSP), ak to vyžaduje slovenské právo.

3. Niektoré definície slúžia na doplnenie definícií uvedených v nariadení (EÚ) 2019/881 (CSA), nariadení (EÚ) č. 910/2014 (eIDAS) a nariadení (EÚ) 2024/2981. Úplnejší zoznam pojmov je uvedený v prílohe XV.

1.3. Úroveň záruky

1. Certifikačné orgány vydávajú certifikáty EUDIW-SK na úroveň záruky vysoká, ako je definované v článku 52 ods. 7 nariadenia (EÚ) 2019/881.

1.4. Vlastné posúdenie zhody

1. Samohodnotenie zhody v zmysle článku 53 nariadenia (EÚ) 2019/881 nie je povolené.

2. Hodnotiace kritériá a metódy (normatívne)

2.1. Hodnotiace kritériá pre služby IKT EUDIW-SK

1. Služba IKT predložená na certifikáciu sa musí vyhodnotiť aspoň z hľadiska zhody s:
   a) platnými kritériami definovanými v prílohe X;
   b) špecifickými kritériami týkajúcimi sa používania komponentov služby IKT, založenými na predpokladoch a usmerneniach pre používateľov poskytnutých pre každý komponent a na analýze závislostí informácií o záruke dostupných pre každý komponent.
   c) Externý technický odkaz: Bezpečnostné požiadavky na poskytovateľov služieb súvisiacich s peňaženkami, verzia 0.5.614, marec 2026, na základe normy EN 319 401, vrátane jej prepojení s normami, referenčnými dokumentmi, registrom rizík EUDIW a nariadením CIR (EÚ) 2015/1502[1] . Účelom tohto odkazu je podporiť interpretáciu hodnotiacich kritérií prílohy X, najmä v prípadoch, keď je potrebné priradiť požiadavky špecifické pre peňaženky, poskytovateľov PID, validačné služby alebo súvisiace s registrom rizík ku konkrétnym opatreniam, dôkazom a hodnotiacim činnostiam. Ak

[1] Alebo posledná dostupná verzia

odkazovaný dokument obsahuje požiadavky, priradenia alebo poznámky k posudzovaniu zhody, ktoré sú relevantné pre predmet certifikácie na Slovensku, CAB ich použije ako technický podklad pre plán hodnotenia, preskúmanie posúdenia rizík a priradenie kritérií k dôkazom. Slovenská schéma nezahŕňa odkazovaný dokument formou úplného textového prepisovania, pretože dokument je rozsiahly, vyvíja sa a je určený na použitie ako technický základ, ktorý môže byť aktualizovaný nezávisle.

2. V prípade neexistencie platných noriem a technických špecifikácií sú hodnotiace kritériá uplatniteľné v tomto schéme definované v prílohe k schéme.

2.2. Metódy hodnotenia služieb IKT v rámci EUDIW-SK

1. Služba IKT predložená na certifikáciu sa musí hodnotiť minimálne v súlade s metódami definovanými v prílohe XI.
2. V prípade služby IKT, ktorá prechádza hodnotením zložených služieb, ako je definované v prílohe IX, CAB, ktorá vykonala hodnotenie základnej služby IKT, poskytne príslušné informácie CAB vykonávajúcej hodnotenie zloženej služby IKT.
3. V prípade služby IKT, ktorá obsahuje komponent certifikovaný v rámci európskej certifikačnej schémy pre kybernetickú bezpečnosť, CAB, ktorý vydal certifikát pre tento komponent, poskytne príslušné informácie CAB vykonávajúcemu hodnotenie služby IKT.
4. Poskytovateľ IKT služieb EUDIW-SK sa podľa slovenského práva hodnotí ako QTSP.
5. Metodika hodnotenia služieb IKT EUDIW-SK vychádza z normy ETSI EN 319 403-1 (vychádza z normy EN ISO/IEC 17065), doplnená o procesné požiadavky a metódy z technickej špecifikácie CEN TS 18072 a o špecifické metódy a požiadavky na metódy definované v prílohe schémy.
6. Metodika hodnotenia služieb IKT v rámci EUDIW-SK vychádza z normy ETSI EN 319 403-1, ktorá sama vychádza z normy EN ISO/IEC 17065 pre certifikáciu služieb, a je doplnená procesnými požiadavkami a metódami odvodenými z CEN TS 18072 a metódami špecifickými pre toto schéma definovanými v prílohe XI. Táto kombinácia je nevyhnutná, pretože schéma sa opiera o požiadavky na vysokej úrovni, komplexné a modulárne hodnotenie, opätovné použitie informácií o záruke z rôznych zdrojov a úroveň záruky vysoká.
7. Certifikačný orgán (CAB) musí byť preto pripravený vykonávať nielen audítorské činnosti, ale aj inšpekčné a v prípade potreby aj skúšacie činnosti. Audítorské činnosti sa používajú predovšetkým na posúdenie riadenia, organizačných a prevádzkových procesov poskytovateľa. Inšpekčné činnosti sa používajú na overenie technickej architektúry, konfigurácie, integračnej logiky, návrhových predpokladov a mechanizmov vynútiteľnosti. Skúšacie činnosti sa používajú v prípadoch, keď funkčná zhoda, odolnosť voči zraniteľnosti alebo zostatkové nedostatky v opätovne použitých informáciách o záruke vyžadujú priame technické overenie.
8. CAB uplatňuje trojstupňovú logiku hodnotenia pre všetky služby a procesy v predmete pôsobnosti: po prvé, potvrdenie správnosti informácií predložených poskytovateľom; po druhé, potvrdenie vhodnosti návrhu a opatrení na splnenie príslušných hodnotiacich kritérií; a po tretie, potvrdenie prevádzkovej účinnosti týchto opatrení počas stanoveného

obdobia alebo, v prípade počiatočnej certifikácie, prostredníctvom dôkazov zhromaždených priamo počas testov, pilotných projektov alebo kontrolovanej prevádzky.

9. Ak sa certifikácia opiera o zloženie v rámci schémy alebo o dôkazy z iných schém, ako sú EUCC, audity založené na ETSI, ISO/IEC 27001 alebo národné audity kybernetickej bezpečnosti, CAB vykoná analýzu závislosti a prípustnosti pred opätovným použitím takýchto dôkazov. Táto analýza overí predmet, úroveň záruky vysoká, spôsobilosť vydavateľa, platnosť, predpoklady, nezhody a potrebu kompenzačných opatrení alebo zostávajúcich činností CAB. Opätovné použitie dôkazov sa odporúča, avšak len v prípade, ak bola preukázaná ich relevantnosť a primeranosť.
10. Posudzovanie zhody sa považuje za odlišné od hodnotenia zabezpečenia kybernetickej bezpečnosti. Funkčné testy, či už založené na rámci posudzovania zhody (FCAF)[2] , určených národných súboroch integračných testov alebo ekvivalentných technických špecifikáciách, sa nesmú používať ako náhrada za činnosti hodnotenia bezpečnosti požadované pre úroveň záruky vysoká. Podobne sa posudzovanie zraniteľnosti a penetračné testovanie musia plánovať a vykonávať spôsobom primeraným architektonickému profilu, kritickosti komponentu a zostatkovému vystaveniu po opätovnom použití iných informácií o zabezpečení.
11. Poskytovateľ služieb IKT EUDIW-SK sa v súlade so slovenským právom posudzuje aj v kontexte povinností týkajúcich sa dôveryhodných služieb a národnej kybernetickej bezpečnosti, ak sú relevantné pre predmet služby. CAB preto zohľadní nielen priame artefakty produktu alebo služby, ale aj súvisiaci životný cyklus, Riadenie zmien, riadenie incidentov, riadenie zraniteľností, riadenie verzií, mechanizmy aktualizácie a ďalšie prevádzkové opatrenia potrebné na udržanie certifikovaného stavu služby v čase.
12. Certifikačný orgán použije externý technický referenčný dokument o bezpečnostných požiadavkách na poskytovateľov služieb súvisiacich s peňaženkami ako podporný zdroj pri výbere hodnotiacich činností podľa prílohy XI. Tento dokument nenahrádza metódy uvedené v prílohe XI. Namiesto toho pomáha CAB určiť, ktoré požiadavky možno posúdiť prostredníctvom auditu, inšpekcie, funkčného skúšania, špecifického skúšania, interaktívneho skúšania, posúdenia zraniteľnosti, penetračného skúšania alebo analýzy závislostí. Ak uvedený dokument navrhuje poznámky k posudzovaniu zhody, tieto poznámky sa považujú za usmernenia, pokiaľ nie sú stanovené ako povinné touto schémou, prílohou X, prílohou XI alebo príslušnými právnymi predpismi Únie alebo Slovenskej republiky.

