

EUDIW-CZ

České národní certifikační schéma evropské peněženky digitální identity

Identifikace schématu: EUDIW-CZ

Verze schématu: 1.2

Vlastník schématu: Digitální a informační agentura (dále DIA)

Orgán dohledu: DIA

Národní akreditační orgán: Český institut pro akreditaci (dále ČIA)

Typ schématu dle ISO 17067: 6

Flexibilita: není

Použité termíny a zkratky jsou uvedeny v příloze XVI.

Obsah

1	OBECNÁ USTANOVENÍ	3
	Článek 1 PŘEDMĚT A ROZSAH CERTIFIKACE	3
2	SPECIFICKÉ STANDARDY A POŽADAVKY PRO HODNOCENÍ	3
	Článek 3 Certifikační kritéria	3
	Článek 4 METODY CERTIFIKACE IKT SLUŽEB EUDIW	4
3	VYDÁVÁNÍ, OBNOVA A ODEBÍRÁNÍ CERTIFIKÁTŮ EUDIW-CZ	4
	Článek 5 INFORMACE NEZBYTNÉ PRO CERTIFIKACI	4
	Článek 6 PODMÍNKY PRO VYDÁNÍ CERTIFIKÁTU EUDIW-CZ	4
	Článek 7 VYDÁNÍ CERTIFIKÁTU EUDIW-CZ	5
	Článek 8 Značka důvěry EU pro peněženku digitální identity	5
	Článek 9 DOBA PLATNOSTI CERTIFIKÁTU EUDIW-CZ	6
	Článek 10 DOZOR CERTIFIKÁTU EUDIW-CZ	6
	Článek 11 ODEJMUTÍ CERTIFIKÁTU EUDIW-CZ	6
4	ORGÁNY POSUZOVÁNÍ SHODY	7
	Článek 12 SPECIFIKACE POŽADAVKŮ NA AKREDITACI ORGÁNŮ POSUZOVÁNÍ SHODY	7
	Článek 13 DALŠÍ NEBO ZVLÁŠTNÍ POŽADAVKY NA CERTIFIKAČNÍ ORGÁN	7
5	MONITOROVÁNÍ SHODY S PŘEDPISY	7
	Článek 14 MONITOROVACÍ ČINNOSTI PROVÁDĚNÉ VLASTNÍKEM SCHÉMATU	7
	Článek 15 MONITOROVACÍ ČINNOSTI CERTIFIKAČNÍHO ORGÁNU	8
	Článek 16 MONITOROVACÍ ČINNOSTI DRŽITELEM CERTIFIKÁTU	8
6	SHODA A DODRŽOVÁNÍ PŘEDPISŮ.....	9
	Článek 17 Důsledky neshody certifikované služby IKT	9
	Článek 18 Důsledky nedodržení požadavků držitelem certifikátu	9
	Článek 19 POZASTAVENÍ PLATNOSTI CERTIFIKÁTU EUDIW-CZ	9
	Článek 20 Důsledky nedodržení požadavků ze strany certifikačního orgánu	10
7	SPRÁVA ZRANITELNOSTÍ	11
	Článek 21 ROZSAH ŘÍZENÍ ZRANITELNOSTI	11
	Článek 22 POSTUPY ŘÍZENÍ ZRANITELNOSTI	11
	Článek 23 Analýza dopadu zranitelnosti	11
	Článek 24 Zpráva o analýze dopadů zranitelnosti	11
	Článek 25 Náprava zranitelnosti	12
8	ZVEŘEJNĚNÍ ZRANITELNOSTI.....	12
	Článek 26 Koordinované zveřejnění zranitelnosti	12
	Článek 27 INFORMACE SDÍLENÉ S ORGÁNY DOHLEDU	12
	Článek 28 Zveřejnění zranitelnosti	13
9	UCHOVÁVÁNÍ, ZVEŘEJŇOVÁNÍ A OCHRANA INFORMACÍ.....	13
	Článek 29 Uchovávání záznamů certifikačními orgány	13
	Článek 30 INFORMACE POSKYTNUTÉ DRŽITELEM CERTIFIKÁTU	13
	Článek 31 OCHRANA INFORMACÍ	14
10	VZÁJEMNÉ UZNÁVÁNÍ A VZÁJEMNÉ HODNOCENÍ SUBJEKTŮ POSUZOVÁNÍ SHODY.....	14
11	ÚDRŽBA A ZÁVĚREČNÁ USTANOVENÍ	14
	Článek 32 Údržba EUDIW-CZ schématu	14

12	SEZNAM PŘÍLOH	15
----	---------------------	----

1 Obecná ustanovení

Tato kapitola se zaměřuje na rozsah certifikace, který je zde uveden, ale podrobněji je popsán v příloze I.

