

29 Příloha XVI: Použité termíny a zkratky

Termín	Význam
přístupová práva	oprávnění pro subjekt k přístupu k určitému objektu pro konkrétní typ operace [ZDROJ: Z ISO/IEC 2382:2015, 2126298]
akreditace	osvědčení třetí strany týkající se subjektu posuzování shody, které formálně prokazuje jeho způsobilost, nestrannost a důsledné fungování při provádění specifických činností posuzování shody [ZDROJ: Z ISO/IEC 17000:2020(en), 7.7]
akreditační orgán	orgán posuzování shody, který provádí akreditaci Poznámka 1: Pravomoc akreditačního orgánu stanovuje vláda. [ZDROJ: Z ISO/IEC 17000:2020(en), 2.6]
dokument žádosti	dokument, který žadatel poskytne CAB při žádosti o certifikaci
aktivum	cokoli, co má pro organizaci hodnotu Poznámka 1 k heslu: V kontextu informační bezpečnosti lze rozlišit dva druhy aktiv: — primární aktiva: — informace; — obchodní procesy a činnosti; — podpůrná aktiva (na kterých závisí primární aktiva) všech typů, například: — hardware; — software; — síť; — personál;

	— pracoviště; — struktura organizace. [ZDROJ: Z ISO/IEC 27002:2022(en), 3.1.2]
záruka	důvody pro oprávněnou důvěru, že produkt, služba nebo proces splňuje stanovené požadavky [ZDROJE: Inspirováno z ISO/IEC 15408-1:3(2009).1.4 a z ISO/IEC/IEEE 15026-1(2019):3.1]
informace o záruce	informace včetně tvrzení o systému, důkazů podporujících toto tvrzení, argumentů ukazujících, jak důkazy podporují dosažení daného tvrzení, a kontextu pro tyto položky [ZDROJ: Z ISO/IEC/IEEE 15026-1(2019):3.4]
úroveň záruky	[CSA] základ důvěry, že produkt IKT, služba IKT nebo proces IKT splňuje bezpečnostní požadavky konkrétního evropského systému certifikace kybernetické bezpečnosti, udává úroveň, na které byl produkt IKT, služba IKT nebo proces IKT hodnocen, ale jako takový neměří bezpečnost daného produktu IKT, služby IKT nebo procesu IKT Poznámka 1: Schéma často definuje diskrétní úrovně záruky a každá taková diskrétní úroveň definuje stupeň záruky ve splnění požadavků produktem IKT, službou IKT nebo procesem IKT. [ZDROJ: Z (EU) 2019/881, 2.21]
	[EUDIF] základ pro definovanou úroveň důvěry v deklarovanou nebo uplatňovanou identitu osoby, charakterizovaný s odkazem na související technické specifikace, normy a postupy, včetně technických kontrol, jejichž účelem je zmírnit riziko zneužití nebo změny identity na definované úrovni.
útok	úspěšný nebo neúspěšný neoprávněný pokus o zničení, změnu, znefunkčnění, získání přístupu k aktivu nebo jakýkoli pokus o odhalení, krádež nebo neoprávněné použití aktiva. [ZDROJ: Z ISO/IEC 27002:2022, 3.1.3]

atestace	vydání prohlášení na základě rozhodnutí, že bylo prokázáno splnění stanovených požadavků Poznámka 1: Výsledné prohlášení (...) má vyjádřit ujištění, že stanovené požadavky byly splněny. Takové ujištění samo o sobě neposkytuje smluvní ani jiné právní záruky. Poznámka 2: Ověření první stranou a ověření třetí stranou se rozlišují pojmy prohlášení, certifikace a akreditace, ale neexistuje žádný odpovídající termín použitelný pro ověřování druhou stranou. [ZDROJ: Z ISO/IEC 17000:2020(en), 7.3]
atribut	vlastnost, kvalita, právo nebo povolení fyzické nebo právnické osoby nebo předmětu [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(43)]
audit	proces pro získání relevantních informací o předmětu posouzení shody a jeho objektivní hodnocení za účelem určení rozsahu, v jakém jsou splněny stanovené požadavky. Poznámka 1: Stanovené požadavky jsou definovány před provedením auditu, aby bylo možné získat relevantní informace. Poznámka 2: Příklady předmětů auditu jsou systémy managementu, procesy, produkty a služby. Poznámka 3: Pro účely akreditace se proces auditu nazývá „posouzení“. [ZDROJ: Z ISO 17000:2020(en), 6.4]
autentický zdroj	úložiště nebo systém, za který odpovídá subjekt veřejného sektoru nebo soukromý subjekt, který obsahuje a poskytuje atributy o fyzické nebo právnické osobě nebo objektu a který je považován za primární zdroj těchto informací nebo je uznáván za autentický v souladu s právem Unie nebo vnitrostátním právem, včetně správní praxe [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(47)]
ověřování, též autentizace	[kybernetická bezpečnost] zajištění správnosti deklarované charakteristiky subjektu [ZDROJ: Z ISO/IEC 27022:2022, 3.1.4] [identita] elektronický proces, který umožňuje potvrzení elektronické identifikace fyzické nebo právnické osoby nebo potvrzení původu a integrity údajů v elektronické podobě [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(5)]
autenticita	vlastnost, že entita je tím, za co se vydává [ZDROJ: Z ISO/IEC 27000:2018(en), 3.6]

