

14 Příloha I: Rozsah certifikace

Příloha definuje rozsah certifikace, který se skládá z předmětu certifikace a z celkového pohledu na požadavky na každou komponentu služby. Certifikáty se v rámci tohoto schématu vydávají pro služby IKT související s evropskými peněženkami digitální identity a se systémy elektronické identifikace, v jejichž rámci jsou poskytovány, jak je uvedeno v článku 1 tohoto schématu.

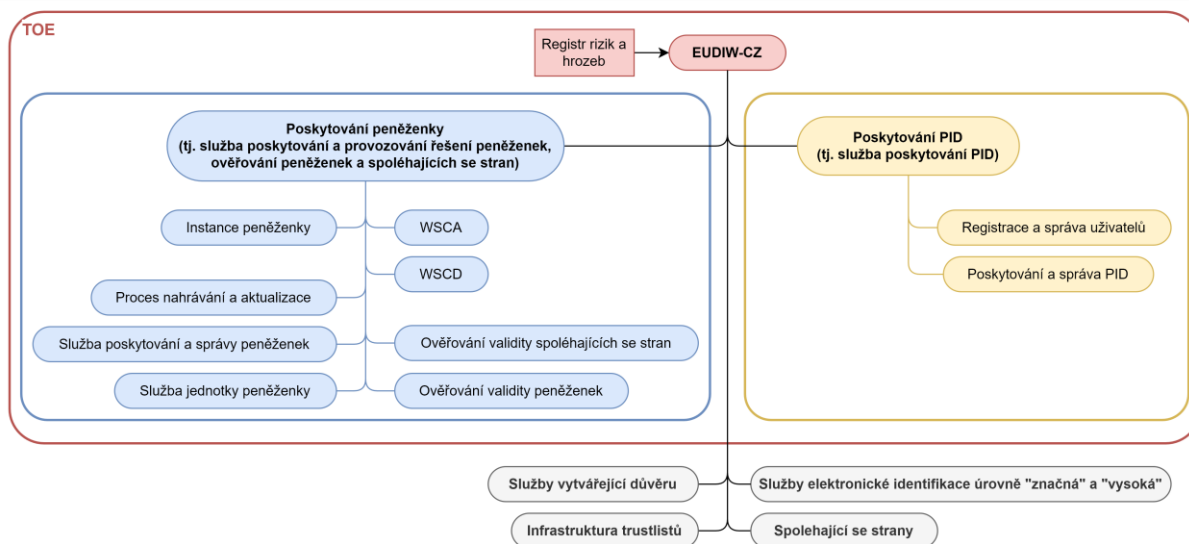


Schéma je složené z certifikace:

- Poskytovatele peněženky, tj. služby pro poskytování a provozování řešení peněženky, ověřování peněženek a spolehlivých se stran.
- Poskytovatele PID, tj. služby pro poskytování údajů o identifikaci osoby (PID)
- Zastřešující certifikace dle tohoto schématu EUDIW-CZ

Mimo rozsah certifikace jsou:

- Služby vytvářející důvěru (např. vydávání kvalifikovaných certifikátů, kvalifikovaného podepisování / pečetení, vydávání kvalifikovaných atributů, ...)
- Služby elektronické identifikace atestované dle zákona 250/2017 Sb. pro oblast elektronické identifikace - pro kontext EUDIW-CZ jsou relevantní úrovně značná a vysoká.
- Služby poskytující seznamy kvalifikovaných služeb (LoTL) a důvěryhodných entit (LoTE)
- Všechny další spolehliví se strany kromě PID

Vztah k rámci ochrany osobních údajů a k čl. 5c nařízení eIDAS

Certifikace dle tohoto schématu pokrývá požadavky čl. 5c odst. 1 nařízení eIDAS, tj. požadavky čl. 5a odst. 4, 5 a 8, požadavek na logické oddělení dle čl. 5a odst. 14 a použitelné normy a specifikace dle čl. 5a odst. 24, v rozsahu upřesněném CIR (EU) 2024/2981.