Článek 1 PŘEDMĚT A ROZSAH CERTIFIKACE

1. Toto schéma stanoví české národní certifikační schéma EUDIW-CZ pro evropské peněženky digitální identity.
2. Certifikát vydaný podle tohoto schématu je certifikátem podle čl. 5c odst. 1 nařízení (EU) č. 910/2014 ve znění nařízení (EU) 2024/1183, a to v rozsahu vymezeném přílohou I tohoto schématu. Certifikát osvědčuje shodu řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno, s požadavky na kybernetickou bezpečnost dle přílohy X a s funkčními požadavky dle přílohy III CIR (EU) 2024/2981. K prokázání shody se nevyžaduje žádný další národní certifikační mechanismus.
3. Toto schéma se vztahuje na všechny služby informačních a komunikačních technologií („IKT“), včetně jejich dokumentace, které jsou předkládány k certifikaci v rámci EUDIW-CZ, a to zejména včetně:
 - a. služeb pro poskytování řešení peněženek (nadále Poskytovatel peněženky) a systémů elektronické identifikace („eID“), v jejichž rámci jsou poskytovány (nadále Poskytovatel PID);
 - b. Toto schéma je kompozitní, může se skládat z certifikace jednotlivých částí a následně certifikace celku.
 - c. Samostatně certifikovány mohou být např. Poskytovatel peněženky, Poskytovatel PID, jejich části atp.
4. Předmět a rozsah certifikace jsou podrobně popsány v přílohách I, Ia, Ib a Ic.
5. Toto certifikační schéma je veřejně dostupné a otevřené. Postupy certifikace jsou uplatňovány nediskriminačním způsobem. Přístup k certifikaci není omezen velikostí žadatele, jeho členstvím v jakémkoli sdružení nebo skupině, ani počtem již vydaných certifikátů. Všechny subjekty splňující technické požadavky tohoto schématu mají rovná práva a povinnosti.
6. Toto schéma je vydáno v českém a anglickém jazyce. Obě jazykové verze mají stejný obsah. V případě jakéhokoli rozporu nebo rozdílného výkladu mezi jazykovými verzemi je rozhodující české znění schématu. Anglická verze je poskytována pouze pro informační účely.

2 Specifické standardy a požadavky pro hodnocení

Tato kapitola je převážně odkazem na přílohy, které definují kritéria (příloha X) a metody (příloha XI), jež mají být použity v procesu certifikace.

Článek 3 Certifikační kritéria

1. Služby peněženky a systém elektronické identifikace, v rámci kterého je řešení EUDIW poskytováno, které jsou předloženy k certifikaci, musí být minimálně vyhodnoceny z hlediska souladu s kritérii definovanými v příloze X.

Článek 4 METODY CERTIFIKACE IKT SLUŽEB EUDIW

1. Služby IKT předložené k certifikaci musí být minimálně hodnoceny v souladu s metodami definovanými v příloze XI.
2. V případě služby IKT, která podléhá hodnocení složeného schématu, sdílí certifikační orgán (CB), který provedl hodnocení dílčí služby IKT, příslušné informace s certifikačním orgánem provádějícím hodnocení složeného schématu IKT.
3. V případě služby IKT zahrnující složku, která byla certifikována v rámci Evropského schématu certifikace kybernetické bezpečnosti, sdílí CAB, který provedl hodnocení složky, příslušné informace s certifikačním orgánem provádějícím hodnocení služby IKT.

3 Vydávání, obnova a odebírání certifikátů EUDIW-CZ

Tato kapitola definuje podmínky pro certifikaci a také životní cyklus certifikátů.

Článek 5 INFORMACE NEZBYTNÉ PRO CERTIFIKACI

1. Žadatel o certifikaci podle EUDIW-CZ poskytne nebo jinak zpřístupní certifikačnímu orgánu veškeré informace nezbytné pro certifikační činnosti.
2. Informace uvedené v odstavci 1 zahrnují informace uvedené v příloze IV.
3. Žadatelé o certifikaci mohou certifikačnímu orgánu poskytnout příslušné výsledky hodnocení z předchozí certifikace podle:
 - a. tohoto schématu;
 - b. Evropského schématu certifikace kybernetické bezpečnosti přijatého podle článku 49 nařízení (EU) 2019/881;
 - c. kvalifikace a certifikace subjekty posuzování shody akreditovanými podle požadavků CIR (EU) 2025/2162;
 - d. certifikace v rámci jiného schématu orgánem posuzování shody akreditovaným k vydávání takových certifikátů národním akreditačním orgánem členského státu EU podle nařízení (EU) 765/2008.
 - e. posuzování dle zákona 250/2017 Sb.
4. Pokud jsou výsledky hodnocení relevantní, může certifikační orgán výsledky hodnocení znovu použít za předpokladu, že tyto výsledky splňují příslušné požadavky a je potvrzena jejich pravost.
5. Žadatelé o certifikaci rovněž poskytnou certifikačnímu orgánu odkaz na své webové stránky obsahující informace, které mají být zveřejněny, jak je definováno v příloze III.
6. Veškerá relevantní dokumentace uvedená v tomto článku musí být certifikačním orgánem a žadatelem uchovávána po dobu 5 let po uplynutí platnosti certifikátu.

Článek 6 PODMÍNKY PRO VYDÁNÍ CERTIFIKÁTU EUDIW-CZ

1. Certifikační orgány vydají certifikát EUDIW-CZ, pokud jsou splněny všechny následující podmínky:
 - a. kategorie služby IKT a jejích komponent spadají do rozsahu akreditace a případně autorizace certifikačního orgánu vydávajícího certifikát;
 - b. žadatel o certifikaci podepsal prohlášení o přijetí všech závazků uvedených v odstavci 2;
 - c. certifikační orgán dokončil hodnocení bez neshody v souladu s kritérii a metodami hodnocení uvedenými v článcích 3 a 4;

- d. certifikační orgán dokončil přezkum výsledků hodnocení bez neshody.
2. Žadatel o certifikaci se zavazuje k následujícím závazkům:
 - a. poskytnout certifikačnímu orgánu veškeré potřebné, úplné a správné informace a na požádání poskytnout další potřebné informace;
 - b. nepropagovat službu IKT jako certifikovanou podle EUDIW-CZ před vydáním certifikátu EUDIW-CZ;
 - c. propagovat službu IKT jako certifikovanou pouze s ohledem na rozsah stanovený v certifikátu EUDIW-CZ;
 - d. okamžitě ukončit propagaci služby IKT jako certifikované v případě pozastavení, odebrání nebo vypršení platnosti certifikátu EUDIW-CZ;
 - e. zajistit, aby služba IKT poskytovaná s odkazem na certifikát EUDIW-CZ byla službou IKT, na kterou se vztahuje certifikace;
3. Pokud se certifikát vztahuje na služby poskytování peněženek a/nebo na poskytování PID, musí žadatel o certifikaci splňovat relevantní požadavky čl. 5a odst. 2 nařízení (EU) 2024/1183.