2.3. Subdodávanie hodnotiacich činností

Ak CAB zadáva hodnotiace činnosti subdodávateľom, MUSÍ dodržiavať článok 10 vykonávacieho nariadenia Komisie (EÚ) 2024/2981 a niesť plnú zodpovednosť za všetky subdodávateľské činnosti a ich výsledky. Subdodávatelia vykonávajúci skúšobné, inšpekčné, audítorské alebo validačné/verifikačné činnosti MUSIA spĺňať príslušné normy spôsobilosti, vrátane EN ISO/IEC 17025 pre skúšanie, EN ISO/IEC 17020 pre inšpekciu, EN ISO/IEC 17021-1 pre audítorské činnosti a EN ISO/IEC 17029

[2] V čase certifikácie by sa mala používať posledná verzia FCAF

pre validačné alebo verifikačné činnosti, ak je to relevantné pre subdodávateľskú úlohu.

CAB MUSÍ identifikovať všetky subdodávateľské hodnotiace činnosti v pláne hodnotenia, posúdiť a zdokumentovať spôsobilosť, nestrannosť, dôvernosť a opatrenia na ochranu informácií subdodávateľa a zabezpečiť, aby boli výsledky subdodávateľských činností preskúmané predtým, ako sa na ne bude spoliehať. CAB MUSÍ informovať NBÚ / vlastníka schémy pred zadávaním subdodávateľských činností v oblasti hodnotenia citlivých na bezpečnosť, pokiaľ akreditácia, autorizácia alebo slovenské právo nestanovujú prísnejšie požiadavky na schválenie.

3. Vydávanie, obnovenie a odňatie certifikátov EUDIW -SK(normatívne)

3.1. Informácie potrebné na certifikáciu

1. Žiadateľ o certifikáciu podľa EUDIW-SK poskytne certifikačnému orgánu alebo mu iným spôsobom zabezpečí dostupnosť všetkých informácií potrebných na činnosti posudzovania zhody.
2. Informácie uvedené v odseku 1 musia obsahovať informácie uvedené v prílohe IV.
3. Žiadatelia o certifikáciu môžu certifikačnému orgánu poskytnúť primerané výsledky hodnotenia z predchádzajúcich posudzovaní zhody podľa:
    a) tejto schémy;
    b) európska certifikačná schéma kybernetickej bezpečnosti prijatá podľa článku 49 nariadenia (EÚ) 2019/881;
    c) kvalifikácie a certifikácie orgánmi posudzovania zhody akreditovanými podľa požiadaviek nariadenia (EÚ) 2025/2162;
    d) certifikácie orgánmi posudzovania zhody určenými členskými štátmi, ako sa uvádza v článku 12a ods. 1 a článku 30 ods. 1 nariadenia (EÚ) č. 910/2014;
    e) posudzovanie zhody v rámci akejkoľvek schémy orgánom posudzovania zhody akreditovaným národným akreditačným orgánom členského štátu EÚ v súlade s nariadením (EÚ) č. 765/2008 na vydávanie takýchto posudkov o zhode;
    f) povinný interný audit podľa slovenského zákona o kybernetickej bezpečnosti **č. 69/2018 Z. z. o kybernetickej bezpečnosti**
    g) slovenský **zákon o dôveryhodných službách** – audit QTSP a kvalifikovaný status.
4. Po potvrdení pravosti výsledkov hodnotenia a po analýze vhodnosti, relevantnosti a zhody výsledkov hodnotenia s platnými požiadavkami môže certifikačný orgán výsledky hodnotenia opätovne použiť v súlade s výsledkami analýzy.
5. Žiadatelia o certifikáciu poskytnú certifikačnému orgánu aj odkaz na svoju webovú stránku, ktorá obsahuje informácie, ktoré majú byť verejne dostupné, ako je definované v prílohe III.
6. Všetku relevantnú dokumentáciu uvedenú v tejto časti uchová certifikačný orgán a žiadateľ po dobu 5 rokov po uplynutí platnosti certifikátu.

7. Žiadateľ o certifikáciu musí poskytnúť všetky informácie požadované certifikačným orgánom a odporúča sa, aby poskytol výsledky predchádzajúcej certifikácie relevantných zložiek svojej služby, napríklad v rámci EUCC, v rámci schém súvisiacich s nariadením eIDAS alebo v rámci iných schém posudzovania zhody založených na akreditácii schém posudzovania zhody.

8. Uvedené informácie musia obsahovať minimálne kategórie informácií uvedené v prílohe IV. Zoznam v prílohe IV je zámerne komplexný, ale nie je vyčerpávajúci. Žiadateľ naďalej nesie zodpovednosť za poskytnutie akýchkoľvek dodatočných informácií, prístupu, technických artefaktov, odôvodnení alebo vysvetľujúcich materiálov potrebných na to, aby certifikačný orgán mohol bez námietok dospieť k záveru o dostatočnosti, vhodnosti a účinnosti poskytnutých dôkazov.
9. Žiadatelia o certifikáciu môžu certifikačnému orgánu poskytnúť primerané výsledky hodnotenia z predchádzajúcich posúdení zhody, vrátane výsledkov v rámci tejto schémy, európskych certifikačných schém kybernetickej bezpečnosti prijatých podľa nariadenia (EÚ) 2019/881, kvalifikácie a certifikácie orgánmi posudzovania zhody akreditovanými podľa CIR (EÚ) 2025/2162, posúdenia poskytovateľov dôveryhodných služieb, posudzovanie zhody v rámci iných akreditovaných schém, povinné audity podľa slovenského zákona o kybernetickej bezpečnosti a výstupy z auditov a dohľadu súvisiace so statusom kvalifikovaného poskytovateľa dôveryhodných služieb.
10. Po potvrdení pravosti výsledkov hodnotenia a analýze ich vhodnosti, zrelosti, relevantnosti, predmetu, predpokladov a zhody s platnými požiadavkami môže certifikačný orgán tieto výsledky opätovne použiť len v rozsahu odôvodnenom analýzou závislostí definovanou v schéme. CAB určí, či dôkazy možno prijať bez ďalších činností, prijať s kompenzačnými kontrolami, prijať s dodatočným skúšaním alebo inšpekciou CAB , alebo zamietnuť na účely súčasnej certifikácie.
11. Žiadateľ štruktúruje podanie tak, aby certifikačný orgán mohol vysledovať požiadavky k implementovaným opatreniam, implementované opatrenia k systémovým komponentom a prevádzkovým procesom a tieto komponenty a procesy ku konkrétnym dôkazom. Žiadateľ by mal najmä poskytnúť ucelený balík zahŕňajúci právny a organizačný kontext, architektúru a predpoklady, bezpečnostné opatrenia a úroveň záruky vysoká, opätovne použiteľné informácie o záruke, posúdenie rizík a plánovanie hodnotenia, artefakty implementácie, artefakty riadenia zraniteľností a incidentov a povinnosti v oblasti informovania verejnosti.
12. Ak sa poskytovateľ pri zdôvodňovaní zhody opiera o základné normy, návrhy noriem, architektonické rámce alebo certifikáty komponentov, vysvetlí, ako boli požiadavky interpretované a uplatnené, ako sa riešili odchýlky alebo neuplatniteľné časti a ako sa zmierňujú zvyškové rizika. Ak chýbajú určité relevantné dôkazy alebo sú nedostatočné, certifikačný orgán môže proces pozastaviť alebo prerušiť, kým nebudú poskytnuté chýbajúce informácie.
13. Vzhľadom na predmet a očakávanú hĺbku posudzovania na úroveň záruky vysoká by žiadatelia mali vo všeobecnosti začať s prípravou dôkazov o certifikácii s dostatočným predstihom pred očakávaným termínom certifikácie. Ako osvedčený postup by poskytovateľ mal naplánovať časovú rezervu najmenej šesť mesiacov pred predpokladaným dátumom požadovaného rozhodnutia o certifikácii, bez započítania oneskorení spôsobených neúplnými alebo nedostatočnými podaniami.

3.2. Podmienky na vydanie certifikátu EUDIW-SK

1. Certifikačný orgán vydá certifikát EUDIW-SK, ak sú splnené všetky tieto podmienky:

a) typ služby IKT, ako je definovaný v odseku 2 časti 1.1, a všetky činnosti posudzovania zhody spadajú do predmetu akreditácie a, ak je to relevantné, do predmetu oprávnenia certifikačného orgánu vydávajúceho certifikát;

b) žiadateľ o certifikáciu podpísal vyhlásenie, v ktorom sa zaviazal dodržiavať všetky záväzky uvedené v odseku 2;

c) certifikačný orgán ukončil hodnotenie bez námietok v súlade s hodnotiacimi kritériami a metódami uvedenými v oddieloch 2.1 a 2.2;

d) v prípade počiatočného hodnotenia, ak nebola posúdená účinnosť bezpečnostných opatrení, neexistuje na konci hodnotenia žiadna nevyriešená nezhoda, ktorú by bolo potrebné nahlásiť;

e) certifikačný orgán bez námietok ukončil preskúmanie výsledkov hodnotenia.