kontinuita činností	schopnost organizace pokračovat v dodávkách produktů a služeb v přijatelných časových rámcích s předem definovanou kapacitou během přerušení provozu [ZDROJ: Z ISO 22301:2019(en), 2019, 3.3]
plán kontinuity činností	zdokumentované informace, které organizaci pomohou reagovat na narušení a znovu zahájit, zotavit a obnovit dodávky produktů a služeb v souladu s jejími cíli kontinuity činností [ZDROJ: Z ISO 22301:2019(en), 2019, 3.4]
certifikace	osvědčení třetí strany týkající se předmětu posuzování shody, s výjimkou akreditace [ZDROJ: Z ISO/IEC 17000:2020(en), 7.6]
certifikační orgán	subjekt posuzování shody třetí strany, který provádí činnosti přezkumu a certifikace.
certifikační zpráva	dokument, který je součástí certifikátu a poskytuje jednoduchou prezentaci služby a shrnutí činností posuzování shody
certifikační schéma	systém posuzování shody, který zahrnuje certifikační činnost Poznámka 1: V certifikačním schématu vede úspěšné posouzení k vydání certifikátu.
klient	organizace, jejíž služba je auditována pro účely certifikace Poznámka 1 k heslu: „systém managementu“ byl nahrazen výrazem „služba“ [ZDROJ: Adaptováno z ISO/IEC 17021-1:2015(en), 3.5]
stížnost	vyjádření nespokojenosti jakékoli osoby nebo organizace vůči CAB nebo akreditačnímu orgánu nebo NCCA CAB, týkající se činnosti daného CAB, kde se očekává odpověď [ZDROJ: Adaptováno z ISO/IEC 17000:2020, 8.7]
dodržování	shoda v kontextu pravidel a požadavků definovaných v certifikačním schématu, které se vztahují na poskytovatele certifikovaného produktu, služby nebo procesu Poznámka 1 k heslu: Toto je zpřesnění normy ISO 19011, která definuje dodržování jako shodu v kontextu zákonného požadavku nebo regulačního požadavku. V tomto případě je dodržování shodou v kontextu daného schématu.

shoda	splnění požadavku Poznámka 1: Pokud se používá v opozici k termínu „dodržování“, vztahuje se termín „shoda“ k požadavkům týkajícím se předmětu posuzování shody, nikoli k požadavkům týkajícím se certifikačního systému. [ZDROJ: Z normy ISO/IEC 19011:2018(en), 3.20]
posouzení shody	prokázání, že jsou splněny stanovené požadavky
orgán posuzování shody	orgán, který provádí služby posuzování shody, s výjimkou akreditace [ZDROJ: Z ISO/IEC 17000:2020(en), 4.6]
systém posuzování shody	soubor pravidel a postupů, který popisuje předměty posuzování shody, identifikuje specifikované požadavky a poskytuje metodiku pro provádění posuzování shody [ZDROJ: Z ISO/IEC 17000:2020(en), 4.9]
pověření	reprezentace identity Poznámka 1: Pověření se obvykle vytváří za účelem usnadnění ověřování dat identifikačních informací v identitě, kterou reprezentuje. PŘÍKLAD: Pověřením může být uživatelské jméno, uživatelské jméno s heslem, PIN, čipová karta, token, otisk prstu, cestovní pas atd. [ZDROJ: Z ISO/IEC 24760-1:2011, 3.3.5]
kritická aktiva	aktiva v rámci jednotky peněženky nebo ve vztahu k ní, která jsou tak mimořádně důležitá, že ohrožení jejich dostupnosti, důvěrnosti nebo integrity by mělo velmi vážný a oslabující účinek na schopnost spoléhat se na jednotku peněženky [ZDROJ: Z CIR (EU) 2024/2981, článek 2(11)]
kybernetická bezpečnost	činnosti nezbytné k ochraně sítí a informačních systémů, uživatelů těchto systémů a dalších osob postižených kybernetickými hrozbami [ZDROJ: Z nařízení (EU) 2019/881, článek 2(1)]
rozhodnutí	závěr, založený na výsledcích přezkoumání, zda bylo či nebylo prokázáno splnění stanovených požadavků [ZDROJ: Z ISO/IEC 17000:2020(en), 7.2]