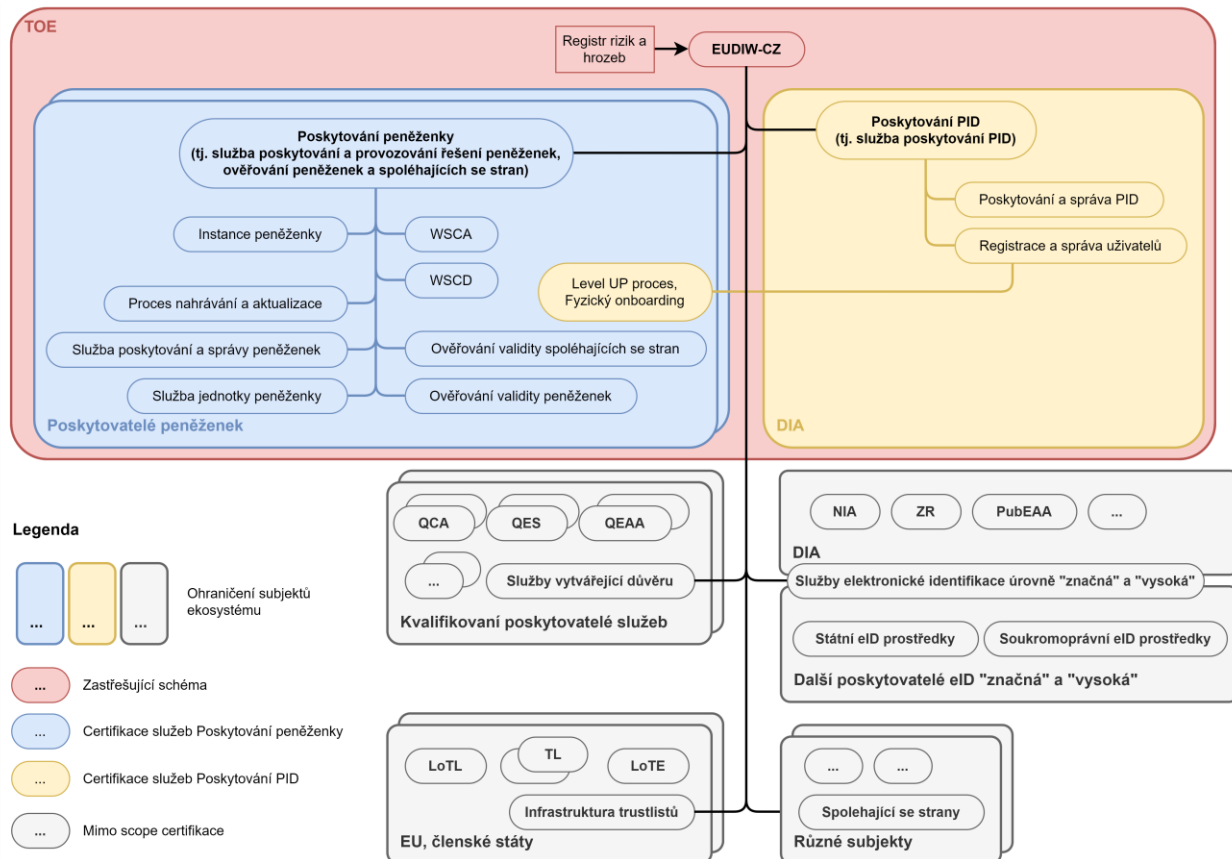
Tato verze schématu se primárně soustřeďuje (ale neomezuje) na architekturu peněženek založenou na:

- Mobilních aplikací

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

- Využití vzdálené WSCA a WSCD, případně lokálního externího WSCD
- Implementaci služeb kvalifikovaného podepisování / pečetění pomocí kvalifikované služby správy prostředků pro vytváření elektronických podpisů / pečeti na dálku.