2. Žiadateľ o certifikáciu sa zaviaže k nasledujúcim záväzkom:

a) poskytne certifikačnému orgánu všetky potrebné úplné a správne informácie a na požiadanie poskytne ďalšie potrebné informácie;

b) nepropagovať službu IKT ako certifikovanú podľa EUDIW-SK pred vydaním certifikátu EUDIW-SK;

c) propagovať službu IKT ako certifikovanú iba v predmete stanovenom v certifikáte EUDIW-SK;

d) v prípade pozastavenia, odňatia alebo uplynutia platnosti certifikátu EUDIW-SK okamžite prestať propagovať službu IKT ako certifikovanú;

e) zabezpečiť, aby služba IKT poskytovaná s odkazom na certifikát EUDIW-SK bola službou IKT, ktorá podlieha certifikácii;

f) dodržiavať pravidlá používania značky a označenia stanovené pre certifikát EUDIW v súlade s oddielom 3.4.

3. Okrem úspešného hodnotenia a následného preskúmania je vydanie certifikátu EUDIW-SK podmienené tým, že žiadateľ sa zaviaže poskytovať certifikačnému orgánu pravdivé a úplné informácie a riadne používať certifikát.

3.3. Vydanie certifikátu EUDIW-SK

1. Certifikát EUDIW-SK obsahuje aspoň informácie uvedené v prílohe V.
2. Predmet a hranice certifikovanej služby IKT musia byť jednoznačne špecifikované v certifikáte EUDIW-SK alebo v certifikačnej správe.
3. Certifikačný orgán poskytne žiadateľovi certifikát EUDIW aspoň v elektronickej forme.
4. Certifikačný orgán vypracuje certifikačnú správu v súlade s prílohou VI pre každý certifikát EUDIW-SK, ktorý vydá. Správa o certifikácií sa zakladá na technickej správe o hodnotení. Správa o certifikácií uvádza konkrétne hodnotiace kritériá a metódy uvedené v oddieloch 2.1 a 2.2, ktoré sa použili pri hodnotení.
5. Certifikačný orgán vypracuje technickú hodnotiacu správu pre komplexné hodnotenie v súlade s prílohou VII pre každý certifikát EUDIW-SK, ktorý vydá, a túto správu poskytne orgánu posudzovania zhody, ktorý bude vykonávať hodnotiace činnosti na základe tohto certifikátu EUDIW-SK
6. Certifikačný orgán poskytne národnému certifikačnému orgánu pre kybernetickú bezpečnosť a agentúre ENISA každý certifikát EUDIW-SK a certifikačnú správu, ktoré

vydá, v elektronickej forme.

7. Ku každému certifikátu vydanému v rámci EUDIW-SK musí byť priložená Správa o certifikácií, pričom ich obsah je definovaný v prílohách a musí byť verejne dostupný. Okrem toho musí certifikačný orgán vypracovať certifikačnú hodnotiacu správu obsahujúcu podrobnejšie informácie, ktorá sa bude zdieľať iba v kontexte s príslušnými vnútroštátnymi dozornými orgánmi (z nariadení CSA aj eIDAS).

3.4. Značka a označenie

Poznámka o prechodnej uplatniteľnosti: *Táto časť a príloha XII sú zahrnuté s cieľom zachovať štruktúru kandidátskej schémy EÚ. V slovenskom národnom systéme sa nebudú používať v prevádzke, kým sa nestane uplatniteľným európsky systém EUDIW alebo kým príslušný slovenský orgán výslovne nezavedie alebo neaktivuje mechanizmus národnej značky a označenia.*

Poznámka o zosúladení so slovenskou legislatívou: *Do tej doby sa verejná transparentnosť zakladá na certifikáte, certifikačnej správe a verejne dostupnom informačnom balíku definovanom v prílohe III, prílohe V a prílohe VI. Značka dôveryhodnosti EUDI Wallet-SK zostáva oddelená od akejkoľvek certifikačnej značky alebo označenia v oblasti kybernetickej bezpečnosti.*

Držiteľ certifikátu, poskytovatelia komponentov, subdodávatelia a ďalšie strany zapojené do certifikovanej služby IKT nesmú uvádzať, že jednotlivá zložka, modul, produkt, proces alebo služba je certifikovaná v rámci tejto schémy, pokiaľ táto zložka, modul, produkt, proces alebo služba nie je výslovne identifikovaná ako certifikovaná služba IKT alebo ako súčasť certifikovaného predmetu v certifikáte EUDIW-SK a certifikačnej správe. Akýkoľvek verejný odkaz na certifikáciu musí presne odrážať predmet, obmedzenia a verziu, na ktoré sa certifikát vzťahuje.

3.5. Doba platnosti certifikátu EUDIW-SK

1. Certifikačný orgán stanoví dobu platnosti každého vydaného certifikátu EUDIW-SK s prihliadnutím na charakteristiky certifikovanej služby IKT.
2. Doba platnosti certifikátu EUDIW-SK nesmie presiahnuť 5 rokov.
3. Počas platnosti certifikátu sa MUSÍ vykonávať posúdenie zraniteľnosti 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. Harmonogram v prílohe II MUSÍ odrážať túto minimálnu frekvenciu. Dvojročné posúdenie zraniteľnosti MÔŽE byť začlenené do ročného dohľadu, recertifikácie alebo osobitného hodnotenia za predpokladu, že sa aspoň raz za dva roky zdokumentuje úplné posúdenie zraniteľnosti.

4. Odôvodnenie

    a) Obmedzenie vyplýva z článku 5c ods. 4 nariadenia eIDAS. Keďže ide o zákonnú požiadavku, neexistuje žiadna výnimka, ktorá by umožňovala dlhšiu dobu platnosti, a to ani s predchádzajúcim súhlasom národného certifikačného orgánu (NCCA).

    b) Tento termín je preto potrebné starostlivo sledovať, pretože peňaženka EUDI by musela byť deaktivovaná, ak by už nebola certifikovaná, a preto je potrebné jasne uviesť odporúčanie, aby sa posudzovanie zhody na účely recertifikácie začalo dostatočne včas.

5. Doba platnosti certifikátu je stanovená na päť rokov, aby bola v súlade s článkom 5c ods. 4 nariadenia eIDAS. Činnosti posudzovania zraniteľnosti, ktoré sa tiež vyžadujú v uvedenom článku, boli začlenené do celkového procesu údržby certifikátov EUDIW-SK.

3.6. Údržba certifikátu EUDIW-SK

1. V súlade s harmonogramom stanoveným v prílohe II certifikačný orgán na žiadosť držiteľa certifikátu alebo z iných odôvodnených dôvodov pravidelne vykonáva posudzovanie zhody v rámci údržby a preskúmava certifikát EUDIW-SK pre službu IKT. Posudzovanie zhody v rámci údržby sa vykonáva v súlade s prílohou II.
2. Na základe výsledkov posudzovania zhody a preskúmania v rámci údržby certifikačný orgán:
    a) potvrdí certifikát EUDIW-SK;
    b) odníme certifikát EUDIW-SK v súlade s oddielom 3.7;
    c) pripojí k certifikátu EUDIW-SK dodatok, ktorý definuje aktualizovaný predmet; alebo
    d) odníme certifikát EUDIW-SK v súlade s oddielom3.7 a vydá nový certifikát EUDIW-SK s identickým alebo aktualizovaným predmetom a predĺženou dobou platnosti.
3. Certifikačný orgán môže bez zbytočného odkladu rozhodnúť o pozastavení platnosti certifikátu EUDIW-SK v súlade s oddielom 6.3, kým držiteľ certifikátu EUDIW-SK neprijme nápravné opatrenia.
4. Okrem údržbových činností súvisiacich so zmenami v poskytovanej službe EUDIW ICT sa vyžadujú pravidelné posudzovania zhody s cieľom zabezpečiť, aby sa základné procesy používané pri poskytovaní služby EUDIW ICT účinne vykonávali, a aby sa primerane zohľadňoval vývoj hrozbového prostredia. Je stanovený harmonogram údržby a každé posudzovanie zhody v rámci údržby môže viesť k potvrdeniu, zrušeniu alebo aktualizácii certifikátu.

3.7. Zrušenie certifikátu EUDIW-SK

1. Bez toho, aby bol dotknutý článok 58 ods. 8 písm. e) nariadenia (EÚ) 2019/881, certifikát EUDIW-SK odníme certifikačný orgán, ktorý tento certifikát vydal.
2. Certifikačný orgán uvedený v odseku 1 oznámi vnútroštátnemu orgánu pre certifikáciu - kybernetickej bezpečnosti - NBÚ NOKC zrušenie certifikátu. O takomto zrušení informuje aj agentúru ENISA s cieľom uľahčiť jej výkonnosť podľa článku 50 nariadenia (EÚ) 2019/881.
3. Certifikačný orgán o tom informuje ostatné príslušné orgány dohľadu nad trhom.
4. Držiteľ certifikátu SK-certifikátu EUDIW-SK môže požiadať o zrušenie osvedčenia.
5. Zrušenie certifikátov EUDIW-SK je úlohou zverenou certifikačnému orgánu, ktorý certifikát vydal, a to v dôsledku problému, ktorý nie je možné napraviť (zraniteľnosť alebo nezhoda), alebo v dôsledku nedodržiavania požiadaviek zo strany držiteľa certifikátu, alebo na základe pokynov držiteľa certifikátu alebo NCCA.

