Digitální a informační agentura

DIAPX007L3GI
PRVOTNÍ IDENTIFIKÁTOR

Dokument konkretizující požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru [DKP]

Historie dokumentu:

Verze	*Vytvořeno*	*Autor*	*Poznámka*	*Status*
1	25.07.2016	FB	první draft	Návrh
2	1.8.2016	FB, kolektiv EG	Reakce na připomínky	Ke zveřejnění
2	12.3.2018	FB	Pouze formální úprava – oprava překlepu v názvu kapitoly č. 4	Ke zveřejnění
3	22.01.2020	FB	Změny reflektující nové verze norem a standardů, upřesnění aplikovatelných požadavků ČSN EN ISO/IEC 17021-1 a ČSN ISO/IEC 27006, doplnění sekce řízení rizik a další na základě obdržených připomínek od zúčastněných stran.	Ke zveřejnění
4	1.12.2020 15.2.2021	FB	Doplnění požadavků pro QTSP poskytující kvalifikovanou službu elektronického doporučeného doručování (QERDS a QREMS). Úprava dokumentu na základě došlých připomínek.	Ke zveřejnění
5	12.4.2026	Kolektiv OSEG	Změna orgánu dohledu z MV ČR na DIA.	

			Doplnění změn reflektující nové typy kvalifikovaných služeb vytvářejících důvěru dle Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu. Dále změny reflektujících prováděcí nařízení Komise (EU) 2025/2162 a prováděcí nařízení k některým typům kvalifikovaných služeb vytvářejících důvěru. Zapracovány návrhy ze strany QTSP,TSP a CAB. Č.j. DIA- 135-2/OSEG-2026	

Obsah

1. Účel dokumentu

Tento dokument je určen k upřesnění požadavků pro akreditaci subjektů posuzování shody (conformity assessment body, dále jen „CAB“) ze strany národního akreditačního orgánu (national accreditation body, dále jen „NAB“).

Dokument obsahuje výčet použitelných požadavků nařízení eIDAS (nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES) ve znění Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024 kladených na kvalifikované poskytovatele služeb vytvářejících důvěru a na jimi poskytované kvalifikované služby vytvářející důvěru a odkazy na příslušné části technických norem, standardů a specifikací, jejichž splněním je možno demonstrovat soulad s požadavky nařízení eIDAS, případně také výčet technických norem, standardů a specifikací, které se váží ke konkrétní oblasti. Vzhledem k tomu, že nařízení eIDAS cílí na technologickou neutralitu, není možno v dokumentu stanovit povinný výčet norem, pouze jejichž splněním poskytovatel služeb vytvářejících důvěru demonstruje splnění požadavků stanovených nařízením eIDAS. Zároveň dokument reflektuje požadavky prováděcího nařízení Komise (EU) 2025/2162 ze dne 27. října 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o akreditaci subjektů posuzování shody provádějících posuzování kvalifikovaných poskytovatelů služeb vytvářejících důvěru a jimi poskytovaných kvalifikovaných služeb vytvářejících důvěru, zprávu o posouzení shody a režim posuzování shody (dále jen „CIR 2025/2162“).

Požadavky vychází z normy **ČSN EN *ISO/IEC 17065 (Posuzování shody - Požadavky na orgány certifikující produkty, procesy a služby)*** jakožto obecného rámce stanovujícího požadavky pro certifikační subjekty, provádějící certifikaci shody produktů, procesů a služeb. Obecná norma ČSN EN ***ISO/IEC 17065*** vyžaduje od CAB plnění:

- aplikovatelných požadavků ***ČSN EN ISO/IEC 17021-1 (Conformity assessment -- Requirements for bodies providing audit and certification of management systems)***
- aplikovatelných požadavků **ČSN** ***ISO/IEC 27006 (Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems)***