Subjekty, které jsou v ekosystému EUDIW a které souvisejí s certifikačním schématem:



- **Poskytovatelé peněženek** - jeden nebo více poskytovatelů řešení evropských peněženek digitální identity. Zajišťují dodávku a provoz komponent certifikovaných podle části "Poskytování peněženky".
 - Vybraný koncesionář doručí i služby pro fyzické ověření totožnosti a level-up proces ověření totožnosti na základě eID úrovně značná s cílem možné přepoužitelnosti dalšími poskytovateli peněženek. Dále také službu pro ověřování totožnosti za fyzické přítomnosti žadatele o PID. Tato funkčnost podléhá certifikaci podle části "Poskytování PID".
 - Všichni poskytovatelé peněženek musí zajistit i bezplatné poskytování služeb "Ověřování validity spoléhajících se stran" a "Ověřování validity peněženek" dle nařízení eIDAS, čl. 5a(8).
- **Digitální informační agentura (DIA)** - zastřešuje dodávku a provoz certifikovaných i necertifikovaných komponent ekosystému EUDIW v ČR.
 - Certifikované komponenty jsou certifikovány podle části "Poskytování PID".
 - Komponenty, které nejsou ve scope certifikace, ale účastní se procesů podpory funkcí ekosystému EUDIW. Jde zejména o:
 - Národní bod pro identifikaci a autentizaci (NIA) - národní systém elektronické identifikace, přímo poskytující nebo zprostředkující využití prostředků elektronické identifikace úrovně vysoká a značná.

- Základní registry (ZR), především

Registr obyvatel – vede evidenci občanů ČR, popř. cizinců a je autoritativním zdrojem dat pro PID.

- Poskytovatel PubEAA
- Další podpůrné systémy
- **Další poskytovatelé eID "značná" a "vysoká"** - poskytovatelé služeb elektronické identifikace značná a vysoká, jejichž prostředky jsou poskytovány NIA a které mohou být použity v procesech ověření identity za účelem vydání PID. **Kvalifikovaní poskytovatelé služeb vytvářejících důvěru** (QTSP) - poskytovatelé různých kvalifikovaných služeb vytvářejících důvěru, v kontextu EUDIW jsou důležití poskytovatelé vydávání certifikátů pro elektronické podpisy a pečeti (QCA), správy prostředků pro vytváření elektronických podpisů / pečeti na dálku (QES), vydávání elektronických potvrzení atributů (QEAA) a dalších.
- **EU, členské státy** - zajišťující chod služeb publikace trustlistů a seznamů důvěryhodných entit, zahrnují mj. i komerční subjekty publikující služby ověření platnosti certifikátů.
- Různé subjekty – prakticky bez omezení typů subjektů, které jsou spoléhajícími se stranami, případně vč. poskytovatelů EAA.

1.1. Společný rozsah pro všechny služby

Každá certifikovaná služba IKT je kombinací komponent, které samy o sobě mohou být IKT produkty, IKT služby, systémy řízení informační bezpečnosti (ISMS) nebo procesy.

Každá služba IKT certifikovaná v rámci tohoto schématu musí zahrnovat alespoň následující komponenty, které musí být prokázány v souladu s požadavky uvedenými v následující tabulce.

POZNÁMKA: V tabulce níže jsou hlavní požadavky, které je třeba splnit, uvedeny jako „**Referenční**“. Naplnění požadavků může být doplněno dalšími/alternativními požadavky („**Další**“), jejichž využití je blíže specifikováno v Příloze IX.

POZNÁMKA: Vydání norem uvedených ve sloupci „Platné požadavky“ stanoví Rejstřík referenčních dokumentů v této příloze.

Komponenta	Popis	Platné požadavky
Systém IKT	Systém IKT, na kterém je pro své poskytování služba IKT závislá. Upozorňujeme, že systém IT je zahrnut jako „full-stack“, takže se očekává, že důkazy o shodě budou k dispozici pro celý systém.	Referenční: ● ETSI EN 319 401 ● NIS2 CIR (EU) 2024/2690 ● Zákon č. 264/2025 Sb., o kybernetické bezpečnosti a příslušné prováděcí vyhlášky Další: ● CEN TS 18026, úroveň „značná“ ● EN ISO/IEC 27001