4. Orgány posudzovania zhody (normatívne)

4.1. Požiadavky na akreditáciu orgánu posudzovania zhody

1. Pri akreditácii orgánu posudzovania zhody sa zohľadnia špecifikácie požiadaviek na akreditáciu certifikačných orgánov stanovené v prílohe VIII.

4.2. Dodatočné alebo osobitné požiadavky na orgán posudzovania zhody

Poznámka o prechodnej uplatniteľnosti: *Táto časť je zahrnutá s cieľom zachovať štruktúru kandidátskej schémy EÚ. V slovenskom národnom systéme sa nebude operatívne používať, kým sa nestane uplatniteľným európsky systém EUDIW alebo kým príslušný slovenský orgán výslovne nezavedie alebo neaktivuje mechanizmus národnej značky a označenia. Mechanizmus autorizácie sa neuplatňuje, kým nevstúpi do platnosti schéma EUDIW. Slovenská NCCA spolupracuje so slovenskou NAB (SNAS) a je ňou informovaná o akreditácii CAB.*

4.3. Oznamovanie certifikačných orgánov

1. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť oznámi Komisii certifikačné orgány na svojom území, ktoré sú na základe svojej akreditácie a rozhodnutia o autorizácii oprávnené certifikovať na úroveň záruky vysoká.
2. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť poskytne Komisii pri oznamovaní certifikačných orgánov aspoň tieto informácie:
    a) nasledujúce informácie týkajúce sa akreditácie:
        1) dátum akreditácie;
        2) názov a adresa certifikačného orgánu;
        3) krajina registrácie certifikačného orgánu;
        4) referenčné číslo akreditácie;
        5) predmet a platnosť akreditácie;
        6) adresa, sídlo a odkaz na príslušnú webovú stránku národného orgánu pre akreditáciu; a
    b) nasledujúce informácie týkajúce sa povolenia:
        1) dátum povolenia;
        2) referenčné číslo povolenia;
        3) doba platnosti povolenia;
        4) predmet povolenia.
3. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť bez zbytočného odkladu preskúma všetky informácie týkajúce sa zmeny stavu akreditácie, ktoré poskytol vnútroštátny akreditačný orgán. Ak bola akreditácia alebo povolenie odňaté, vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť o tom informuje Komisiu a môže Komisii predložiť žiadosť v súlade s článkom 61 ods. 4 nariadenia (EÚ) 2019/881.

4. Proces oznamovania je požiadavkou CSA a bude spočívať v pridávaní relevantných informácií týkajúcich sa akreditovaných a autorizovaných orgánov do databázy NANDO Komisie.

4.4. Ukončenie činnosti certifikačného orgánu

1. Ak sa notifikovaný certifikačný orgán rozhodne ukončiť svoje činnosti súvisiace s EUDIW, je povinný:
    a) bezodkladne informovať vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť o ukončení činnosti spolu s harmonogramom ukončenia;
    b) pripraviť plán ukončenia činnosti, vrátane prevodu svojich činností na iný akreditovaný certifikačný orgán;
    c) predložiť tento plán národnému certifikačnému orgánu pre kybernetickú bezpečnosť a držiteľom certifikátov;
    d) pomáhať národnému certifikačnému orgánu pre kybernetickú bezpečnosť a držiteľom certifikátov pri vykonávaní plánu prechodu.
2. Keď certifikačný orgán oznámi ukončenie svojich činností súvisiacich s EUDIW, vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť:
    a) upozorní Komisiu na ukončenie činnosti certifikačných orgánov na svojom území;
    b) preskúma plán ukončenia činnosti, ktorý predložil certifikačný orgán ukončujúci činnosť;
    c) koordinovať vykonávanie plánu ukončenia činnosti, a to najmä:
        1) určí potrebnú dokumentáciu a dôkazy týkajúce sa platných certifikátov EUDIW s podporou certifikačného orgánu, ktorý ukončuje činnosť, a v prípade potreby akéhokoľvek iného akreditovaného certifikačného orgánu, ktorý môže mať lepšie technické predpoklady na vykonávanie týchto činností;
        2) predloží všetku identifikovanú dokumentáciu a dôkazy týkajúce sa platných certifikátov EUDIW akémukoľvek inému akreditovanému certifikačnému orgánu, ktorý môže mať lepšie technické predpoklady na vykonávanie týchto činností. Patrí sem najmä certifikačné správy a dôkazy predložené žiadateľom. Osobné údaje alebo osobné informácie, ako sú e-maily, sa nezahŕňajú.
3. Ak sa nepodarí okamžite nájsť orgán s akreditáciou, ktorý by prevzal činnosti ukončujúceho certifikačného orgánu, národný certifikačný orgán pre kybernetickú bezpečnosť vykonáva počas prechodného obdobia monitorovacie a dozorné činnosti v súvislosti s dotknutými certifikátmi.

5. Monitorovanie dodržiavania (normatívne)

5.1. Monitorovacie činnosti vykonávané NCCA

1. Bez toho, aby bol dotknutý článok 58 ods. 7 nariadenia (EÚ) 2019/881, vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť (NCCA) monitoruje dodržiavanie (predpisov/zhody):

a) certifikačných orgánov s ich povinnosťami podľa tejto schémy a nariadenia (EÚ) 2019/881;

b) držiteľov certifikátu EUDIW-SK s ich povinnosťami podľa tejto schémy a nariadenia (EÚ) 2019/881;

c) certifikovaných služieb IKT s požiadavkami stanovenými v EUDIW;

d) záruky uvedenej v certifikáte EUDIW-SK, ktorá sa týka meniaceho sa prostredia hrozieb.

2. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť vykonáva svoje monitorovacie činnosti najmä na základe:

a) informácií pochádzajúcich od certifikačných orgánov, vnútroštátnych orgánov akreditácie a príslušných orgánov dohľadu nad trhom;

b) informácií vyplývajúcich z vlastných auditov a vyšetrovaní alebo z auditov a vyšetrovaní iného orgánu;

c) prijatých sťažností.

d) Vlastník schémy MUSÍ tiež monitorovať fungovanie tejto národnej certifikačnej schémy na základe informácií od certifikačných orgánov, národného orgánu pre akreditáciu, dozorných orgánov, sťažností, odvolaní, výsledkov dohľadu a skúseností s certifikáciou. Toto monitorovanie zo strany vlastníka schémy podporuje udržiavanie schémy a odlišuje sa od monitorovania dodržiavania (predpisov/zhody) zo strany NCCA v konkrétnych prípadoch.

3. Vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti vyberie certifikované služby IKT, ktoré sa majú kontrolovať, na základe objektívnych kritérií, vrátane:

a) držiteľa certifikátu;

b) certifikačný orgán;

c) konkrétne body, na ktoré sa má venovať pozornosť, definované národným certifikačným orgánom pre kybernetickú bezpečnosť;

d) akékoľvek ďalšie informácie, na ktoré bol orgán upozornený.

4. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť informuje držiteľov certifikátu EUDIW-SK o vybraných službách IKT a o výberových kritériách.

5. Certifikačný orgán, ktorý certifikoval vzorku služby IKT, vykoná na žiadosť vnútroštátneho certifikačného orgánu pre kybernetickú bezpečnosť dodatočné preskúmanie podľa pokynov vnútroštátneho certifikačného orgánu pre kybernetickú bezpečnosť a informuje vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť o výsledkoch.

6. Ak má vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť dostatočný dôvod domnievať sa, že certifikovaná služba IKT už nie je v súlade s touto schémou alebo nariadením (EÚ) 2019/881, môže vykonať vyšetrovanie alebo využiť akékoľvek iné monitorovacie právomoci uvedené v článku 58 ods. 8 nariadenia (EÚ) 2019/881.

7. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť informuje príslušný certifikačný orgán o prebiehajúcich vyšetrovaniach týkajúcich sa vybraných služieb IKT.

8. Ak vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť zistí, že prebiehajúce vyšetrovanie sa týka služieb IKT, ktoré sú certifikované certifikačnými orgánmi so sídlom v iných členských štátoch, informuje o tom vnútroštátne certifikačné orgány pre

kybernetickú bezpečnosť príslušných členských štátov s cieľom v prípade potreby spolupracovať pri vyšetrovaní. Takýto vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť tiež informuje Európsku skupinu pre certifikáciu v oblasti kybernetickej bezpečnosti o cezhraničných vyšetrovaniach a ich výsledkoch.