Článek 7 VYDÁNÍ CERTIFIKÁTU EUDIW-CZ

1. Certifikát EUDIW-CZ musí obsahovat alespoň informace uvedené v příloze V.
2. Rozsah a hranice certifikované služby IKT musí být jednoznačně specifikovány v certifikátu EUDIW-CZ nebo v **Certifikační zprávě**.
3. Certifikační orgán poskytne žadateli certifikát EUDIW-CZ alespoň v elektronické podobě.
4. Certifikační orgán vypracuje pro každý certifikát EUDIW-CZ, který vydává, **Certifikační zprávu** v souladu s přílohou VI. **Certifikační zpráva** musí být založena na **Technické zprávě o hodnocení**. **Certifikační zpráva** musí uvádět specifická kritéria a metody hodnocení uvedené v člancích 5 a 6 použité pro hodnocení.
5. Certifikační orgán vypracuje pro každý certifikát EUDIW-CZ, který vydá, **Zprávu o posouzení/hodnocení** v souladu s přílohou VII.
6. Certifikační orgán poskytne DIA [vlastník schématu] a [orgán dohledu] [a dalším] každý certifikát EUDIW-CZ, **Certifikační zprávu** a **Zprávu o posouzení/hodnocení**, které vydá, v elektronické podobě.
7. DIA [Česká republika] bez zbytečného odkladu poskytne Komisi a skupině pro spolupráci zřízené podle nařízení (EU) 2024/1183 čl. 46e odst. 1 každý certifikát EUDIW-CZ, **Certifikační zprávu** a **Zprávu o posouzení/hodnocení** v elektronické podobě, spolu s informacemi požadovanými v čl. 5d odst. 2 nařízení (EU) 2024/1183 a v příloze nařízení (EU) 2025/849.

Článek 8 Značka důvěry EU pro peněženku digitální identity

1. Poskytovatel peněženky jako držitel certifikátu může na certifikovanou službu IKT umístit značku důvěry (viz Článek 3(50) nařízení (EU) 910/2014). Značka důvěry prokazuje, že služba IKT byla certifikována v souladu s tímto systémem. Značka důvěry se umístí v souladu s prováděcím nařízením Komise (EU) 2024/2979, s tímto oddílem a s přílohou XII.
2. Značka důvěry se zobrazí viditelným, čitelným a jednoznačným způsobem v souvislosti s certifikovanou službou IKT v peněženkách. Pokud je to relevantní, značka důvěry se může adekvátním způsobem zobrazit rovněž:
 - a. na oficiálních webových stránkách držitele certifikátu popisujících certifikovanou službu IKT;
 - b. v katalogích služeb, datových listech nebo jiných materiálech s popisem služeb, ať už v elektronické nebo tištěné podobě;
 - c. ve smluvní nebo předmluvní dokumentaci týkající se certifikované služby IKT.

3. Specifikace a využití značky důvěry musí splňovat požadavky prováděcího nařízení Komise (EU) 2024/2979.

Článek 9 DOBA PLATNOSTI CERTIFIKÁTU EUDIW-CZ

1. Certifikační orgán stanoví dobu platnosti pro každý vydaný certifikát EUDIW-CZ s přihlédnutím k charakteristikám certifikované služby IKT.
2. Doba platnosti certifikátu EUDIW-CZ nesmí překročit 4 roky.
3. Odchylně od odstavce 2 může být tato lhůta prodloužena až na 5 let (4 roky + 1 rok prodloužení) s předchozím souhlasem DIA [vlastník schématu]. DIA [vlastník schématu] bez zbytečného odkladu oznámí udělení schválení skupině pro spolupráci uvedené v čl. 46e odst. 1 nařízení (EU) 2024/1183.

Článek 10 DOZOR CERTIFIKÁTU EUDIW-CZ

1. Certifikační orgán bude na žádost držitele certifikátu nebo z jiných odůvodněných důvodů pravidelně provádět dozorové posouzení shody a přezkoumávat certifikát EUDIW-CZ pro službu IKT podle harmonogramu stanoveného v příloze II. Dozorové posouzení shody se provádí v souladu s přílohou II.
2. Na základě výsledků dozorového posouzení a přezkumu shody certifikační orgán:
 - a. potvrdí certifikát EUDIW-CZ;
 - b. odebere certifikát EUDIW-CZ v souladu s článkem 11;
 - c. připojí k certifikátu EUDIW-CZ dodatek, který definuje aktualizovaný rozsah; nebo
 - d. odebere certifikát EUDIW-CZ v souladu s článkem 11 a vydá nový certifikát EUDIW-CZ se shodným nebo aktualizovaným rozsahem a prodlouženou dobou platnosti.
3. Certifikační orgán může bez zbytečného odkladu rozhodnout o pozastavení certifikátu EUDIW-CZ v souladu s článkem 19, dokud držitel certifikátu EUDIW-CZ neprovede nápravná opatření.
4. Je-li k certifikátu EUDIW-CZ přidána změna, certifikační orgán o tom bez zbytečného odkladu informuje orgán dohledu uvedený v čl. 46a odst. 1 nařízení (EU) 2024/1183, Komisi a skupinu pro spolupráci uvedenou v čl. 46e odst. 1 nařízení (EU) 2024/1183 a sdělí jim pozměněný certifikát, **Certifikační zprávu a Zprávu o posouzení/hodnocení**.