Komponenta	Popis	Platné požadavky
Proces vývoje	Proces, který poskytovatel služeb IKT provozuje pro vývoj svých služeb IKT.	Referenční: - ETSI EN 319 401 Další: - NIS2 CIR (EU) 2024/2690 - Zákon č. 264/2025 Sb., o kybernetické bezpečnosti a příslušné prováděcí vyhlášky - CEN TS 18026, úroveň „značná“ - EN ISO/IEC 27001
Proces řízení změn	Proces provozovaný poskytovatelem služeb IKT pro správu změn ve službě IKT.	Referenční: - ETSI EN 319 401 Další: - NIS2 CIR (EU) 2024/2690 - Zákon č. 264/2025 Sb., o kybernetické bezpečnosti a příslušné prováděcí vyhlášky - CEN TS 18026, úroveň „značná“ - EN ISO/IEC 27001
Proces správy zranitelností	Proces provozovaný poskytovatelem služeb IKT pro správu a řešení zranitelností v rámci služby IKT.	Referenční: - ETSI EN 319 401 Další: - CRA, Příloha I, Sekce 2 - NIS2 CIR (EU) 2024/2690 - Zákon č. 264/2025 Sb., o kybernetické bezpečnosti a příslušné prováděcí vyhlášky - CEN TS 18026, úroveň „značná“ - EN ISO/IEC 27001
Proces řízení incidentů	Proces provozovaný poskytovatelem služeb IKT pro řízení a řešení kybernetických bezpečnostních incidentů v rámci služby IKT.	Referenční: - ETSI EN 319 401 Další: - NIS2 CIR (EU) 2024/2690 - Zákon č. 264/2025 Sb., o kybernetické bezpečnosti a příslušné prováděcí vyhlášky 2024/2690 - CEN TS 18026, úroveň „značná“ - EN ISO/IEC 27001

Komponenta	Popis	Platné požadavky
Proces řízení podvodů	Proces provozovaný poskytovatelem služeb IKT pro řízení podvodů v oblasti služeb IKT.	Referenční: Příloha X

POZNÁMKA: Tyto procesy budou s největší pravděpodobností definovány a propojeny jako součást systému řízení bezpečnosti informací (ISMS), který by mohl být vyhodnocen samostatně.

Poskytovatel služeb IKT musí prokázat platnost předpokladů definovaných pro prostředí používané komponentami IKT služby:

- pokud prostředí poskytuje poskytovatel IKT služeb, pak poskytovatel poskytne důkazy, že prostředí splňuje všechny pro něj definované předpoklady
- pokud prostředí poskytuje uživatel peněženky, pak poskytovatel IKT služeb definuje vhodné kontroly k ověření předpokladů týkajících se prostředí a ověří dostatečnost těchto opatření a jejich účinnost.

POZNÁMKA: Pojem „prostředí poskytuje poskytovatel IKT služeb“ zahrnuje prostředí, která poskytuje třetí strana smluvně najatá poskytovatelem IKT služeb (např. poskytovatel cloudových služeb).

1.2. Funkční požadavky na řešení peněženky

Kromě aspektů kybernetické bezpečnosti musí certifikace potvrdit i shodu s funkčními požadavky zajišťujícími konzistentní, interoperabilní a na uživatele zaměřený provoz peněženky.

Orgány pro posuzování shody (CAB) by se měly spoléhat na oficiální evropské referenční sady testů tak, jak budou definovány v rámci frameworku pro posuzování funkční shody (*Functional Conformance Assessment Framework*, FCAF). Jejich pokrytí musí být zdokumentováno ve zprávě o certifikaci.

Dále je třeba reflektovat v rámci funkčního testování národní specifika, jak budou definována a samostatně zveřejněna vlastníkem schématu, a to zejména mechanismus vydání a předání tzv. „onboarding atestace“ sloužící pro účely vydání PID. Účelem onboarding atestace je svázání uživatele, který prokazuje svojí totožnost s konkrétní jednotkou peněženky, do které se má vydat PID pro tuto osobu. Také pokrytí testů definovaných na základě národních specifik musí být zdokumentováno ve zprávě o certifikaci.

Komise aktuálně prostřednictvím FCAF zajišťuje vznik specifikací pro testování, a kde je potřeba, i potřebných nástrojů.

V době vzniku tohoto dokumentu je FCAF ve verzi 0.0.10 a neobsahuje popis testovacích scénářů pro ověření funkčních požadavků na EUDIW dle prováděcích nařízení CIR (EU) 2024/2977, CIR (EU) 2024/2979 a CIR (EU) 2024/2982.