Vzhledem k obecné použitelnosti **ČSN EN *ISO/IEC 17065*** je nutné stanovit speciální sektorové požadavky pro CAB, které mají provádět posouzení shody u kvalifikovaných poskytovatelů služeb vytvářejících důvěru (qualified trust service providers, dále jen „QTSP“). Tyto sektorové požadavky jsou definovány v normě ***ČSN ETSI EN 319 403 -1 (Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatelů důvěryhodných služeb - Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodných služeb)*** a specifikují jak obecné požadavky na CABy, tak i obecná pravidla pro provádění příslušných auditů. Součástí ČSN EN 319 403-1 jsou rovněž výše uvedené aplikovatelné požadavky norem ČSN EN ISO/IEC 17021-1 a ČSN ISO/IEC 27006[1]. Zároveň je tato problematika rovněž upravena v CIR 2025/2162.

Aby mohl být režim akreditace skutečně účinný, je nutné definovat tzv. „TSP audit kriteria“, vůči kterým by kompetentnost CABů měla být akreditována ze strany NAB a rovněž podle kterých

[1] Viz ustanovení z ČSN EN 319 403-1: „The present document also incorporates many requirements relating to the audit of a TSP's management system, as defined in ISO/IEC 17021 [i.12] and in ISO/IEC 27006 [i.11]. These requirements are incorporated by including text to derived from these documents in the present document, as well indirectly through references to requirements of ISO/IEC 17021 [i.12].“

by mělo probíhat samotné posuzování shody ze strany CABů u QTSP. Podle normy ***ČSN EN 319 403-1*** by auditní kritéria měla být založena na následujícím:

a) take into account specificities of the type of trust service to be assessed;

b) ensure that all aspects of the TSP activity are fully covered; and

c) be based on standards, publicly available specifications and/or regulatory requirements.

EXAMPLE: Standards on which those criteria could be based include ETSI EN 319 401 [i.6], ETSI EN 319 411-1 [i.2], or ETSI EN 319 411-2 [i.3] or ETSI EN 319 421 [i.9]. Regulatory requirements on which those criteria could be based include those defined in Regulation (EU) No 910/2014 [i.1].

a) brala v úvahu specifika posuzované služby vytvářející důvěru,

b) zajistila, aby všechny aspekty činnosti TSP byly pokryty a

c) vycházela ze standardů, veřejně dostupných specifikací a/nebo regulatorních požadavků.

Příklad: Standardy, na kterých mohou být tato kritéria založena, zahrnují ETSI EN 319 401, ETSI EN 319 411-1, nebo ETSI EN 319 411-2 nebo ETSI EN 319 421. Regulatorní požadavky, na základě kterých mohou být založena kritéria, zahrnují požadavky nařízení eIDAS a jeho prováděcích aktů.

Zároveň CIR 2025/2162 obsahuje odkazy na normy a standardy, které by subjekty posuzování shody měly používat jako referenční hodnoty pro posuzování kvalifikovaných poskytovatelů služeb vytvářejících důvěru a jimi poskytovaných kvalifikovaných služeb vytvářejících důvěru, přičemž by měly zohlednit verze a úpravy těchto norem stanovené v prováděcích aktech pro jednotlivé služby na základě nařízení (EU) č. 910/2014. Tímto způsobem budou moci akreditované CABy provádět nejen pravidelné audity podle článku 20.1 nařízení eIDAS, ale rovněž také počáteční posouzení shody dle článku 21 nařízení eIDAS a rovněž ad-hoc posouzení shody podle článku 20.2 nařízení eIDAS - stejná audit kritéria pro všechny tři typy posouzení shody.

Vyžaduje se, aby CAB byl certifikační orgán a nikoliv „jen“ inspekční orgán či laboratoř, jelikož CAB musí certifikovat poskytovatele vůči definovaným auditním kritériím. Certifikace vyžaduje pravidelné sledování služeb s cílem zjistit, zda jsou trvale plněny požadavky na produkt-službu, stejně jako požadavky na stálou snahu zlepšovat poskytované služby.

Cílem normy ***ČSN EN 319 403-1*** a CIR 2025/2162 je rovněž umožnit posouzení shody podle osvědčených postupů z praxe a stejně také podle technických požadavků nařízení eIDAS.