Článek 11 ODEJMUTÍ CERTIFIKÁTU EUDIW-CZ

1. Certifikát EUDIW-CZ bude odebrán certifikačním orgánem, který jej vydal, nebo DIA [vlastník schématu], pokud certifikát EUDIW-CZ není v souladu s tímto schématem.
2. Certifikační orgán uvedený v odstavci 1 oznámí odebrání certifikátu DIA [vlastník schématu] a [orgánu dohledu] [a dalším]. DIA [vlastník schématu] oznámí odebrání certifikátu dalším příslušným orgánům, pokud je to relevantní.
3. DIA [Česká republika] bez zbytečného odkladu oznámí Komisi a Skupině pro spolupráci zřízené podle čl. 46e odst. 1 odnětí osvědčení.
4. Držitel certifikátu EUDIW-CZ může požádat o jeho odebrání.

4 Orgány posuzování shody

Tato kapitola definuje požadavky, které musí splňovat orgány posuzování shody a které budou ověřovány prostřednictvím akreditace.

Článek 12 SPECIFIKACE POŽADAVKŮ NA AKREDITACI ORGÁNŮ POSUZOVÁNÍ SHODY

1. Certifikační orgány jsou akreditovány národními akreditačními orgány jmenovanými podle nařízení (ES) č. 765/2008 v souladu s normami EN ISO/IEC 17065:2012 a ETSI EN 319 403-1 V2.3.1 (2020-06).
2. Akreditace subjektů posuzování shody musí zohledňovat specifikaci požadavků na akreditaci certifikačních subjektů, jak je stanoveno v Příloze VIII.

Článek 13 DALŠÍ NEBO ZVLÁŠTNÍ POŽADAVKY NA CERTIFIKAČNÍ ORGÁN

(prázdné)

5 Monitorování shody s předpisy

U každého vydaného certifikátu musí vlastník systému, certifikační orgán a držitel certifikátu sledovat soulad systému peněženky EUDI a eID s požadavky certifikátu.

Článek 14 MONITOROVACÍ ČINNOSTI PROVÁDĚNÉ VLASTNÍKEM SCHÉMATU

1. DIA [vlastník schématu] sleduje, zda:
 - a. certifikační orgány plní své povinnosti podle nařízení (EU) 2024/1183 a podle tohoto schématu;
 - b. držitelé certifikátu EUDIW-CZ plní své povinnosti podle tohoto schématu;
 - c. certifikované služby IKT splňují požadavky stanovené v EUDIW-CZ;
 - d. záruka vyjádřená v certifikátu EUDIW-CZ splňuje vyvíjející se prostředí hrozeb.
2. DIA [vlastník schématu] provádí své monitorovací činnosti zejména na základě:
 - a. informací pocházejících od certifikačních orgánů, národních akreditačních orgánů a případně dalších orgánů, pokud je to relevantní;
 - b. informací vyplývajících z jeho vlastních auditů a šetření nebo auditů a šetření jiných orgánů;
 - c. obdržených stížností a odvolání.
3. DIA [vlastník schématu] vybere vzorek certifikovaných služeb IKT, které mají být prověřeny, s využitím objektivních kritérií, včetně:
 - a. kategorie služby;
 - b. držitele certifikátu;
 - c. certifikačního orgánu;
 - d. specifických bodů, na které je třeba zaměřit pozornost, definovaných DIA [vlastníkem schématu];
 - e. jakýchkoli dalších informací, které byly orgánu předloženy.
4. DIA [vlastník schématu] informuje držitele certifikátu EUDIW-CZ o vybraných IKT službách a kritériích výběru.
5. Certifikační orgán, který certifikoval vybranou službu IKT, provede na žádost DIA [vlastníka schématu] dodatečný přezkum v souladu s postupem stanoveným v příloze II a informuje [vlastníka schématu] o výsledcích.

6. Pokud má DIA [vlastník schématu] dostatečný důvod se domnívat, že certifikovaná služba IKT již není v souladu s tímto schématem nebo nařízením (EU) 2024/1183, může provést šetření.
7. DIA [vlastník schématu] splňuje a dohlíží nad dodržováním zákona 250/2017 Sb.
8. DIA [vlastník schématu] informuje příslušný certifikační orgán o probíhajících šetřeních týkajících se vybraných služeb IKT.
9. Pokud DIA [vlastník schématu] zjistí, že probíhající šetření se týká služeb IKT, které jsou certifikovány certifikačními orgány usazenými v jiných členských státech, informuje o tom [vlastníka schématu] příslušných členských států za účelem spolupráce na šetřeních, je-li to relevantní. Tento [vlastník schématu] rovněž informuje skupinu pro spolupráci uvedenou v čl. 46e odst. 1 nařízení (EU) 2024/1183 o přeshraničních šetřeních a následných výsledcích.
10. DIA [vlastník schématu] může své činnosti vykonávat za využití subdodavatelů.

Článek 15 MONITOROVACÍ ČINNOSTI CERTIFIKAČNÍHO ORGÁNU

1. Certifikační orgán sleduje soulad:
 - a. plnění povinností držitelů certifikátu podle tohoto schématu a nařízení (EU) č. 910/2014 v souvislosti s certifikátem EUDIW-CZ, který certifikační orgán vydal;
 - b. soulad služeb IKT, které certifikoval, s jejich příslušnými bezpečnostními požadavky.
2. Certifikační orgán provádí své monitorovací činnosti na základě:
 - a. informací poskytnutých na základě závazků žadatele o certifikaci uvedených v článku 6(2);
 - b. informací vyplývajících z činností jiných příslušných orgánů dohledu nad trhem;
 - c. obdržených stížností a odvolání;
 - d. informací o zranitelnosti, které by mohly mít dopad na certifikované IKT služby.