Oblasti, které je nutné pokrýt, zahrnují:

- Správa životního cyklu credentials – vydávání, ukládání, selektivní zveřejňování, zrušení a aktualizace credentials v souladu s prováděcími předpisy, s rozlišením mezi PID, které podléhají

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

- požadavkům na vysokou úroveň záruky, a jinými přihlašovacími údaji nebo elektronickými ověřeními atributů, které podléhají funkčním požadavkům, požadavkům na interoperabilitu a příslušným požadavkům na důvěryhodné služby
- Interakce a souhlas uživatele – srozumitelné udělování souhlasů, přístupnost a výměna dat chránící soukromí v souladu s GDPR a přílohou II prováděcího aktu
 - Interoperabilita – dodržování společných API, protokolů pro výměnu a datových formátů umožňujících přeshraniční akceptaci
 - Funkční integrita a výkon – spolehlivé provádění ověřování identity, kryptografických operací souvisejících s elektronickou identifikací založenou na PID a prezentace credentials v rámci definovaných prahových hodnot latence a dostupnosti
 - Záložní a obnovovací funkce – bezpečné zálohování, obnova a migrace peněženek a credentials.
 - Testování funkční shody – provádění sad testů interoperability a chování.

Do doby zveřejnění referenčních sad testů FCAF pro funkční požadavky prováděcích nařízení CIR (EU) 2024/2977, CIR (EU) 2024/2979 a CIR (EU) 2024/2982 se uplatní tento přechodný postup: CAB stanoví rozsah funkčního testování tak, aby pokrýval oblasti uvedené výše a funkční požadavky těchto prováděcích nařízení, využije přitom nejnovější verzi FCAF dostupnou ke dni zahájení hodnocení a testovací scénáře, které FCAF dosud nepokrývá, odvodí přímo z těchto prováděcích nařízení. Použitou verzi FCAF, rozsah funkčního testování a jeho pokrytí CAB zdokumentuje v certifikační zprávě dle přílohy VI.

Rozsah funkčního testování procesů spojených s funkčními požadavky vyplývajícími z národních specifik stanoví na základě vlastním schématu zveřejněných informací v rámci řešení EUDIW CAB tak, aby pokrýval funkční požadavky uvedené v popisu způsobu práce a procesů spojených s onboarding atestací, které bude zveřejněno ze strany DIA.

Je nutno upozornit na to, že Komise i vlastník schématu definuje jen funkční testy, nebo požadavky na ně, ale nepočítá s dodávkou testovacích nástrojů ani jakékoliv testovací infrastruktury. CAB tedy budou zodpovědní za zajištění testovacích nástrojů (buď, že je získají, vyvinou nebo budou používat) a ověření, že řešení naplňuje všechny funkční požadavky dle FCAF a případně další požadavky, které jsou národními specifiky či specifiky konkrétní architektury řešení peněženky.

Pro testy mohou být použity i nástroje dodavatelů řešení za předpokladu, že je CAB umožněn plný přístup k těmto nástrojům a logům, které tyto nástroje poskytují. CAB je finálně zodpovědný za to, že tyto nástroje provádějí testy v požadovaném rozsahu a kvalitě.

V rámci dalších aktualizací bude upřesněno rovněž funkční testování v závislosti na vývoji Functional Conformance Assessment Frameworku a definici funkčních požadavků vyplývajících z národních specifik, zveřejněných vlastním schématu.

1.3. Subdodavatelé

Certifikační subjekty mohou podle CIR EU 2024/2981 zadat hodnotící činnosti třetím stranám. Tyto třetí strany podle článku 10(1) CIR EU 2024/2981 „musí podle potřeby a vhodnosti pro prováděné činnosti splňovat požadavky harmonizovaných norem, jako je EN ISO/IEC 17025:2017 pro zkoušení, EN ISO/IEC

pro audit a EN ISO/IEC 17029:2019 pro validaci a ověřování“.

Využití třetích stran je na zvážení certifikačního subjektu a bude nutné, zejména pokud certifikační subjekt nedisponuje přílišnými kapacitami.