dokument	zaznamenaná informace nebo hmotný objekt, který lze považovat za jednotku [ZDROJ: Z ISO 5127:2001, 1.2.02]
EUDIF	Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zavedení evropského rámce digitální identity
elektronické potvrzení atributů - EAA	potvrzení v elektronické podobě, které umožňuje autentizaci atributů POZNÁMKA: V přílohách schématu se ve stejném významu používá též označení „atestace atributů“. [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(44)]
elektronická identifikace - eID	proces používání osobních identifikačních údajů v elektronické podobě, které jedinečně reprezentují buď fyzickou, nebo právnickou osobu, nebo fyzickou osobu zastupující jinou fyzickou nebo právnickou osobu [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(1)]
prostředky elektronické identifikace - prostředky eID	hmotná a/nebo nehmotná jednotka obsahující osobní identifikační údaje, která se používá k ověřování v rámci online služby nebo případně v rámci offline služby [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(2)]
Evropská skupina pro certifikaci kybernetické bezpečnosti - ECCG	Skupina složená ze zástupců národních orgánů pro certifikaci kybernetické bezpečnosti nebo jiných příslušných národních orgánů. [ZDROJ: Adaptováno z aktu o kybernetické bezpečnosti, článek 62]
Evropská peněženka digitální identity – EUDIW - peněženka	prostředek elektronické identifikace, který uživateli umožňuje bezpečně ukládat, spravovat a ověřovat osobní identifikační údaje a elektronická potvrzení atributů za účelem jejich poskytování spoléhajícím se stranám a dalším uživatelům evropských peněženek digitální identity a podepisovat je pomocí kvalifikovaných elektronických podpisů nebo pečeti kvalifikovanými elektronickými pečeti [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(42)]
značka důvěry EU pro peněženku digitální identity	Ověřitelné, jednoduché a rozpoznatelné označení, které jasným způsobem sděluje, že evropská peněženka digitální identity byla poskytnuta v souladu s nařízením eIDAS [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(50)]
hodnocení	kombinace výběrových a určovacích funkcí činností posuzování shody [ZDROJ: Z ISO/IEC 17065:2012(en), 3.3]

úroveň hodnocení	kombinace složek záruky v rámci metodiky hodnocení, která odpovídá úrovni záruky a vhodné úrovni hloubky a důslednosti, odpovídající kategorii bezpečnostních problémů [ZDROJ: Z EC 881/2019, 52.8]
hodnotící zpráva	dokument vypracovaný CAB, který popisuje hodnotící činnosti a jejich výsledky, včetně auditu a analýzy závislostí
technická zpráva o hodnocení - ETR	[CC] dokumentace celkového verdiktu a jeho odůvodnění, vypracovaná hodnotitelem a předložená hodnotícímu orgánu [ZDROJ: Z ISO 15408-1: 2022, 3.43]
proces IKT	soubor činností prováděných za účelem návrhu, vývoje, dodání nebo údržby produktu nebo služby IKT Poznámka 1 k heslu: Tento termín se používá, pokud má být proces předmětem certifikace kybernetické bezpečnosti. Termín „proces“ je obecnější a měl by se používat v jiných situacích. [ZDROJ: Z CSA, článek 2(14)]
produkt IKT	prvek nebo skupina prvků sítě nebo informačního systému Poznámka 1: V definici certifikačních schémat se použití pojmu „produkt IKT“ řídí touto definicí z normy EC 881-2019 a bude se většinou používat k označení certifikačních schémat a produktů certifikovaných pomocí těchto schémat. Je podmnožinou obecnějšího pojmu produkt, jehož definice pochází z normy ISO 9000. [ZDROJ: Z CSA, článek 2(12)]
služba IKT	služba spočívající zcela nebo převážně v přenosu, ukládání, vyhledávání nebo zpracování informací prostřednictvím sítí a informačních systémů Poznámka 1: V definici certifikačních schémat se použití pojmu „služba IKT“ řídí touto definicí z normy EC 881-2019 a bude se většinou používat k označení certifikačních schémat a produktů certifikovaných pomocí těchto schémat. Pro obecnější použití je vhodnější používat termín „služba“. [ZDROJ: Z CSA, článek 2(13)]
systém řízení bezpečnosti informací - ISMS	součást celkového systému managementu, založená na přístupu k obchodním rizikům, používaná k zavedení, implementaci, provozu, monitorování, kontrole, údržbě a zlepšování bezpečnosti informací [ZDROJ: Z ISO/TS 12812-2:2017, 3.11]