Článek 16 MONITOROVACÍ ČINNOSTI DRŽITELEM CERTIFIKÁTU

1. Držitel certifikátu EUDIW-CZ provádí následující úkony za účelem sledování shody certifikované služby IKT s jejími bezpečnostními požadavky:
 - a. monitorovat informace o zranitelnosti týkající se certifikované služby IKT, včetně známých závislostí, vlastními prostředky, ale také s ohledem na:
 - 1) publikaci nebo podání týkající se informací o zranitelnosti uživatelem nebo bezpečnostním výzkumníkem, či prostřednictvím kontaktování poskytovatele za tímto účelem;
 - 2) podání z jakéhokoli jiného zdroje;
 - b. monitorovat záruky vyjádřené v certifikátu EUDIW-CZ, a zejména vývoj stavu jakéhokoli certifikátu nebo zprávy o záruce použité jako objektivní důkaz při hodnocení služby IKT.
2. Držitel certifikátu EUDIW-CZ je povinen spolupracovat s certifikačním orgánem a případně s DIA [vlastníkem schématu] na podpoře jejich monitorovacích činností.
3. Držitel certifikátu EUDIW-CZ je povinen bez zbytečného odkladu oznámit certifikačnímu orgánu následující události:
 - a. jakékoli narušení nebo ohrožení poskytované IKT služby;
 - b. jakoukoli podstatnou změnu IKT služby.

6 Shoda a dodržování předpisů

Jakmile je zjištěna neshoda nebo nedodržení požadavků, má to důsledky, které jsou definovány v této kapitole.

Článek 17 Důsledky neshody certifikované služby IKT

1. Pokud certifikační orgán zjistí neshodu certifikované služby IKT s požadavky stanovenými v nařízení (EU) 2024/1183, informuje držitele certifikátu EUDIW-CZ o zjištěné neshodě a požádá o nápravná opatření a neprodleně o tom informuje orgán dohledu uvedený v čl. 46a odst. 1 nařízení (EU) 2024/1183.
2. Po obdržení informací uvedených v odstavci 1 držitel certifikátu EUDIW-CZ ve lhůtě stanovené certifikačním orgánem, která nesmí překročit 30 dnů, navrhne certifikačnímu orgánu nápravná opatření nezbytná k řešení neshody.
3. Certifikační orgán může bez zbytečného odkladu pozastavit platnost certifikátu EUDIW-CZ v souladu s článkem 19 v případě nouze nebo pokud držitel certifikátu EUDIW-CZ řádně nespolutupracuje s certifikačním orgánem.
4. Certifikační orgán provede šetření, aby posoudil, zda nápravná opatření řeší neshodu.
5. Pokud držitel certifikátu EUDIW-CZ nenavrhne vhodná nápravná opatření ve lhůtě uvedené v odstavci 2, bude certifikát pozastaven v souladu s článkem 19 nebo odebrán v souladu s článkem 11.
6. Tento článek se nevztahuje na případy zranitelností ovlivňujících certifikovanou službu IKT, které se řeší v souladu s kapitolou 7 tohoto schématu.

Článek 18 Důsledky nedodržení požadavků držitelem certifikátu

1. Pokud certifikační orgán zjistí, že:
 - a. držitel certifikátu EUDIW-CZ nebo žadatel o certifikaci neplní své závazky a povinnosti stanovené v článku 6(2), článku 16 a článku 31; nebo
 - b. držitel certifikátu EUDIW-CZ neplní kapitolu 8 tohoto schématu;stanoví se lhůta nepřesahující 30 dnů, ve které držitel certifikátu EUDIW-CZ přijme nápravná opatření.
2. Pokud držitel certifikátu EUDIW-CZ nenavrhne vhodná nápravná opatření ve lhůtě uvedené v odstavci 1, bude certifikát pozastaven v souladu s článkem 19 nebo odebrán v souladu s článkem 11.
3. Trvalé nebo opakované porušování povinností uvedených v odstavci 1 držitelem certifikátu EUDIW-CZ má za následek odebrání certifikátu EUDIW-CZ v souladu s článkem 11.
4. Certifikační orgán informuje DIA [vlastníka schématu] [orgán dohledu], případně další relevantní subjekty.

Článek 19 POZASTAVENÍ PLATNOSTI CERTIFIKÁTU EUDIW-CZ

1. Pokud se jedná o pozastavení certifikátu EUDIW-CZ, certifikační orgán pozastaví platnost dotčeného certifikátu EUDIW-CZ na dobu odpovídající okolnostem, které k pozastavení vedly, nepřesahující 42 dnů. Doba pozastavení začíná dnem následujícím po dni rozhodnutí certifikačního orgánu. Pozastavení nemá vliv na platnost certifikátu.

2. Certifikační orgán bez zbytečného odkladu informuje držitele certifikátu a DIA [vlastníka schématu] o pozastavení a uvede důvody pozastavení, požadovaná opatření a dobu pozastavení.
3. Držitel certifikátu informuje dotčené uživatele služeb IKT o pozastavení a o důvodech pozastavení uvedených certifikačním orgánem, s výjimkou těch částí důvodů, jejichž sdílení by představovalo bezpečnostní riziko nebo které obsahují citlivé informace, jakož i pokyny pro uživatele služby IKT. Držitel certifikátu tyto informace rovněž zveřejní.
4. (prázdný)
5. V řádně odůvodněných případech může DIA [vlastník schématu] povolit prodloužení doby pozastavení certifikátu EUDIW-CZ. Celková doba pozastavení nesmí překročit 1 rok.