1.4. Rejstřík referenčních dokumentů

Normy, technické specifikace a další referenční dokumenty, na které schéma EUDIW-CZ a jeho přílohy odkazují, se použijí ve vydání uvedeném v následujícím rejstříku. Není-li v textu schématu u odkazu vydání uvedeno, rozumí se vydání dle tohoto rejstříku. Právní předpisy se použijí v platném znění a v rejstříku se neuvádějí.

Změna vydání v rejstříku je změnou schématu. Řídí se článkem 32 hlavního textu, včetně stanovení časového harmonogramu přechodu s ohledem na probíhající a plánované činnosti posuzování shody, a její dopad na platné certifikáty se posuzuje dle přílohy II.

Referenční dokument	Závazné vydání	Poznámka
ETSI EN 319 401	v3.2.1	Vydání, proti kterému je psána příloha X a které uvádí příloha IX.
ETSI EN 319 403-1	V2.3.1 (2020-06)	Dle článku hlavního textu o akreditaci certifikačních orgánů.
ETSI TS 119 461	V2.1.1 (2025-02)	Použije se dle CIR (EU) 2026/798.
EN 17640 (FitCEM)	EN 17640:2022	CIR (EU) 2024/2981 na normu odkazuje označením EN 17640:2018.
EN ISO/IEC 15408 (Common Criteria)	EN ISO/IEC 15408-3:2022 pro posouzení zranitelností	Dle přílohy IV CIR (EU) 2024/2981.
EN ISO/IEC 27001	EN ISO/IEC 27001:2022	Certifikáty dle vydání 2013 pouze za podmínek přílohy IX.
ISO/IEC 27002	ISO/IEC 27002:2022	
EN ISO/IEC 17065	EN ISO/IEC 17065:2012	
EN ISO/IEC 17067	EN ISO/IEC 17067:2013	
EN ISO/IEC 17025	EN ISO/IEC 17025:2017	Dle čl. 10 odst. 1 CIR (EU) 2024/2981.
EN ISO/IEC 17020	EN ISO/IEC 17020:2012	Dle čl. 10 odst. 1 CIR (EU) 2024/2981.
EN ISO/IEC 17021-1	EN ISO/IEC 17021-1:2015	Dle čl. 10 odst. 1 CIR (EU) 2024/2981.

Referenční dokument	Závazné vydání	Poznámka
EN ISO/IEC 17029	EN ISO/IEC 17029:2019	Dle čl. 10 odst. 1 CIR (EU) 2024/2981.
IAF MD 25	IAF MD 25:2023	
ETSI EN 319 411-1, EN 419 211, EN 419 221-5, EN 419 241-2, CEN TS 18026, TS 18099, EN ISO/IEC 30111, EN ISO/IEC 29147, ISO/IEC 18045, ISO/IEC 30107-3, ISO/IEC 19795-1, ISO/IEC 19989-3, ICAO Doc 9303	Vydání platné k datu podání žádosti o certifikaci	Schéma u těchto dokumentů dosud vydání neurčuje. Vlastník schématu je doplní při nejbližší aktualizaci rejstříku.
ARF, ECCG Agreed Cryptographic Mechanisms, OWASP MAS, MASWE a ASVS, FitCEM Wallet Instance Protection Profile, FCAF, národní specifika	Verze účinná k datu podání žádosti o certifikaci	

Příloha Ia Rozsah certifikace: Poskytování peněženky

Aby mohla být služba IKT používaná k poskytování řešení peněženek EUDI a systém elektronické identifikace, v jehož rámci jsou poskytovány, certifikovány v rámci tohoto schématu, musí být v souladu s čl. 5c odst. 4 a 5c odst. 5 nařízení eIDAS a specificky musí splňovat požadavky na prostředek elektronické identifikace pro systém elektronické identifikace s úrovní zabezpečení „vysoká“.