inspekce	[CASCO] přezkoumání předmětu posuzování shody a určení jeho shody s podrobnými požadavky nebo na základě odborného úsudku s obecnými požadavky. Poznámka 1: Přezkoumání může zahrnovat přímá nebo nepřímá pozorování, která mohou zahrnovat měření nebo výstupy z přístrojů. Poznámka 2: Programy posuzování shody nebo smlouvy mohou specifikovat inspekci pouze jako přezkoumání. [ZDROJ: Z ISO/IEC 17000:2020, 6.3]
	[IAASB] činnost zahrnující zkoumání záznamů nebo dokumentů, ať už interních nebo externích, v papírové podobě, elektronické podobě nebo na jiných médiích, nebo fyzické zkoumání důkazů [ZDROJ: Z Příručky IAASB pro mezinárodní řízení kvality, audit, prověrku, další Prohlášení o ověřování a souvisejících službách, vydání 2017, Slovník pojmů]
interní audit	audit prováděný samotnou organizací nebo jejím jménem pro účely přezkoumání managementem a další interní účely, který může tvořit základ pro vlastní prohlášení organizace o shodě Poznámka 1: V mnoha případech, zejména v menších organizacích, lze nezávislost prokázat tím, že auditor nenese odpovědnost za auditovanou činnost. [ZDROJ: Z ISO 22300:2021(en), 3.1.134]
životní cyklus	fáze zahrnuté v řízení aktiva Poznámka 1: Názvy a počet fází a činnosti v rámci každé fáze se obvykle liší v různých odvětvích a jsou určeny organizací. [ZDROJ: Z ISO 55000:2014(en), 3.2.3]
významná neshoda – velká neshoda	neshoda, která ovlivňuje schopnost systému managementu dosáhnout zamýšlených výsledků Poznámka 1: Neshody lze klasifikovat jako významné za následujících okolností: - pokud existují závažné pochybnosti o tom, že je zavedeno účinné řízení procesů nebo že produkty či služby splňují stanovené požadavky; - řada méně významných neshod spojených se stejným požadavkem nebo problémem by mohla prokázat systémové selhání, a proto by mohla představovat významnou neshodu. [ZDROJ: Adaptováno z ISO/IEC 17021-1:2015(en), 3.12]

méně významná neshoda – malá neshoda	neshoda, která neovlivňuje schopnost systému managementu dosáhnout zamýšlených výsledků [ZDROJ: Adaptováno z ISO/IEC 17021-1:2015(en), 3.12]
monitorování	určení stavu systému, procesu nebo činnosti Poznámka 1: Pro určení stavu může být nutné provést kontrolu, dohled nebo kritické pozorování.
národní akreditační orgán - NAB	jediný orgán v členském státě, který provádí akreditaci s oprávněním odvozeným od státu [ZDROJ: Z EC765/2008:2.1]
nedodržování	neshoda v kontextu pravidel a požadavků definovaných v certifikačním schématu Poznámka 1: Toto je zpřesnění normy ISO 19011, která definuje nedodržování jako neshodu v kontextu zákonného požadavku nebo regulačního požadavku. Dodržování je zde shoda v kontextu daného schématu. [ZDROJ: Inspirováno z ISO 19011:2018(en), 3.7]
neshoda	nesplnění požadavku Poznámka 1: Pokud se používá v opozici k nedodržování, vztahuje se neshoda k požadavkům týkajícím se předmětu posuzování shody, nikoli k požadavkům týkajícím se certifikačního systému. [ZDROJ: Z dodatku ISO: 3.19]
outsourcing	pořízení služeb (s produkty nebo bez nich) na podporu obchodní funkce pro provádění činností s využitím zdrojů dodavatele, nikoli zdrojů nabyvatele Poznámka 1: Pro účely tohoto dokumentu se pojmy „outsourcing“ a „subdodávky“ považují za synonyma. [ZDROJ: Z ISO/IEC 27036-1:2015, 3.6] [ZDROJ Poznámka 1: Z ISO/IEC 17065:2012(en), § 6.2.2.1]
vzájemné hodnocení	posouzení orgánu podle specifických požadavků zástupci jiných orgánů v dohodové skupině nebo kandidáty na členy do dohodové skupiny [ZDROJ: Z ISO/IEC 17000:2020(en), 4.5]

osobní identifikační údaje - PID	soubor údajů vydaných v souladu s právem Unie nebo vnitrostátním právem a umožňujících určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující jinou fyzickou či právnickou osobu [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(3)]
politika	záměry a směr organizace, formálně vyjádřené jejím vrcholovým vedením [ZDROJ: Z ISO/IEC 27000:2018(en), 3.53]
poskytovatel osobních identifikačních údajů - poskytovatel PID	fyzická nebo právnická osoba odpovědná za vydávání a odvolávání osobních identifikačních údajů a za zajištění toho, aby osobní identifikační údaje uživatele byly kryptograficky svázané s jednotkou peněženky [ZDROJ: Z CIR (EU) 2024/2977, článek 2(4)]
kvalifikované elektronické potvrzení atributů	elektronické potvrzení atributů, které vydává kvalifikovaný poskytovatel služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze V [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(45)]
kvalifikovaný elektronický podpis	zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(12)]
spoléhající strana	fyzická nebo právnická osoba, která se spoléhá na elektronickou identifikaci nebo službu vytvářející důvěru [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(6)]
zbytkové riziko	riziko zbývající po ošetření rizik Poznámka 1: Zbytkové riziko může obsahovat neidentifikované riziko. Poznámka 2: Zbytkové riziko může být také známé jako „zachované riziko“. [ZDROJ: Z ISO Guide 73:2009, 3.8.1.6]
zpráva o přezkoumání	dokument vypracovaný CAB po provedení kontroly hodnocení provedeného auditorským týmem
riziko	působení nejistoty na cíle Poznámka 1: Působení je odchylka od očekávání – pozitivní a/nebo negativní. Poznámka 2: Cíle mohou mít různé aspekty (například finanční, zdravotní a bezpečnostní a environmentální cíle) a mohou se vztahovat na různé úrovně (například strategickou, celoorganizační, projektovou, produktovou a procesní).