9. Odôvodnenie

    a) Smernica CSA v článku 54 ods. 1 písm. j) vyžaduje, aby certifikačné schémy kybernetickej bezpečnosti EÚ obsahovali pravidlá na monitorovanie dodržiavania certifikovaných položiek, a v článku 58 ods. 7 pripisuje dôležitú úlohu pri tomto monitorovaní národným certifikačným orgánom (NCCA). Okrem dodržiavania produktov, služieb a procesov IKT musia NCCA monitorovať všetky ostatné zainteresované strany, vrátane držiteľov certifikátov a certifikačných orgánov.

    b) Je potrebné poznamenať, že tento mechanizmus nie je určený na riešenie núdzových situácií, keď sa využíva nová hrozba a je potrebné ju zmierniť. V takomto prípade by sa skôr postupovalo tak, že by sa certifikačné orgány informovali, aby mohli v prípade potreby začať osobitné hodnotenie s cieľom určiť, ako sa hrozba zmierňuje prostredníctvom IKT služieb, ktoré certifikovali.

5.2. Monitorovacie činnosti certifikačného orgánu

1. Certifikačný orgán monitoruje dodržiavanie predpisov:

    a) dodržiavanie povinností držiteľov certifikátov podľa tejto schémy a nariadenia (EÚ) 2019/881 vo vzťahu k certifikátu EUDIW-SK, ktorý vydal certifikačný orgán;

    b) dodržiavanie služieb IKT, ktoré certifikoval, s príslušnými hodnotiacimi kritériami.

2. Certifikačný orgán vykonáva svoje monitorovacie činnosti na základe:

    a) informácií poskytnutých na základe záväzkov žiadateľa o certifikáciu uvedených v oddiele 3.2;

    b) informácií vyplývajúcich z činností iných príslušných orgánov dohľadu nad trhom; prijatých sťažností a odvolaní;

    c) informácií o zraniteľnosti, ktoré by mohli mať vplyv na služby IKT, ktoré certifikoval.

3. Certifikačný orgán je tiež zodpovedný za vykonávanie monitorovacích činností zameraných na dodržiavanie predpisov a zhodu certifikovaných služieb IKT EUDIW a držiteľov certifikátov, ako sa stanovuje v norme EN ISO/IEC 17065.

5.3. Monitorovacie činnosti držiteľa certifikátu

1. Držiteľ certifikátu EUDIW-SK vykonáva nasledujúce úlohy s cieľom monitorovať zhodu certifikovanej služby IKT s jej bezpečnostnými požiadavkami:

    a) monitorovať informácie o zraniteľnosti týkajúce sa certifikovanej služby IKT, vrátane známych závislostí, vlastnými prostriedkami, ale aj s ohľadom na:

        1) publikácie alebo podania týkajúce sa informácií o zraniteľnosti zo strany používateľa alebo bezpečnostného výskumníka prostredníctvom kontaktného poskytovateľa, ktorý je k dispozícii na tento účel;

        2) podania z akéhokoľvek iného zdroja;

b) monitorovať záruku vyjadrenú v certifikáte EUDIW-SK, a to najmä vývoj stavu akéhokoľvek certifikátu alebo správy o záruke použitej ako objektívny dôkaz pri hodnotení služby IKT.

2. Držiteľ certifikátu EUDIW-SK spolupracuje s certifikačným orgánom a v prípade potreby s vnútroštátnym certifikačným orgánom pre kybernetickú bezpečnosť s cieľom podporiť ich monitorovacie činnosti.
3. Držiteľ certifikátu EUDIW-SK bez zbytočného odkladu informuje certifikačný orgán, ak nastanú tieto udalosti:
    a) akékoľvek porušenie alebo ohrozenie služby IKT, ktorú poskytuje;
    b) akákoľvek podstatná zmena služby IKT.
4. Odôvodnenie
    a) Keďže systém EUDIW sa má vo veľkej miere opierať o zloženie a nezávislú certifikáciu komponentov peňaženky EUDI, pridáva sa osobitná povinnosť monitorovať vývoj certifikátov, na ktorých sa zakladá certifikácia služby, a prijať primerané opatrenia, ak sa aktualizuje niektorá z komponentov, ak sa zmení predmet jej certifikácie alebo ak sa certifikát odníme.
5. Držiteľ certifikátu má tiež povinnosti súvisiace s monitorovaním dodržiavania predpisov pre certifikované služby IKT EUDIW, ktoré poskytuje, a to najmä s cieľom identifikovať relevantné zraniteľnosti a možné nezhody.

5.4. Sťažnosti a odvolania

1. Vlastník schémy a každý certifikačný orgán pôsobiaci v rámci tejto schémy MUSIA zaviesť, udržiavať a uplatňovať zdokumentované postupy na podávanie, prijímanie, posudzovanie a riešenie sťažností a odvolaní týkajúcich sa certifikačných činností, vrátane certifikačných rozhodnutí, pozastavenia, zrušenia, monitorovacích činností a údajného zneužitia certifikačných tvrdení, v súlade s článkom 15 vykonávacieho nariadenia (EÚ) 2024/2981. Postupy MUSIA zabezpečiť nestranné preskúmanie osobami nezávislými od pôvodného rozhodnutia, potvrdenie prijatia a uchovávanie záznamov.
2. Certifikačný orgán MUSÍ vybavovať sťažnosti a odvolania v súlade s Metodickým usmernením NCCA – Pre podávanie sťažností a odvolaní (referenčné číslo: 02620/2025/OBC-002), uverejneným na webovej stránke NBÚ.
3. Ak sťažnosť alebo odvolanie patrí do správnej alebo dozornej spôsobilosti slovenského orgánu, postup sa MUSÍ uplatňovať v súlade s platnými slovenskými právnymi predpismi, vrátane zákona č. 71/1967 Z. z. o správnom konaní a zákona č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov. Právo na súdnu ochranu podľa platných právnych predpisov tým nie je dotknuté. Nevyriešené alebo podstatné sťažnosti alebo odvolania, ktoré môžu ovplyvniť integritu schémy, spôsobilosť CAB alebo platnosť certifikátu, MUSIA byť bez zbytočného odkladu postúpené NBÚ / vlastníkovi schémy.

6. Nezhody a nedodržiavanie požiadaviek (normatívne)

6.1. Dôsledky nezhody certifikovanej služby

1. Ak certifikačný orgán zistí nezhodu certifikovanej služby IKT s požiadavkami stanovenými v tomto schéme a v nariadení (EÚ) 2019/881, certifikačný orgán informuje držiteľa certifikátu EUDIW-SK o zistenej nezhode s normou a požiada o nápravné opatrenia.
2. Ak by prípad nezhody s požiadavkami tohto systému mohol ovplyvniť dodržiavanie nariadenia (EÚ) č. 910/2014, certifikačný orgán bezodkladne informuje vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť, ako aj dozorný orgán uvedený v článku 46a ods. 1 nariadenia (EÚ) č. 910/2014 o zistenej nezhode.
3. Po prijatí informácií uvedených v odseku 1 predloží držiteľ certifikátu EUDIW-SK certifikačnému orgánu v lehote stanovenej certifikačným orgánom, ktorá nesmie presiahnuť 30 dní, návrh na posúdenie závažnosti nezhody a nápravné opatrenia potrebné na jej odstránenie.
4. Certifikačný orgán môže bez zbytočného odkladu pozastaviť platnosť certifikátu EUDIW-SK v súlade s oddielom 6.3 v prípade núdze alebo ak držiteľ certifikátu EUDIW-SK riadne nespolupracuje s certifikačným orgánom.
5. Certifikačný orgán vykoná analýzu navrhovaného posúdenia a validáciu s cieľom posúdiť, či navrhované nápravné opatrenie rieši nezhodu, a ak je nezhoda závažná, verifikáciu s cieľom posúdiť účinnosť nápravného opatrenia.
6. Ak je certifikovaná služba IKT zloženou službou IKT a zistí sa, že na nezhode sa podieľa jedna z jej zložiek, orgán posudzovania zhody o tejto skutočnosti informuje orgán posudzovania zhody, ktorý vydal certifikát pre danú zložku.
7. Odôvodnenie
    a) Článok 54 ods. 1 písm. l) CSA vyžaduje, aby schémy opisovali dôsledky nezhody certifikovaných služieb. Táto časť opisuje proces, v ktorom certifikačný orgán, keď zistí nezhodu, musí informovať držiteľa certifikátu a požiadať o posúdenie vplyvu, ako aj o návrh nápravného opatrenia.
    b) Certifikačný orgán následne posúdi posúdenie vplyvu a vhodnosť navrhovaného nápravného opatrenia. V súlade so zásadami normy CEN TS 18072 je potrebné overiť účinnosť nápravného opatrenia len v prípade, ak je nezhoda podstatná. V opačnom prípade sa verifikácia môže odložiť až do nasledujúceho ročného posudzovania zhody.
    c) V praxi bude tento proces pravdepodobne oveľa zjednodušený, pretože je pravdepodobné, že držiteľ certifikátu bude subjektom, ktorý certifikačný orgán na nezhodu upozorní. V takom prípade je dosť pravdepodobné, že okamžite poskytne prvý návrh posúdenia vplyvu a prípadne návrh nápravných opatrení, ktoré už mohli byť aj implementované.
    d) Ak držiteľ certifikátu nedodrží pravidlá, certifikačný orgán má k dispozícii viacero spôsobov, ako ho prinútiť konať, vrátane pozastavenia platnosti certifikátu a v prípade potreby jeho odňatia.