2. Režim posuzování shody

Tato kapitola shrnuje požadavky uvedené ve článku 6 CIR 2025/2162, které se vztahují jak na vlastníka režimu posuzování shody, tak CAB a kvalifikované poskytovatele služeb vytvářejících důvěru.

- Vlastníkem dokumentu DKP jakožto dokumentu upravující režim posuzování shody (conformity assessment schemes) je Digitální a informační agentura. Případné stížnosti ohledně provádění režimu posuzování shody je tak nutné adresovat na tuto agenturu[2], stejně tak jako informace o vydávání certifikátů shody a jejich změn.
- Je umožněna akreditace s flexibilním rozsahem - konkrétní verze dokumentu DKP použitá v rámci certifikace konkrétní kvalifikované služby vytvářející důvěru musí být uvedena v certifikačním rozhodnutí.

[2] Digitální a informační agentura, Na Vápence 915/14, 130 00 Praha 3,IČO: 17651921, ID DS: yukd8p7, emailová adresa: posta@dia.gov.cz.

- Subjekty posuzování shody jsou povinny provádět roční činnosti dozoru pro každou z kvalifikovaných služeb vytvářejících důvěru na základě příslušných požadavků bodu 7.9 normy ČSN ISO/IEC 17065:2012.
- Digitální a informační agentura bude informovat o změnách v rámci tohoto dokumentu a poskytne možnost tyto změny připomínkovat ze strany kvalifikovaných poskytovatelů služeb vytvářejících důvěru a CAB.
- CAB musí zajistit dostupnost týmu nejméně dvou kvalifikovaných osob, které mají potřebné odborné znalosti k provedení takového posouzení shody.
- Kvalifikovaní poskytovatelé služeb vytvářejících důvěru musí mít zavedeny procesy, postupy a pracovní pokyny pro informování CAB nejméně jeden měsíc před tím, než kvalifikovaní poskytovatelé služeb vytvářejících důvěru provedou jakoukoli významnou změnu v poskytování kvalifikovaných služeb vytvářejících důvěru certifikovaných v rámci daného režimu, a nejméně tři měsíce před tím, než hodlají poskytování služeb nebo jejich částí ukončit.
- CAB nevydá kladné rozhodnutí o certifikaci nebo jakýchkoliv certifikát shody, pokud posouzení shody vede ke zjištění nesouladu posuzovaných kvalifikovaných poskytovatelů služeb vytvářejících důvěru a jimi poskytovaných kvalifikovaných služeb vytvářejících důvěru s požadavky nařízení eIDAS a článku 21 směrnice NIS2.
- Kvalifikovaní poskytovatelé služeb vytvářejících důvěru musí neprodleně informovat Digitální a informační agenturu jakožto orgán dohledu v ČR o jakékoli změně certifikátu shody. Kvalifikovaní poskytovatelé služeb vytvářejících důvěru se zdrželi poskytování dotčených kvalifikovaných služeb vytvářejících důvěru nebo propagace jakýchkoli odkazů na ně, dokud Digitální a informační agentura znovu nepotvrdí status kvalifikovaného poskytovatele nebo kvalifikované služby.
- CAB při posuzování shody musí zajistit dostatečné zdroje a čas s ohledem na rozsah a složitost posouzení konkrétního poskytovatele a služby. Údaje o délce trvání posouzení shody musí být uvedeny ve zprávě o posouzení shody.

Rozsah posouzení shody, včetně technického ověřování a bezpečnostních testů, se stanovuje s ohledem na povahu, rozsah a složitost poskytované kvalifikované služby a vychází z rizik a relevance jednotlivých komponent pro její poskytování. Posouzení se zaměřuje na ty části systému, které mají vliv na plnění požadavků nařízení eIDAS.

3. Požadavky na QTSP

3.1. Zpracování a ochrana údajů

Zpracování osobních údajů se obecně provádí v souladu s nařízením (EU) 2016/679 (známé pod zkratkou GDPR), což rovněž potvrzuje článek 2 odst. 4 nařízení eIDAS. CAB ověří při posuzování shody soulad s GDPR.

eIDAS článek 2 odst.4	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Kapitola 7.13, REQ[3]-7.13-05. TSP provozující služby v EU se musí řídit GDPR.