	Poznámka 3: Riziko je často charakterizováno odkazem na potenciální události a důsledky nebo jejich kombinaci. Poznámka 4: Riziko je často vyjádřeno jako kombinace důsledků události (včetně změn okolností) a související pravděpodobnosti jejího výskytu. Poznámka 5: Nejistota je stav, byť i částečný, nedostatku informací týkajících se události, jejího důsledku nebo pravděpodobnosti, pochopení nebo znalosti o ní. [ZDROJ: Z ISO 31073:2022, 3.1.1]
analýza rizik	proces pro pochopení povahy rizika a určení jeho úrovně Poznámka 1: Analýza rizik poskytuje základ pro hodnocení rizik a rozhodnutí o nakládání s nimi. Poznámka 2: Analýza rizik zahrnuje odhad rizik. [ZDROJ: Z ISO 31073:2022(en), 3.3.1]
posouzení rizik	celkový proces identifikace rizik, analýzy rizik a hodnocení rizik [ZDROJ: Z ISO 31073:2022, 3.3.8]
hodnocení rizik	proces porovnávání výsledků analýzy rizik s kritérii rizika za účelem určení, zda je riziko a/nebo jeho rozsah přijatelný nebo tolerovatelný Poznámka 1: Hodnocení rizik pomáhá při rozhodování o jejich ošetření. [ZDROJ: Z ISO 31073:2022(en), 3.3.2]
vlastník rizika	osoba nebo subjekt s odpovědností a pravomocí řídit riziko [ZDROJ: Z ISO 31073:2022(en), 3.3.14]
registr rizik	záznam informací o zjištěných rizicích, které jsou důležité pro proces certifikace [ZDROJ: Z CIR (EU) 2024/2981, článek 2(7)]
role	soubor aktivit, které slouží společnému účelu [ZDROJ: Z ISO/IEC 22123-1:2023(en), 3.3.10]
vlastník schématu	organizace, která je odpovědná za vývoj a údržbu certifikačního schématu POZNÁMKA 1: Vlastníkem schématu EUDIW-CZ je Digitální a informační agentura (DIA). POZNÁMKA 2: České znění CIR (EU) 2024/2981 používá ve stejném významu termíny „vlastník systému“ a „systém certifikace“. [ZDROJ: Z CIR (EU) 2024/2981, článek 2(2), poznámky doplněny]

rozsah certifikace	Identifikace: — služby (služeb), pro kterou (které) je certifikace udělena, — příslušného certifikačního schématu a možností schématu a — normy (norem) a jiného normativního dokumentu (dokumentů), včetně data jejich vydání, s nimiž se má za to, že služba (služby) splňují Poznámka: Definice byla upravena tak, aby zahrnovala „možnosti schématu“, které mohou v kontextu EUCS zahrnovat zejména vybranou úroveň hodnocení a profily rozšíření. [ZDROJ: Adaptováno z ISO/IEC 17065:2012, 3.10]
zajištění bezpečnosti	důvody pro oprávněnou důvěru, že tvrzení o splnění bezpečnostních cílů bylo nebo bude dosaženo [ZDROJ: Z ISO/IEC/IEEE 15026-1(2019):3.4]
dodavatel	organizace nebo jednotlivec, který uzavírá s nabyvatelem smlouvu o dodávce produktu nebo služby Poznámka 1: Dalšími běžně používanými termíny pro dodavatele jsou zhotovitel, výrobce nebo prodejce. Poznámka 2: Termín „poskytovatel služeb“ se v tomto schématu obvykle používá pro dodavatele služeb. Poznámka 3: Na rozdíl od „poskytovatele služeb“ se termín „dodavatel“ vztahuje na dodavatele produktů. [ZDROJ: Adaptováno z ISO/IEC 27036:1-2014, 3.9]
dohled	systematické opakování činností posuzování shody jako základ pro udržení platnosti prohlášení o shodě [ZDROJ: Z ISO/IEC 17000:2020(en), 8.1]
pozastavení	dočasné omezení prohlášení o shodě orgánem, který prohlášení vydal, pro celý nebo část stanoveného rozsahu certifikace [ZDROJ: Z ISO/IEC 17000:2020, 8.2]
třetí strana	osoba nebo orgán, který je nezávislý na osobě nebo organizaci, která poskytuje předmět posouzení shody, a na zájmech uživatelů v tomto předmětu [ZDROJ: Z ISO/IEC 17000:2020(en), 2.2]