Článek 20 Důsledky nedodržení požadavků ze strany certifikačního orgánu

6. V případě nedodržení povinností certifikačním orgánem DIA [vlastník schématu] bez zbytečného odkladu:
 - a. identifikuje potenciálně dotčené certifikáty EUDIW-CZ;
 - b. v případě potřeby k podpoře této identifikace požádá o provedení činností posuzování shody u jedné nebo více služeb IKT buď certifikačním orgánem, který certifikát vydal, nebo jakýmkoli jiným akreditovaným a autorizovaným certifikačním orgánem, který může být technicky lépe schopen provádět tyto činnosti;
 - c. analyzuje dopady nedodržení povinností certifikačním orgánem;
 - d. informuje držitele certifikátů EUDIW-CZ dotčených nedodržením povinností ze strany certifikačního orgánu.
2. Pro každý certifikát dotčený neshodou certifikačního orgánu DIA [vlastník schématu] bez zbytečného odkladu:

identifikuje činnosti posuzování shody, které je třeba provést znovu, v případě potřeby s podporou dotčeného (nesouladného) certifikačního orgánu nebo jiného akreditovaného a autorizovaného certifikačního orgánu, který může být technicky lépe vybaven pro provedení těchto činností;

pro každou takovou činnost posuzování shody požádá o provedení činnosti buď certifikační orgán, který certifikát vydal, nebo jiný akreditovaný a autorizovaný certifikační orgán, který může být technicky lépe vybaven pro provedení této činnosti.
3. Jakákoli neshoda certifikované služby IKT zjištěná při opětovném provádění činností posuzování shody se zpracuje podle článku 17.
4. Nevyhovující certifikační orgán je odpovědný za náklady spojené s činnostmi uvedenými v odstavci 2.
5. Na základě opatření uvedených v odstavci 1 DIA [vlastník schématu]:
 - a. v případě potřeby oznámí neshodu certifikačního orgánu národnímu akreditačnímu orgánu (ČIA);
 - b. v případě potřeby posoudí potenciální dopad na autorizaci.
1. Proti rozhodnutí orgánu posuzování shody je možné se odvolat.
 - a. Odvolacím orgánem je Digitální a informační agentura jako vlastník schématu.
 - b. Digitální a informační agentura si může vyžádat posouzení od jí stanovené nezávislé osoby.
 - c. Náklady spojené s odvoláním hradí:
 - i. orgán posuzování shody, v případě uznání, že orgán posuzování shody pochybil.
 - ii. v opačném případě odvolávající se osoba

7 Správa zranitelností

Tato kapitola se zabývá pravidly pro správu zranitelností, která jsou zde poměrně omezená, protože většinou omezují politiku správy zranitelností, kterou je povinen zavést každý poskytovatel certifikovaných služeb.

Článek 21 ROZSAH ŘÍZENÍ ZRANITELNOSTI

Tato kapitola se vztahuje na služby IKT, pro které byl vydán certifikát EUDIW-CZ.

Článek 22 POSTUPY ŘÍZENÍ ZRANITELNOSTI

1. Držitel certifikátu EUDIW-CZ zavede, udržuje a provozuje všechny nezbytné postupy pro řízení zranitelností v souladu s pravidly stanovenými v tomto oddíle a v případě potřeby doplněné postupy stanovenými v normě EN ISO/IEC 30111.
2. Pro všechny relevantní komponenty služby IKT zahrnují postupy řízení zranitelností uvedené v odstavci 1:
 - a. Soupis softwarových komponent v běžně používaném a strojově čitelném formátu, který zahrnuje alespoň závislosti komponenty na nejvyšší úrovni;
 - b. použití bezpečnostních aktualizací k nápravě zranitelností, a pokud je to technicky proveditelné, odděleně od funkčních aktualizací;
 - c. aktivuje mechanismus pro bezpečnou distribuci aktualizací, včetně mechanismu k zajištění neprodlené nápravy zranitelností, případně automatizované distribuce bezpečnostních aktualizací a případně mechanismu pro deaktivaci provozu peněženky, dokud nebudou použity požadované bezpečnostní aktualizace;
 - d. použije distribuci v souvislosti s aktualizacemi informačních zpráv poskytujících uživatelům relevantní informace, včetně informací o možných opatřeních, která je třeba podniknout.
3. Držitel certifikátu EUDIW-CZ musí udržovat a zveřejňovat vhodné metody pro získávání informací o zranitelnostech souvisejících s jeho produkty z externích zdrojů, včetně uživatelů, certifikačních orgánů a bezpečnostních výzkumníků.
4. Pokud držitel certifikátu EUDIW-CZ zjistí nebo obdrží informaci o potenciální zranitelnosti ovlivňující certifikovanou službu IKT, zaznamená ji a provede analýzu dopadu zranitelnosti.
5. Na základě odůvodněné žádosti certifikačního orgánu, který certifikát vydal, předá držitel certifikátu EUDIW-CZ tomuto certifikačnímu orgánu veškeré relevantní informace o potenciálních zranitelnostech.

Článek 23 Analýza dopadu zranitelnosti

1. Analýza dopadu zranitelnosti se musí vztahovat k popisu předmětu certifikace a k prohlášením o zárukách obsaženým v certifikátu. Analýza dopadu zranitelnosti se provádí v časovém rámci odpovídajícím využitelnosti a kritičnosti potenciální zranitelnosti certifikované služby IKT.
2. Významnost dopadu se určí v souladu s příslušnou metodikou definovanou v příloze XI, aby se určila možnost zneužití a dopad zranitelností.