6.2. Dôsledky nedodržiavania predpisov držiteľom certifikátu

1. Ak certifikačný orgán zistí, že:
    a) držiteľ certifikátu EUDIW-SK alebo žiadateľ o certifikáciu nedodržiava svoje záväzky a povinnosti uvedené v oddieloch 3.2, 5.3 a 9.2; alebo

b) držiteľ certifikátu EUDIW-SK nedodržiava článok 56 ods. 8 nariadenia (EÚ) 2019/881 alebo kapitoly 7 a 8 tejto schémy;

c) stanoví lehotu najviac 30 dní, v ktorej držiteľ certifikátu EUDIW-SK prijme nápravné opatrenia.

2. Ak držiteľ certifikátu EUDIW-SK nenavrhne primerané nápravné opatrenia v lehote uvedenej v odseku 1, certifikát sa pozastaví v súlade s oddielom 6.3 alebo sa odníme v súlade s oddielom 3.7.

3. Trvalé alebo opakované porušenie povinností uvedených v odseku 1 zo strany držiteľa certifikátu EUDIW-SK má za následok zrušenie certifikátu EUDIW-SK v súlade s oddielom 3.7.

4. Certifikačný orgán informuje vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť o zisteniach uvedených v odseku 1. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť bezodkladne informuje dozorný orgán uvedený v článku 46a nariadenia (EÚ) č. 910/2014.

6.3. Pozastavenie platnosti certifikátu EUDIW-SK

1. Ak sa tento systém odvoláva na pozastavenie platnosti certifikátu EUDIW-SK, certifikačný orgán pozastaví platnosť príslušného certifikátu EUDIW-SK na obdobie primerané okolnostiam, ktoré viedli k pozastaveniu, ktoré nepresiahne 42 dní. Obdobie pozastavenia začína plynúť dňom nasledujúcim po dni rozhodnutia certifikačného orgánu. Pozastavenie nemá vplyv na platnosť osvedčenia.

2. Certifikačný orgán bez zbytočného odkladu informuje držiteľa certifikátu a vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť o pozastavení a uvedie dôvody pozastavenia, požadované opatrenia, ktoré sa majú prijať, a dobu pozastavenia.

3. Držiteľ osvedčenia informuje používateľov príslušných služieb IKT o pozastavení a o dôvodoch, ktoré certifikačný orgán uviedol ako dôvod pozastavenia, s výnimkou tých častí dôvodov, ktorých zverejnenie by predstavovalo bezpečnostné riziko alebo ktoré obsahujú citlivé informácie, ako aj o usmerneniach pre používateľov služby IKT. Tieto informácie držiteľ osvedčenia sprístupní aj verejnosti.

4. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť môže o pozastavení informovať dozorný orgán uvedený v článku 46a ods. 1 nariadenia (EÚ) č. 910/2014.

5. O pozastavení platnosti certifikátu sa informuje agentúru ENISA v súlade s oddielom 9.3.

6. V riadne odôvodnených prípadoch môže vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť povoliť predĺženie lehoty pozastavenia platnosti certifikátu EUDIW-SK. Celková lehota pozastavenia platnosti nesmie presiahnuť 1 rok.

6.4. Dôsledky nedodržiavania povinností certifikačným orgánom

1. V prípade nedodržiavania povinností certifikačným orgánom vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť bez zbytočného odkladu:

a) určí certifikáty EUDIW-SK, ktorých sa to môže týkať;

b) v prípade potreby na účely tejto identifikácie požiadať o vykonanie činností posudzovania zhody v súvislosti s jednou alebo viacerými službami IKT buď certifikačný orgán, ktorý certifikát vydal, alebo akýkoľvek iný akreditovaný a

oprávnený certifikačný orgán, ktorý môže mať lepšie technické predpoklady na vykonanie týchto činností;

c) analyzovať vplyvy nedodržiavania požiadaviek certifikačným orgánom;

d) upozorniť držiteľov certifikátov EUDIW, ktorých sa nedodržiavanie predpisov zo strany certifikačného orgánu týka.

2. V prípade každého certifikátu, na ktorý má vplyv nedodržiavanie predpisov certifikačným orgánom, vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť bez zbytočného odkladu:

a) určí činnosti posudzovania zhody, ktoré sa musia vykonať opakovane, v prípade potreby s podporou certifikačného orgánu, ktorý nedodržal požiadavky, alebo akéhokoľvek iného akreditovaného a oprávneného certifikačného orgánu, ktorý môže mať lepšie technické predpoklady na vykonávanie týchto činností;

b) v prípade každej takejto činnosti posudzovania zhody požiadať, aby túto činnosť vykonal buď certifikačný orgán, ktorý vydal certifikát, alebo akýkoľvek iný

c) akreditovaný a autorizovaný certifikačný orgán, ktorý môže mať lepšie technické predpoklady na vykonanie tejto činnosti.

3. Akákoľvek nezhoda certifikovanej služby IKT zistená pri opätovnom vykonávaní činností posudzovania zhody sa spracuje podľa oddielu 6.1.

4. Certifikačný orgán, ktorý nespĺňa požiadavky, znáša náklady súvisiace s činnosťami uvedenými v odseku 2.

5. Na základe opatrení uvedených v odseku 1 vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť:

d) v prípade potreby nahlásiť neplnenie povinností certifikačného orgánu národnému orgánu pre akreditáciu;

e) v prípade potreby posúdi potenciálny vplyv na autorizáciu.

6. Dodržiavanie certifikačného orgánu môže samozrejme ovplyvniť jeho akreditáciu, autorizáciu a notifikáciu a môže mať vplyv aj na certifikáty vydané týmto certifikačným orgánom, ak sa zistí, že činnosť certifikačného orgánu pri vydávaní certifikátu bola neprimeraná a vyvoláva pochybnosti o platnosti certifikátu. NCCA môže zorganizovať preskúmanie dotknutých certifikátov iným certifikačným orgánom a v prípade zistenia problémov môže vyžadovať opätovné vykonanie niektorých činností posudzovania zhody.

7. Riadenie zraniteľností (normatívna)

7.1. Postupy riadenia zraniteľnosti

1. Držiteľ certifikátu EUDIW-SK zavedie, udržiava a vykonáva všetky potrebné postupy riadenia zraniteľnosti v súlade s pravidlami stanovenými v tejto kapitole a v prípade potreby doplnenými postupmi stanovenými v norme EN ISO/IEC 30111.

2. Pre všetky príslušné komponenty služby IKT musia postupy riadenia zraniteľnosti uvedené v odseku 1 zahŕňať:

a) používanie zoznamu softvérových komponentov v bežne používanom a strojovo čitateľnom formáte, ktorý zahŕňa aspoň závislosti komponentu na najvyššej úrovni;

b) používanie bezpečnostných aktualizácií na odstránenie zraniteľností a, ak je to technicky možné, oddelene od funkčných aktualizácií;

c) mechanizmus na bezpečnú distribúciu aktualizácií, vrátane mechanizmu na zabezpečenie toho, aby boli zraniteľnosti odstránené bezodkladne, prípadne automatizovanú distribúciu bezpečnostných aktualizácií a prípadne mechanizmus na deaktiváciu prevádzky peňaženky, kým nebudú nainštalované požadované bezpečnostné aktualizácie;

d) distribúcia v súvislosti s aktualizáciami poradenských správ, ktoré poskytujú používateľom relevantné informácie, vrátane informácií o potenciálnych opatreniach, ktoré je potrebné prijať.