hrozba	potenciální příčina nežádoucího incidentu, který může vést k poškození systému nebo organizace [ZDROJ: Z ISO/IEC 27000:2018, 3.74]
uživatel	fyzická nebo právnická osoba, nebo fyzická osoba zastupující jinou fyzickou nebo právnickou osobu, která využívá služby vytvářející důvěru nebo prostředky elektronické identifikace poskytované v souladu s tímto nařízením [ZDROJ: Nařízení (EU) 2024/1183, článek 3(5a)]
validace	[posouzení shody] potvrzení věrohodnosti pro konkrétní zamýšlené použití nebo aplikaci prostřednictvím poskytnutí objektivních důkazů o splnění specifikovaných požadavků (5.1). Poznámka 1: Validaci lze použít na tvrzení k potvrzení informací uvedených v tvrzení týkajících se zamýšleného budoucího použití. [ZDROJ: Z ISO/IEC 17000:2020, 6.5] proces ověřování a potvrzování platnosti dat v elektronické podobě v souladu s tímto nařízením. [ZDROJ: Z nařízení (EU) 2024/1183, článek 3(41)].
verifikace - ověření	potvrzení pravdivosti poskytnutím objektivních důkazů o splnění stanovených požadavků (5.1)
zranitelnost	slabina aktiva nebo kontroly, kterou může zneužít jedna nebo více hrozeb [ZDROJ: Z ISO/IEC 27000:2018(en), 2018, 3.77]
instance peněženky	aplikace nainstalovaná a nakonfigurovaná na zařízení nebo v prostředí uživatele peněženky, která je součástí jednotky peněženky a kterou uživatel peněženky používá k interakci s jednotkou peněženky POZNÁMKA: instance peněženky je instancí jedné nebo více aplikací uživatelského rozhraní peněženky, případně rozdělených mezi zařízení uživatele peněženky a vzdálené prostředí poskytovatele peněženky [ZDROJ: Z CIR (EU) 2024/2981 (EUDIF IA), článek 2(5), poznámka přidána]
poskytovatel peněženky	fyzická nebo právnická osoba, která poskytuje řešení peněženky POZNÁMKA: Vzhledem ke složené povaze řešení peněženky poskytovatel peněženky vyrábí nebo pořizuje hardware a software pro řešení peněženky, spravuje jejich konfigurace nebo nastavení a zpřístupňuje je uživatelům peněženky. Poskytovatel peněženky také poskytuje služby z řešení peněženky a provozuje procesy potřebné ke správě jednotek peněženky.

	[ZDROJ: Z CIR (EU) 2024/2981 (EUDIF IA), článek 2(8)]
zabezpečená kryptografická aplikace peněženky - WSCA	aplikace, která spravuje kritická aktiva propojením s kryptografickými a jinými funkcemi poskytovanými zabezpečeným kryptografickým zařízením peněženky a jejich používáním. POZNÁMKA: zabezpečená kryptografická aplikace peněženky musí běžet v zabezpečeném prostředí, kterým může být zabezpečené kryptografické zařízení peněženky, jiné zabezpečené prostředí na uživatelském zařízení nebo zabezpečené prostředí v rámci backendu poskytovatele peněženky. POZNÁMKA k terminologii: České znění CIR (EU) 2024/2981 používá ve stejném významu termín „bezpečná kryptografická aplikace peněženky“. [ZDROJ: Z CIR (EU) 2024/2981 (EUDIF IA), článek 2(4), poznámka přidána]
zabezpečené kryptografické zařízení peněženky - WSCD	zařízení odolné proti neoprávněné manipulaci, které poskytuje prostředí propojené s bezpečnou kryptografickou aplikací peněženky a používané touto aplikací k ochraně kritických aktiv a poskytování kryptografických funkcí pro bezpečné provádění kritických operací POZNÁMKA k terminologii: České znění CIR (EU) 2024/2981 používá ve stejném významu termín „bezpečný kryptografický prostředek peněženky“. [ZDROJ: Z CIR (EU) 2024/2981 (EUDIF IA), článek 2(6)]
řešení peněženky	kombinace softwaru, hardwaru, služeb, nastavení a konfigurací, včetně instancí peněženky, jedné nebo více zabezpečených kryptografických aplikací peněženky a jednoho nebo více zabezpečených kryptografických zařízení peněženky POZNÁMKA 1: Řešení peněženky zahrnuje všechny komponenty peněženky EUDI, které musí být certifikovány a které lze implementovat do prostředků elektronické identifikace. POZNÁMKA 2: Řešení peněženky bude pravděpodobně zahrnovat několik verzí aplikací uživatelského rozhraní peněženky a případně i zabezpečených kryptografických aplikací peněženky, zaměřených na různé druhy uživatelských zařízení. [ZDROJ: Z CIR (EU) 2024/2981 (EUDIF IA), článek 2(1), poznámky doplněny]