Článek 24 Zpráva o analýze dopadů zranitelnosti

1. Držitel vypracuje zprávu o analýze dopadu zranitelnosti, pokud analýza dopadu ukáže, že zranitelnost má podstatný dopad na bezpečnost služby IKT, jak je definována v příloze XI, což má následně pravděpodobný dopad na shodu služby IKT s jejím certifikátem.

2. Zpráva o analýze dopadu zranitelnosti musí obsahovat posouzení následujících prvků:
 - a. dopad zranitelnosti na certifikovanou službu IKT;
 - b. možná rizika spojená s blízkostí nebo dostupností útoku;
 - c. zda lze zranitelnost napravit;
 - d. pokud lze zranitelnost napravit, možná řešení zranitelnosti.
3. Zpráva o analýze dopadu zranitelnosti musí v příslušných případech obsahovat podrobnosti o možných způsobech zneužití zranitelnosti. S informacemi týkajícími se možných způsobů zneužití zranitelnosti se nakládá v souladu s vhodnými bezpečnostními opatřeními k ochraně jejich důvěrnosti a v případě potřeby k zajištění jejich omezeného šíření.
4. Držitel certifikátu EUDIW-CZ předá certifikačnímu orgánu bez zbytečného odkladu zprávu o analýze dopadu zranitelnosti.
5. Pokud zpráva o analýze dopadu zranitelnosti stanoví, že zranitelnost má podstatný dopad na bezpečnost služby IKT a že ji lze napravit, použije se článek 25.
6. Pokud zpráva o dopadu zranitelnosti uvede, že zranitelnost má podstatný dopad na bezpečnost služby IKT a že ji nelze napravit, certifikát EUDIW-CZ se odebere v souladu s článkem 11.
7. Držitel certifikátu EUDIW-CZ bude monitorovat veškeré zbývající zranitelnosti, aby zajistil, že je nelze zneužít v případě změn v provozním prostředí.
8. Zbývající zranitelnosti se zohlední v pravidelných hodnoceních zranitelností.

Článek 25 Náprava zranitelnosti

1. Držitel certifikátu EUDIW-CZ musí včas navrhnout a implementovat plán nápravy pro všechny zranitelnosti, které mohou mít dopad na certifikovanou službu IKT.
2. Pokud držitel certifikátu EUDIW-CZ předložil svému certifikačnímu orgánu zprávu o analýze dopadu zranitelnosti, předloží certifikačnímu orgánu také návrh na vhodná nápravná opatření. Certifikační orgán přezkoumá certifikát v souladu s článkem 10. Rozsah přezkoumání je určen navrhovanou nápravou zranitelnosti.

8 Zveřejnění zranitelnosti

Zveřejňování zranitelností je třeba provádět zodpovědně, v souladu s koordinovanou politikou zveřejňování zranitelností, a je také třeba organizovat určitou spolupráci.

Článek 26 Koordinované zveřejnění zranitelnosti

1. Držitel certifikátu EUDIW-CZ musí zavést, udržovat a provozovat koordinovanou politiku zveřejňování zranitelností a související postupy v souladu s pravidly stanovenými v tomto oddíle a v případě potřeby doplněnými postupy stanovenými v normě EN ISO/IEC 29147.
2. Držitel certifikátu EUDIW-CZ zveřejní své koordinované zásady a postupy pro zveřejňování zranitelností.

Článek 27 INFORMACE SDÍLENÉ S ORGÁNY DOHLEDU

1. Informace poskytnuté certifikačním orgánem DIA [vlastníkovi schématu] musí zahrnovat všechny prvky nezbytné k tomu, aby DIA [vlastník schématu] pochopil dopad zranitelnosti, změny, které je třeba provést v IKT službě, a pokud jsou k dispozici, veškeré informace od certifikačního orgánu o širších důsledcích zranitelnosti pro další certifikované IKT služby.

2. Informace poskytnuté v souladu s odstavcem 1 neobsahují podrobnosti o způsobech zneužití zranitelnosti. Tímto ustanovením nejsou dotčeny vyšetřovací pravomoci DIA [vlastníka schématu].
3. DIA [vlastník schématu] sdílí relevantní informace obdržené v souladu s článkem 27 s národními orgány dohledu zřízenými v jejich zemi podle článku 46a(1) nařízení (EU) 2024/1183.
4. DIA [orgán dohledu] sdílí příslušné informace obdržené v souladu s článkem 27 s vnitrostátními orgány dohledu zřízenými v jiných členských státech.

Článek 28 Zveřejnění zranitelnosti

Po odebrání certifikátu nebo po odstranění zranitelnosti, případně včetně přidání změny certifikátu, držitel certifikátu EUDIW-CZ zveřejní a zaregistruje jakoukoli veřejně známou a odstraněnou zranitelnost v dané službě IKT nebo jejích složkách v evropské databázi zranitelností zřízené v souladu s článkem 12 směrnice Evropského parlamentu a Rady (EU) 2022/2555 nebo v jiných online úložištích uvedených v popisu certifikované služby.

9 Uchovávání, zveřejňování a ochrana informací

Pravidla definovaná v této kapitole se týkají především správy dokumentace, aby se zajistilo, že zůstane k dispozici v případě technického problému nebo právního sporu.

Článek 29 Uchovávání záznamů certifikačními orgány

1. Certifikační orgány vedou systém záznamů, který obsahuje všechny dokumenty vypracované v souvislosti s každým hodnocením a certifikací, které provádějí.
2. Certifikační orgány uchovávají záznamy bezpečným způsobem a uchovávají je po dobu nezbytnou pro účely tohoto schématu, a to nejméně 5 let po odebrání příslušného certifikátu EUDIW-CZ. Pokud certifikační orgán vydal nový certifikát EUDIW-CZ v souladu s článkem 10(2) písm. d), uchovává dokumentaci k odebranému certifikátu EUDIW-CZ spolu s novým certifikátem EUDIW-CZ, a to po dobu platnosti nového certifikátu EUDIW-CZ.