Kromě komponent uvedených v Příloze I služba IKT musí zahrnovat alespoň následující komponenty, u kterých musí být prokázána shoda s uvedenými požadavky, aby byla IKT služba certifikována v rámci tohoto schématu:

Komponenta	Popis	Platné požadavky
Instance peněženky	Aplikace, která definuje uživatelské rozhraní peněženky. Může existovat několik variant instance peněženky různých typů (webová, mobilní, pro PC atd.) a zaměřených na různé architektury.	Referenční: - CIR (EU) 2015/1502, eIDAS úroveň „vysoká“ (týká se jen částí zajišťujících elektronickou identifikaci) - Příloha X Další: - FitCEM Wallet instance Protection Profile
WSCA	Bezpečná kryptografická aplikace peněženky - aplikace, která spravuje kritická aktiva prostřednictvím propojení s kryptografickými a nekryptografickými funkcemi poskytovanými bezpečným kryptografickým prostředkem peněženky a jejich využívání	Referenční: - CIR (EU) 2015/1502, eIDAS úroveň „vysoká“ - CC EAL4+ a AVA_VAN.5 nebo AVA_VAN.3 Příloha X Další: - FitCEM WSCA Protection Profile
Služba jednotky peněženky	Služba hostovaná na systému IKT poskytovatele peněženky, který podporuje jednotlivé jednotky peněženky.	Referenční: - CIR (EU) 2015/1502, eIDAS úroveň „vysoká“ (týká se jen částí zajišťujících elektronickou identifikaci) - Příloha X
Proces nahrávání a aktualizace	Proces(y) provozovaný(é) poskytovatelem IKT služeb pro načítání a aktualizaci instance peněženky a WSCA.	Referenční: - ETSI EN 319 401 - Příloha X
Služba poskytování a správy peněženek	IKT služba provozovaná poskytovatelem IKT služeb pro zřízení peněženky EUDI a pro její správu po celou dobu jejího životního cyklu.	Referenční: - Zákon 250/2017 Sb. pro oblast elektronické identifikace – zejména §22(2) (týká se jen částí EUDIW) - CIR (EU) 2015/1502, eIDAS úroveň „vysoká“ (týká se jen částí zajišťujících elektronickou identifikaci) - ETSI EN 319 401 - Příloha X
Ověřování validity spoléhajících se stran	IKT služba provozovaná poskytovatelem IKT služeb pro ověřování pravosti a platnosti totožnosti spoléhajících se stran registrovaných v souladu s článkem 5b eIDAS.	Referenční: Příloha X

Komponenta	Popis	Platné požadavky
Ověřování validity peněženek	IKT služba provozovaná poskytovatelem IKT služeb pro ověřování pravosti a platnosti evropských peněženek digitální identity.	Referenční: Příloha X

Služba IKT zahrnuje následující komponentu, u které musí být prokázána shoda s uvedenými požadavky:

Komponenta	Popis	Platné požadavky
WSCD	Bezpečný kryptografický prostředek peněženky - prostředek odolný proti neoprávněné manipulaci, který poskytuje prostředí propojené s bezpečnou kryptografickou aplikací peněženky a používaný touto aplikací k ochraně kritických aktiv a poskytování kryptografických funkcí pro bezpečné provádění kritických operací	Referenční: - CIR (EU) 2015/1502, eIDAS úroveň „vysoká“ - Relevantní certifikace dle CC nebo EUCC (např. EN 419 211 pro lokální WSCD na čipové kartě, EN 419 221-5 pro vzdálené WSCD) – viz příloha IX.

Pokud se WSCA z IKT služby spoléhá na WSCD, který není součástí IKT služby, musí poskytovatel IKT služby definovat předpoklady o tomto WSCD, které jsou dostatečné pro to, aby WSCA splnilo všechny příslušné požadavky, a platnost tohoto předpokladu musí být prokázána.

Součástí certifikace “Poskytování peněženky” je provedení funkčních testů dle kap. 1.2.

Příloha Ib Rozsah certifikace: Poskytování PID

Aby mohla být IKT služba používaná k poskytování osobních identifikačních údajů (PID) za účelem poskytování systému elektronické identifikace, v jehož rámci jsou poskytovány evropské peněženky digitální identity, certifikována v rámci tohoto schématu, musí být v souladu s čl. 5c odst. 4 a 5c odst. 5 nařízení eIDAS, prováděcím nařízením CIR (EU) 2024/2977 a musí zejména splňovat příslušné požadavky na prostředek elektronické identifikace pro systém elektronické identifikace na úrovni záruky „vysoká“.