3. Držiteľ certifikátu EUDIW-SK udržiava a zverejňuje primerané metódy na prijímanie informácií o zraniteľnostiach týkajúcich sa jeho výrobkov z externých zdrojov, vrátane používateľov, orgánov posudzovania zhody a výskumníkov v oblasti bezpečnosti.
4. Ak držiteľ certifikátu EUDIW-SK zistí alebo dostane informácie o potenciálnej zraniteľnosti ovplyvňujúcej certifikovanú službu IKT, zaznamená ju a vykoná analýzu vplyvu zraniteľnosti.
5. Ak potenciálna zraniteľnosť ovplyvňuje produkt IKT, na ktorom je založená zložená služba IKT, držiteľ osvedčenia EUCC informuje držiteľa závislých osvedčení EUDIW o potenciálnej zraniteľnosti.
6. Ak sa v jednej zo zložiek certifikovanej zloženej služby IKT zistí potenciálna zraniteľnosť, orgán posudzovania zhody o nej informuje certifikačný orgán, ktorý vydal certifikát pre túto zložku.
7. V reakcii na odôvodnenú žiadosť certifikačného orgánu, ktorý vydal certifikát, držiteľ certifikátu EUDIW-SK poskytne tomuto certifikačnému orgánu všetky relevantné informácie o potenciálnych zraniteľnostiach.
8. Všetci poskytovatelia služieb IKT EUDIW musia riadiť zraniteľnosti podľa stanovených postupov a požiadavky musia byť zosúladené s osvedčenými postupmi, vrátane noriem, ako je EN ISO/IEC 30111, a v prípade príslušných výrobkov s nariadeniami, ako je CRA.

7.2. Analýza vplyvu zraniteľnosti

1. Analýza vplyvu zraniteľnosti sa musí odvolávať na opis predmetu certifikácie a vyhlásenia o záruke obsiahnuté v certifikáte. Analýza vplyvu zraniteľnosti sa vykoná v časovom rámci primeranom využiteľnosti a kritickosti potenciálnej zraniteľnosti certifikovanej služby IKT.
2. Významnosť vplyvu sa stanoví v súlade s príslušnou metodikou definovanou v prílohe XI s cieľom určiť zneužiteľnosť a vplyv zraniteľnosti.
3. Odôvodnenie

a) Cieľom analýzy vplyvu zraniteľnosti je určiť, do akej miery môže potenciálna zraniteľnosť ovplyvniť certifikovanú službu. Na vypracovanie tejto analýzy neexistuje prísny termín, ale všeobecné posúdenie zraniteľnosti, napríklad na základe skóre zraniteľnosti v systéme ako CVSS, spôsobuje, že riešenie kritických zraniteľností je naliehavejšie ako riešenie zraniteľností s nízkou a strednou závažnosťou.

b) Cieľom analýzy vplyvu zraniteľnosti je premeniť toto počiatočné posúdenie na posúdenie, ktoré je špecifické pre certifikovanú službu. V tomto posúdení nemusí mať kritická zraniteľnosť žiadny vplyv, ak sa týka funkcie, ktorá sa pri implementácii služby nepoužíva. Naopak, zraniteľnosť s nižším skóre sa môže považovať za podstatnú, ak sú v certifikovanej službe splnené podmienky na jej zneužitie.

4. Držitelia certifikátov sú povinní vykonať analýzu vplyvu zraniteľnosti pre každú identifikovanú zraniteľnosť, ktorá by mohla mať vplyv na certifikovanú službu IKT v rámci EUDIW, a sú povinní informovať certifikačný orgán o každej zraniteľnosti, ktorá bola posúdená ako podstatná pre bezpečnosť certifikovanej služby IKT v rámci EUDIW. Nepodstatné zraniteľnosti analyzuje certifikačný orgán v rámci pravidelných posudzovaní zhody pri údržbe.

7.3. Správa o analýze vplyvu zraniteľnosti

1. Držiteľ certifikátu vypracuje správu o analýze vplyvu zraniteľnosti, ak analýza vplyvu preukáže, že zraniteľnosť má podstatný vplyv na bezpečnosť služby IKT, ako je definované v prílohe II, čo má zase pravdepodobný vplyv na zhodu služby IKT s jej certifikátom.
2. Správa o analýze vplyvu zraniteľnosti obsahuje posúdenie týchto prvkov:
    a) vplyv zraniteľnosti na certifikovanú službu IKT;
    b) možné riziká spojené s blízkosťou alebo dostupnosťou útoku;
    c) či je možné zraniteľnosť odstrániť;
    d) ak je možné zraniteľnosť odstrániť, možné riešenia zraniteľnosti.
3. Správa o analýze vplyvu zraniteľnosti obsahuje, ak je to vhodné, podrobnosti o možných spôsoboch zneužitia zraniteľnosti. S informáciami týkajúcimi sa možných spôsobov zneužitia zraniteľnosti sa zaobchádza v súlade s primeranými bezpečnostnými opatreniami na ochranu ich dôvernosti a v prípade potreby na zabezpečenie ich obmedzeného šírenia.
4. Držiteľ certifikátu EUDIW-SK bez zbytočného odkladu zašle certifikačnému orgánu správu o analýze vplyvu zraniteľnosti.
5. Ak sa v správe o analýze vplyvu zraniteľnosti stanoví, že zraniteľnosť má podstatný vplyv na bezpečnosť služby IKT a že ju možno odstrániť, uplatňuje sa oddiel 7.4.
6. Ak sa v správe o analýze vplyvu zraniteľnosti stanoví, že zraniteľnosť má podstatný vplyv na bezpečnosť služby IKT a že ju nie je možné odstrániť, certifikát EUDIW sa odníme v súlade s oddielom 3.7.
7. Držiteľ certifikátu EUDIW-SK monitoruje akékoľvek zostatkové zraniteľnosti, aby zabezpečil, že ich nebude možné zneužiť v prípade zmien v prevádzkovom prostredí.
8. Odôvodnenie
    a) Výsledkom analýzy vplyvu zraniteľnosti je správa, ktorá musí obsahovať informácie o zneužiteľnosti zraniteľnosti a v prípade potreby aj o jej odstránení. Keďže správa môže obsahovať informácie o možnom zneužití zraniteľnosti, ktorá ešte nebola odstránená, všetky zainteresované strany ju musia považovať za vysoko citlivú.
    b) Jednou z dôležitých informácií v správe o analýze vplyvu zraniteľnosti je významnosť vplyvu zraniteľnosti. Ak je tento vplyv významný pre bezpečnosť

certifikovanej služby, je potrebné bezodkladne vykonať nápravu, prípadne s dočasnými kompenzačnými opatreniami. Certifikačný orgán bude musieť overiť aj účinnosť nápravy.

c) Na druhej strane, ak vplyv nie je podstatný, certifikačný orgán sa priamo nezapája. Držiteľ certifikátu uplatňuje svoje postupy posudzovania zraniteľnosti podľa definície a certifikačný orgán overuje účinnosť týchto postupov v rámci ročného posudzovania zhody údržby. Ak niektoré zraniteľnosti nie sú úplne odstránené, čo vedie k zostatkovým zraniteľnostiam, tieto zraniteľnosti je potrebné zohľadniť pri každom posudzovaní zhody údržby.

9. Každé oznámenie o zraniteľnosti s podstatným vplyvom certifikačnému orgánu musí obsahovať správu o analýze vplyvu zraniteľnosti, ktorá opisuje zraniteľnosť, jej vplyv a možné nápravné opatrenia. Ak správa o analýze vplyvu zraniteľnosti obsahuje citlivé informácie, najmä týkajúce sa možných spôsobov zneužitia, sú potrebné osobitné bezpečnostné opatrenia pre komunikáciu medzi držiteľom certifikátu a certifikačným orgánom.

7.4. Odstránenie zraniteľností

1. Držiteľ certifikátu EUDIW-SK včas vypracuje a vykoná plán nápravných opatrení pre všetky zraniteľnosti, ktoré môžu mať vplyv na certifikovanú službu IKT EUDIW.
2. Ak držiteľ certifikátu EUDIW-SK predložil certifikačnému orgánu správu o posúdení vplyvu zraniteľnosti, predloží certifikačnému orgánu aj návrh primeraných nápravných opatrení. Certifikačný orgán preskúma certifikát v súlade s oddielom 3.6. Predmet preskúmania sa určí na základe navrhovaného odstránenia zraniteľnosti.
3. Odôvodnenie
    a) Pravidlá na odstránenie zraniteľnosti sú pomerne jednoduché. Samozrejme, všetky zraniteľnosti je nakoniec potrebné odstrániť včas a spôsobom, ktorý je úmerný ich vplyvu na bezpečnosť certifikovanej služby.
    b) V prípade závažných zraniteľností (tu definovaných skutočnosťou, že poskytovateľ služby predložil správu o analýze vplyvu zraniteľnosti) musí poskytovateľ služby certifikačnému orgánu predložiť aj plán nápravných opatrení (zvyčajne spolu so správou) a tento plán implementovať. Po implementácii musí certifikačný orgán vykonať preskúmanie, ktoré môže viesť k posudzovaniu zhody v rámci dohľadu (v praxi takéto posudzovanie zhody nemusí byť potrebné v jednoduchých prípadoch, ako je aplikácia bezpečnostnej aktualizácie na bežne používanú knižnicu a vykonanie primeraného následného skúšania).