jednotka peněženky	Unikátní konfigurace řešení peněženky, která zahrnuje instance peněženky, zabezpečené kryptografické aplikace peněženky a zabezpečená kryptografická zařízení peněženky poskytovaná poskytovatelem peněženky jednotlivému uživateli peněženky. POZNÁMKA 1: Jednotka peněženky nezahrnuje části řešení peněženky, které přímo nepodporují uživatele, a zejména většinu služeb poskytovaných backendem poskytovatele peněženky. POZNÁMKA 2: Zabezpečená kryptografická zařízení peněženky nemusí být uživateli skutečně poskytnuta, protože mohou být součástí zařízení poskytnutého uživatelem peněženky, nebo může poskytovatel peněženky poskytovat pouze přístup ke vzdálenému zabezpečenému kryptografickému zařízení peněženky sdílenému s mnoha dalšími uživateli. POZNÁMKA 3: Typická peněženka bude obsahovat jednu instanci peněženky a zabezpečenou kryptografickou aplikaci peněženky, vhodnou pro zařízení uživatele peněženky. [ZDROJ: Z CIR (EU) 2024/2981 (EUDIF IA), článek 2(10), poznámky doplněny]
atestace jednotky peněženky - WUA	datový objekt, který popisuje komponenty jednotky peněženky nebo umožňuje autentizaci a validaci těchto komponent [ZDROJ: Z CIR (EU) 2024/2977, článek 2(5)]
uživatel peněženky	uživatel, který má kontrolu nad jednotkou peněženky [ZDROJ: Z CIR (EU) 2024/2981 (EUDIF IA), článek 2(12)]
aplikace uživatelského rozhraní peněženky - WUIA	aplikace, která definuje uživatelské rozhraní řešení peněženky POZNÁMKA 1: Instance peněženky obsahuje instanci aplikace uživatelského rozhraní peněženky. Může také obsahovat kód na straně serveru, který je součástí backendu poskytovatele peněženky. POZNÁMKA 2: Aplikace uživatelského rozhraní peněženky může obsahovat několik modulů, například modul běžící v důvěryhodném prostředí mobilního zařízení. PŘÍKLADY: Aplikace uživatelského rozhraní peněženky může být nativní mobilní aplikace běžící na mobilním zařízení nebo webová aplikace běžící v prohlížeči.
Zkratka	Význam
ACM	dohodnuté kryptografické mechanismy (katalog kryptografických mechanismů ECCG, dříve SOG-IS)

AHWG	ad hoc pracovní skupina (agentury ENISA)
AICPA	Americký institut certifikovaných účetních znalců
APCER	míra chybné klasifikace prezentačních útoků (ISO/IEC 30107-3)
API	rozhraní pro programování aplikací
ARF	architektura a referenční rámec (evropské peněženky digitální identity)
ASVS	standard OWASP pro ověřování bezpečnosti aplikací
AVA_VAN	analýza zranitelností. Rodina záruk třídy AVA (posouzení zranitelností) dle ISO/IEC 15408-3. Číslo za tečkou udává úroveň komponenty (např. AVA_VAN.3)
BLE	Bluetooth s nízkou spotřebou energie
BPCER	míra chybné klasifikace legitimních prezentací (ISO/IEC 30107-3)
BSPA, též BSZA	Baseline Security Product Assessment (národní schéma Nizozemska odvozené z EN 17640). České znění CIR (EU) 2024/2981 uvádí tuto zkratku ve tvaru BSZA
BSZ	Beschleunigte Sicherheitszertifizierung (zrychlená bezpečnostní certifikace, národní schéma Německa odvozené z EN 17640)
CAB	Conformity Assessment Body (orgán posuzování shody, též subjekt posuzování shody)
ČIA	Český institut pro akreditaci, o.p.s. (národní akreditační orgán České republiky)
CAR	zpráva o posouzení shody
CB	certifikační orgán
CC	Společná kritéria pro hodnocení bezpečnosti informačních technologií (ISO/IEC 15408)
CCRA	ujednání o vzájemném uznávání certifikátů Common Criteria
CEM	společná metodika pro hodnocení bezpečnosti informačních technologií (ISO/IEC 18045)
CEN	Evropský výbor pro normalizaci
CI/CD	průběžná integrace a průběžné dodávání
CIR	prováděcí nařízení Komise
CRA	akt o kybernetické odolnosti. Nařízení Evropského parlamentu a Rady (EU) 2024/2847
CSA	akt o kybernetické bezpečnosti. Nařízení Evropského parlamentu a Rady (EU) 2019/881
CSIRT	tým pro reakci na počítačové bezpečnostní incidenty
CSPN	Certification de Sécurité de Premier Niveau (certifikace bezpečnosti první úrovně, národní schéma Francie odvozené z EN 17640)
CSRNG	kryptograficky bezpečný generátor náhodných čísel

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.

CVD	koordinované zveřejňování zranitelností
CVE	Common Vulnerabilities and Exposures (veřejný seznam známých zranitelností)
ČR	Česká republika
CZ-nn	identifikátor hrozby doplněné schématem EUDIW-CZ do registru rizik (příloha X.A)
DAST	dynamické testování bezpečnosti aplikací
DIA	Digitální a informační agentura (vlastník schématu EUDIW-CZ)
EA	Evropská spolupráce pro akreditaci
EAA	elektronické potvrzení atributů
EAL	úroveň záruky hodnocení (ISO/IEC 15408)
ECCG	Evropská skupina pro certifikaci kybernetické bezpečnosti
eID	elektronická identifikace
eIDAS	nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, ve znění nařízení (EU) 2024/1183
eMRTD	elektronický strojově čitelný cestovní doklad (ICAO Doc 9303)
EN	evropská norma
ENISA	Agentura Evropské unie pro kybernetickou bezpečnost
ETR	technická zpráva o hodnocení
ETSI	Evropský ústav pro telekomunikační normy
EU	Evropská unie
EUCC	evropský systém certifikace kybernetické bezpečnosti založený na společných kritériích. CIR (EU) 2024/482
EUCS	evropské schéma certifikace kybernetické bezpečnosti pro cloudové služby (kandidátní schéma)
EUDI	evropská digitální identita
EUDIF	evropský rámec digitální identity. Nařízení (EU) 2024/1183
EUDIW	evropská peněženka digitální identity
EUDIW-CZ	České národní certifikační schéma evropské peněženky digitální identity (toto schéma)
FAR	míra chybného přijetí (ISO/IEC 19795-1)
FCAF	rámec pro posuzování funkční shody

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.