POZNÁMKA: „Příslušné požadavky“ odkazují na příslušné požadavky nařízení CIR (EU) 2015/1502, jelikož poskytovatel PID je zodpovědný pouze za několik komponent prostředku elektronické identifikace.

Kromě komponent uvedených v Příloze I služba IKT musí zahrnovat alespoň následující komponenty, u kterých musí být prokázána shoda s uvedenými požadavky, aby byla IKT služba certifikována v rámci tohoto schématu:

Komponenta	Popis	Platné požadavky
Registrace a správa uživatelů	Registrace a správa uživatelů s ověřením totožnosti: - Vzdáleně - Za fyzické přítomnosti	Referenční: - CIR (EU) 2015/1502, eIDAS úroveň „vysoká“ - Příloha X Další: - Atestace dle zákona 250/2017 Sb. pro oblast elektronické identifikace úrovně „značná“ a „vysoká“ - CIR (EU) 2026/798 - ETSI TS 119 461 V2.1.1 - TS 18099
Poskytování a správa PID	IKT služba provozovaná poskytovatelem IKT služeb pro poskytování identifikačních údajů osob a pro jejich správu po celou dobu jejího životního cyklu.	Referenční: - ETSI EN 319 401 - Atestace dle zákona 250/2017 Sb. pro oblast elektronické identifikace - CIR (EU) 2015/1502, eIDAS úroveň „vysoká“ - CIR (EU) 2024/2977 - Příloha X

Ib.1 Ověřování totožnosti

Prokazování totožnosti může být:

1. Za fyzické přítomnosti žadatele.

2. Vzdáleně za využití prostředku

elektronické identifikace dle čl. 5a odst. 24 nařízení (EU) č. 910/2014, a to:

- a. Pomocí prostředku elektronické identifikace a systému elektronické identifikace, které jsou podle zákona 250/2017 Sb. akreditovány pro úroveň „vysoká“. V tomto případě se dle CIR (EU) 2026/798 aplikuje ETSI TS 119 461 V2.1.1 (2025-02) kap. 9.2.4 Use case for identity proofing by authentication using eID means.
- b. Pomocí prostředku elektronické identifikace a systému elektronické identifikace je podle zákona 250/2017 Sb. akreditován pro úroveň „značná“ ve „spojení s dalšími postupy vzdáleného zapojení, které společně splňují požadavky vysoké úrovně záruky“. V tomto případě se dle CIR (EU) 2026/798 aplikuje ETSI TS 119 461 V2.1.1 (2025-02) kap. 9.5 Use cases for additional identity proofing to enhance an identity proven by use of an eID from Baseline LoIP to Extended LoIP s dodatečnými požadavky uvedenými v příloze CIR (EU) 2026/798. Konkrétně bude v České republice využita možnost ověření totožnosti prostřednictvím dokladu totožnosti v případě vzdáleného automatického ověření bez dohledu, tj. v souladu s odstavcem 9.5.2 Use case for enhancing identity proofing to Extended LoIP by a full identity proofing using an identity document.

Při ověřování totožnosti prostřednictvím dokladu totožnosti v případě vzdáleného automatického ověření bez dohledu musí být systém pro pořizování snímku žadatele hodnocen vůči „biometric injection attack“ nejpozději do konce roku 2026 (viz ETSI 119 461 V2.1.1 požadavek BIN-8.4.2-04C), hodnocení musí být provedeno akreditovanou laboratoří podle TS 18099 (viz ETSI 119 461 V2.1.1 požadavek BIN-8.4.2-04D).

Příloha Ic Rozsah certifikace: Zastřešující certifikát

Certifikační orgán:

1. Ověří, že bylo řádně a úplně provedeno hodnocení dle Příloh Ia a Ib.
2. Jelikož hodnocení dle Přílohy Ia a hodnocení dle Přílohy Ib mohlo proběhnout v různém čase a případně i různými orgány, tak musí ověřit, že proběhly funkční testy dle I.2, které ověří interoperabilitu a funkčnost všech vzájemných integrací.