8. Zverejňovanie zraniteľností (normatívna)

8.1. Koordinované zverejňovanie zraniteľností

1. Držiteľ certifikátu EUDIW-SK zavedie, udržiava a uplatňuje politiku koordinovaného zverejňovania zraniteľností a súvisiace postupy v súlade s pravidlami stanovenými v tejto kapitole a v prípade potreby doplnenými postupmi stanovenými v norme EN ISO/IEC 29147.
2. Držiteľ certifikátu EUDIW-SK sprístupní verejnosti svoju politiku a postupy

koordinovaného zverejňovania zraniteľností.

3. Odôvodnenie

   a) Požiadavka na koordinované zverejňovanie zraniteľností vyplýva zo skutočnosti, že v prípade závažnej krízy súvisiacej so zraniteľnosťou môže byť poskytovateľ služieb IKT s certifikátom EUDIW-SK nútený koordinovať reakciu svojich zákazníkov pred verejným zverejnením (prípadne neopraveného) zraniteľného miesta a zároveň bude musieť o situácii informovať svoj certifikačný orgán a regulačné orgány.

   b) To je oveľa ľahšie dosiahnuť, ak bola stanovená politika koordinovaného zverejňovania zraniteľností, ktorá poskytovateľovi služieb umožňuje v prípade krízy postupovať podľa známeho postupu, namiesto toho, aby musel improvizovať riešenie a riskovať zhoršenie krízy.

   c) Tento článok je mimoriadne jednoduchý a vyžaduje tiež, aby bola politika verejne dostupná.

8.2. Informácie poskytované dozorným orgánom

1. Informácie, ktoré certifikačný orgán poskytuje vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti, musia obsahovať všetky prvky potrebné na to, aby vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti pochopil vplyv zraniteľnosti, zmeny, ktoré sa majú vykonať v službe IKT, a ak sú dostupné, akékoľvek informácie od certifikačného orgánu o širších dôsledkoch zraniteľnosti pre iné certifikované služby IKT.
2. Informácie poskytnuté v súlade s odsekom 1 nesmú obsahovať podrobnosti o spôsoboch zneužitia zraniteľnosti. Toto ustanovenie sa nedotýka vyšetrovacích právomocí národného certifikačného orgánu pre kybernetickú bezpečnosť.
3. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť zdieľa relevantné informácie prijaté v súlade s oddielom 7.2 s ostatnými vnútroštátnymi certifikačnými orgánmi pre kybernetickú bezpečnosť a s agentúrou ENISA.
4. Vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť zdieľa relevantné informácie prijaté v súlade s oddielom 7.2 s vnútroštátnymi dozornými orgánmi zriadenými v ich krajine podľa článku 46a ods. 1 nariadenia (EÚ) č. 910/2014.
5. Vnútroštátne dozorné orgány zriadené v príslušnom členskom štáte podľa článku 46a ods. 1 nariadenia (EÚ) č. 910/2014 zdieľajú relevantné informácie získané v súlade s oddielom 7.2 s vnútroštátnymi dozornými orgánmi zriadenými v iných členských štátoch.
6. V koordinovanej politike zverejňovania zraniteľností je potrebné uviesť NCCA, ktorá sa následne môže rozhodnúť ďalej zdieľať informácie s inými NCCA alebo s dozornými orgánmi nariadenia eIDAS.

8.3. Zverejnenie zraniteľnosti

1. Po zrušení certifikátu alebo po odstránení zraniteľnosti, prípadne vrátane doplnenia zmeny a doplnenia k certifikátu, držiteľ certifikátu EUDIW-SK zverejní a zaregistruje akúkoľvek verejne známu a odstránenú zraniteľnosť v službe IKT alebo jej zložkách v európskej databáze zraniteľností zriadenej v súlade s článkom 12 smernice (EÚ) 2022/2555 Európskeho parlamentu a Rady, alebo v iných online úložiskách uvedených

v popise certifikovanej služby IKT.

9. Uchovávanie, zverejňovanie a ochrana informácií (normatívne)

9.1. Uchovávanie záznamov orgánmi posudzovania zhody

1. Orgány posudzovania zhody vedú systém záznamov, ktorý obsahuje všetky dokumenty vyhotovené v súvislosti s každým hodnotením a certifikáciou, ktoré vykonávajú.
2. Orgány posudzovania zhody uchovávajú záznamy bezpečným spôsobom a uchovávajú ich po dobu potrebnú na účely tejto schémy a najmenej 5 rokov po uplynutí platnosti alebo odňatí príslušného certifikátu EUDIW-SK. Ak certifikačný orgán vydal nový certifikát EUDIW v súlade s oddielom 3.3 ods. 2 písm. c), uchováva dokumentáciu o zrušenom certifikáte EUDIW-SK spolu s novým certifikátom EUDIW-SK a po rovnakú dobu ako tento nový certifikát.

9.2. Informácie dostupné držiteľom certifikátu

1. Informácie uvedené v prílohe III ako verejne dostupné musia byť k dispozícii v jazyku, ktorý je pre používateľov ľahko prístupný.
2. Držiteľ certifikátu EUDIW-SK bezpečne uchováva počas obdobia potrebného na účely tejto schémy a najmenej 5 rokov po zrušení príslušného certifikátu EUDIW-SK:
    a) záznamy o informáciách poskytnutých certifikačnému orgánu počas certifikačného procesu;
    b) vzor komponentov produktu certifikovanej služby IKT.
3. Ak certifikačný orgán vydal nový certifikát EUDIW v súlade s oddielom 3.3 ods. 2 písm. c), držiteľ uchováva dokumentáciu o zrušenom certifikáte EUDIW-SK spolu s novým certifikátom EUDIW-SK a po rovnakú dobu ako v prípade nového certifikátu EUDIW-SK.
4. Na žiadosť certifikačného orgánu alebo vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti držiteľ certifikátu EUDIW-SK sprístupní záznamy a kópie uvedené v odseku 2.
5. Okrem vedenia verejne dostupných informácií musí držiteľ certifikátu uchovávať všetky informácie poskytnuté certifikačnému orgánu v súvislosti s hodnotením najmenej 5 rokov po zrušení certifikátua v prípade potreby po zrušení certifikátu, ktoré tento certifikát rozširujú.

9.3. Informácie o dostupnosti sprístupnené agentúrou ENISA

Poznámka o prechodnej uplatniteľnosti: Táto časť je zahrnutá s cieľom zachovať štruktúru kandidátskej schémy EÚ. V slovenskom národnom systéme sa nebude operatívne používať, kým sa nestane uplatniteľným európsky systém EUDIW.

9.4. Ochrana informácií

Orgány posudzovania zhody, vnútroštátny certifikačný orgán pre kybernetickú bezpečnosť, dozorné orgány, agentúra ENISA, Komisia a všetky ostatné zúčastnené strany zabezpečia bezpečnosť a ochranu obchodného tajomstva, dôverných informácií, ako aj zachovanie práv duševného vlastníctva, a prijmú potrebné a primerané technické a organizačné opatrenia.

10. Vzájomné uznávanie

Poznámka o prechodnej uplatniteľnosti: Táto časť je zahrnutá s cieľom zachovať štruktúru kandidátskej schémy EÚ. V slovenskom národnom systéme sa nebude operatívne používať, kým sa nestane uplatniteľným európsky systém EUDIW.

11. Partnerské hodnotenie

Poznámka o prechodnej uplatniteľnosti: Táto časť je zahrnutá s cieľom zachovať štruktúru kandidátskej schémy EÚ. V slovenskom národnom systéme sa nebude operatívne používať, kým sa nestane uplatniteľným európsky systém EUDIW.

12. Požiadavky na údržbu a konečné požiadavky

Poznámka o prechodnej uplatniteľnosti: Táto časť je zahrnutá s cieľom zachovať štruktúru kandidátskej schémy EÚ. V slovenskom národnom systéme sa nebude používať, kým sa nestane uplatniteľným európsky systém EUDIW. Príloha XII sa zaoberá kontextom prispôsobenia slovenského národného systému európskej certifikačnej schémy.

Normatívna požiadavka: NBÚ / vlastník schémy MUSÍ udržiavať túto národnú certifikačnú schému, preskúmať jej pokračujúcu primeranosť a aktualizovať ju, ak to vyžadujú zmeny v práve Únie, slovenskom práve, európskych usmerneniach, normách, technických špecifikáciách, registroch rizík, rámcoch funkčnej zhody, architektonických profiloch alebo skúsenostiach s certifikáciou. Zmeny schémy MUSIA byť riešené prostredníctvom logiky Riadenia zmien opísanej v informatívnom kontexte a zohľadnené v príslušných prílohách.

Normatívna požiadavka: NBÚ / vlastník schémy MUSÍ zaslať návrh národnej certifikačnej schémy a akúkoľvek podstatnú revíziu skupine pre spoluprácu spolu s primeranými informáciami na účely stanovenia stanovísk a odporúčaní v súlade s nariadením (EÚ) č. 910/2014 a vykonávacím nariadením Komisie (EÚ) 2024/2981. Konečné požiadavky špecifické pre schému EÚ sa uplatnia, keď sa stane uplatniteľnou európska schéma EUDIW.