FitCEM	metodika hodnocení kybernetické bezpečnosti produktů IKT s pevně stanoveným časem (EN 17640)
FRR	míra chybného odmítnutí (ISO/IEC 19795-1)
GDPR	obecné nařízení o ochraně osobních údajů. Nařízení Evropského parlamentu a Rady (EU) 2016/679
HSM	hardwarový bezpečnostní modul
IAF	Mezinárodní akreditační fórum
ICAO	Mezinárodní organizace pro civilní letectví
IKT	informační a komunikační technologie
IEC	Mezinárodní elektrotechnická komise
IPSP	poskytovatel služby ověřování identity (ETSI TS 119 461)
ISMS	systém řízení bezpečnosti informací
ISO	Mezinárodní organizace pro normalizaci
IT	informační technologie
ITSEF	zařízení pro hodnocení bezpečnosti informačních technologií (hodnotící laboratoř)
LINCE	Certificación Nacional Esencial de Seguridad (národní schéma Španělska odvozené z EN 17640)
LoA	úroveň záruky (prostředku pro elektronickou identifikaci dle eIDAS)
LoIP	úroveň ověření identity (ETSI TS 119 461)
MAS	projekt OWASP pro bezpečnost mobilních aplikací
MASWE	katalog slabín mobilních aplikací OWASP
MPA	metodické pokyny pro akreditaci (dokumenty ČIA)
MRA	dohoda o vzájemném uznávání
NAB	národní akreditační orgán
NCCA	vnitrostátní orgán certifikace kybernetické bezpečnosti
NCP, NCP+	normalizovaná certifikační politika, rozšířená normalizovaná certifikační politika (ETSI EN 319 411-1)
NFC	bezkontaktní komunikace na krátkou vzdálenost
NIA	Národní bod pro identifikaci a autentizaci
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

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.

OWASP	Open Worldwide Application Security Project
PAD	detekce prezentačních útoků (ISO/IEC 30107)
PAM	řízení privilegovaného přístupu
PID	osobní identifikační údaje
PIN	osobní identifikační číslo
PKI	infrastruktura veřejných klíčů
PP	profil ochrany (ISO/IEC 15408)
PubEAA	elektronické potvrzení atributů vydané subjektem veřejného sektoru odpovídajícím za autentický zdroj nebo jeho jménem
QEAA	kvalifikované elektronické potvrzení atributů
QES	kvalifikovaný elektronický podpis
QSCD	kvalifikovaný prostředek pro vytváření elektronických podpisů nebo pečetí
QTSP	kvalifikovaný poskytovatel služeb vytvářejících důvěru
ROB	registr obyvatel (základní registr)
RP	spoléhající strana
RPO	cílový bod obnovy
RQSCD	kvalifikovaný prostředek pro vytváření elektronických podpisů nebo pečetí na dálku
RTO	cílová doba obnovy
SAST	statické testování bezpečnosti aplikací
SBOM	soupis softwarových komponent
SDLC	životní cyklus vývoje softwaru
SFR	bezpečnostní funkční požadavek (ISO/IEC 15408)
SLA	dohoda o úrovni služby
SoA	prohlášení o aplikovatelnosti (ISO/IEC 27001)
SOC 2	System and Organization Controls 2 (zpráva o ověření dle kritérií AICPA)
SOG-IS	Senior Officials Group Information Systems Security (skupina vyšších úředníků pro bezpečnost informačních systémů)
SSDLC	bezpečný životní cyklus vývoje softwaru
ST	bezpečnostní cíl (ISO/IEC 15408)

TEE	prostředí důvěryhodného provádění
TLS	Transport Layer Security (protokol zabezpečení transportní vrstvy)
TOE	předmět hodnocení (ISO/IEC 15408)
TRnn	identifikátor hrozby v registru rizik v příloze I CIR (EU) 2024/2981
TS	technická specifikace (ETSI, CEN)
TSC	kritéria důvěryhodných služeb (AICPA)
TSP	poskytovatel služeb vytvářejících důvěru
ÚOOÚ	Úřad pro ochranu osobních údajů
vTPM	virtuální modul důvěryhodné platformy
WIA	atestace instance peněženky
WSCA	zabezpečená kryptografická aplikace peněženky
WSCD	zabezpečené kryptografické zařízení peněženky
WUA	atestace jednotky peněženky
WUIA	aplikace uživatelského rozhraní peněženky
ZR	základní registry