Článek 30 INFORMACE POSKYTNUTÉ DRŽITELEM CERTIFIKÁTU

1. Informace uvedené v příloze III jako informace zpřístupněné veřejnosti musí být dostupné v jazyce, který je pro uživatele snadno přístupný.
2. Držitel certifikátu EUDIW-CZ je povinen po dobu nezbytnou pro účely tohoto schématu, a to nejméně 5 let po odebrání příslušného certifikátu EUDIW-CZ bezpečně uchovávat následující:
 - a. záznamy o informacích poskytnutých certifikačnímu orgánu během certifikačního procesu;
 - b. vzor komponent produktu certifikované služby IKT.
3. Pokud certifikační orgán vydal nový certifikát EUDIW-CZ v souladu s článkem 10(2) písm. d), držitel si uchovává dokumentaci k odebranému certifikátu EUDIW-CZ spolu s novým certifikátem EUDIW-CZ a po dobu platnosti nového certifikátu.
4. Na žádost certifikačního orgánu nebo DIA [vlastníka schématu] zpřístupní držitel certifikátu EUDIW-CZ záznamy a kopie uvedené v odstavci 2.

Článek 31 OCHRANA INFORMACÍ

Orgány posuzování shody, DIA [vlastník schématu] [orgán dohledu], Komise a všechny ostatní strany zajistí bezpečnost a ochranu obchodního tajemství a dalších důvěrných informací, jakož i ochranu práv duševního vlastnictví a přijmou nezbytná a vhodná technická a organizační opatření.

10 Vzájemné uznávání a vzájemné hodnocení subjektů posuzování shody.

Prázdné.

11 Údržba a závěrečná ustanovení

Tato kapitola se zabývá údržbou schématu EUDIW-CZ.

Článek 32 Údržba EUDIW-CZ schématu

1. Schéma EUDIW-CZ bude pravidelně revidováno a aktualizováno tak, aby odráželo změny v prostředí, včetně alespoň:
 - a. změny v právním prostředí, zejména v prováděcích nařízeních Komise k nařízení (EU) 2024/1183;
 - b. změn v prostředí hrozeb, zejména změn v registru rizik definovaném v příloze I nařízení CIR (EU) 2024/2981;
 - c. změn v technickém prostředí, zejména v příslušných normách a schématech posuzování shody, a aktualizací architektur peněženek v rozsahu schématu EUDIW-CZ.
 - d. Změny zákona 250/2017 Sb.
2. Vlastník schématu sleduje:
 - a. změny uvedené v odstavci 1;
 - b. zpětnou vazbu od CAB a držitelů certifikátů, jakož i stížnosti, které CAB a vlastník schématu obdrželi.
3. Vlastník schématu alespoň jednou ročně zváží změny nahromaděné od poslední aktualizace schématu EUDIW-CZ a schéma EUDIW-CZ aktualizuje, pokud jsou tyto změny považovány za podstatné.
4. Každá aktualizace schématu EUDIW-CZ musí definovat časový harmonogram pro přijetí nových opatření definovaných ve schématu a pro změny v referenčních dokumentech, který musí zohledňovat specifické potřeby probíhajících a již plánovaných činností posuzování shody.
5. Vlastník schématu bezodkladně informuje Národní akreditační orgán o změnách schématu.

12 Seznam příloh

PŘÍLOHA I: ROZSAH CERTIFIKACE

PŘÍLOHA Ia: Rozsah certifikace: Poskytování peněženky

PŘÍLOHA Ib: Rozsah certifikace: Poskytování PID

PŘÍLOHA Ic: Rozsah certifikace: Zastřešující certifikát

PŘÍLOHA II: ZAJIŠTĚNÍ KONTINUITY A ŽIVOTNÍ CYKLUS CERTIFIKACE

PŘÍLOHA III: SEZNAM VEŘEJNĚ DOSTUPNÝCH INFORMACÍ

PŘÍLOHA IV: SEZNAM INFORMACÍ POŽADOVANÝCH PŘI ŽÁDOSTI O CERTIFIKACI

PŘÍLOHA V: OBSAH CERTIFIKÁTU

PŘÍLOHA VI: OBSAH Certifikační zprávy

PŘÍLOHA VII: OBSAH ZPRÁVY O POSOUZENÍ/HODNOCENÍ

PŘÍLOHA VIII: POŽADAVKY NA ORGÁNY POSUZOVÁNÍ SHODY (CAB)

PŘÍLOHA IX: KRITÉRIA PRO POSOUZENÍ PŘIJATELNOSTI ZAJIŠTĚNÍ INFORMACÍ

PŘÍLOHA X: BEZPEČNOSTNÍ POŽADAVKY NA PENĚŽENKY EUDI A SYSTÉMY eID, V RÁMCI KTERÝCH JSOU POSKYTOVÁNY

PŘÍLOHA XI: METODY A POSTUPY PRO HODNOTÍCÍ ČINNOSTI

XII ZNAČKA DŮVĚRY A ŠTÍTKY

PŘÍLOHA XIII: SOULAD S NAŘÍZENÍM (EU) 2024/2981

PŘÍLOHA XIV: Soulad s odstavcem 6.5 EN ISO/IEC 17067:2013

PŘÍLOHA XV: SOULAD S REGULACÍ ČIA

PŘÍLOHA XVI: POUŽITÉ TERMÍNY A ZKRATKY