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

3.2. Pseudonymy

eIDAS - článek 5: Aniž jsou dotčeny právní účinky, které vnitrostátní právo přiznává pseudonymům, není používání pseudonymů v elektronických transakcích zakázáno.

eIDAS článek 5	Např. Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons (ETSI EN 319 412-2)	Kapitola 4.2.4.

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

3.3. Odpovědnost za škodu a důkazní břemeno

eIDAS - článek 13.1: Poskytovatelé služeb vytvářejících důvěru odpovídají za škodu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností podle nařízení eIDAS (a aniž jsou dotčeno nařízení GDRP). Každá fyzická nebo právnická osoba, která v důsledku porušení tohoto nařízení poskytovatelem služeb vytvářejících důvěru utrpěla hmotnou či nehmotnou újmu, má právo požadovat náhradu újmy v souladu s právem Unie a vnitrostátním právem.

- Důkazní břemeno, pokud jde o úmysl nebo nedbalost nekvalifikovaného poskytovatele služeb vytvářejících důvěru, nese fyzická nebo právnická osoba uplatňující nárok na náhradu škody.

V případě QTSP se úmysl nebo nedbalost předpokládá, QTSP musí dokázat, že škoda nastala bez jeho úmyslu nebo nedbalosti.

eIDAS - článek 13.2: Pokud poskytovatelé služeb vytvářejících důvěru své zákazníky předem informují o omezeních týkajících se využívání jimi poskytovaných služeb a tato omezení jsou rozpoznatelná pro třetí osoby, poskytovatelé služeb vytvářejících důvěru neodpovídají za škody způsobené využíváním služeb nad rámec uvedených omezení.

eIDAS - článek 13.3: Odpovědnost za škodu a prokazování se řídí vnitrostátními pravidly upravujícími odpovědnost za škodu.

[3] Zkratka REQ značí konkrétní požadavek uvedený v dané normě (REQ - requirement).

eIDAS článek 13(2)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Kapitola 6.2
	Certificate Profiles (ETSI EN 319 412-5)	Kap. 4.3.2 pokud je uváděno omezení maximální hodnoty transakcí formou QCStatementu v certifikátu.
eIDAS článek 13(3)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Kap. REQ-7.1.1-04 a REQ-7.1.1-05.

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

3.4. Přístupnost pro osoby se zdravotním postižením

eIDAS - článek 15: Poskytování služeb vytvářejících důvěru a produktů pro koncové uživatele, které jsou používány při poskytování těchto služeb, se zpřístupní jednoduchým a srozumitelným jazykem, v souladu s Úmluvou Organizace spojených národů o právech osob se zdravotním postižením a s požadavky na přístupnost obsaženými ve směrnici (EU) 2019/882, z čehož mají prospěch i osoby s funkčními omezeními, jako jsou starší osoby a osoby s omezeným přístupem k digitálním technologiím.

eIDAS článek 15	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Kapitola REQ-7.13-03 vyžaduje, aby poskytované služby a konečné uživatelské produkty používané pro poskytování těchto služeb byly přístupné pro osoby se zdravotním postižením (je třeba vzít v úvahu použitelné standardy (kap. REQ-7.13-04), jako je např. EN 301 549).
	Accessibility requirements suitable for public procurement of ICT products and services in Europe (ETSI EN 301 549)	

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

3.5. Řízení kybernetické bezpečnosti (článek 20 nařízení eIDAS)

S cílem zefektivnit povinnosti v oblasti kybernetické bezpečnosti uložené QTSP a umožnit těmto poskytovatelům a jejich příslušným orgánům využívat právní rámec stanovený směrnicí Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen „směrnice NIS 2“) jsou služby vytvářející důvěru povinny přijmout vhodná technická a organizační opatření podle uvedené směrnice (článek 21), jako jsou opatření zaměřená na selhání systémů, chyby způsobené lidským faktorem, svévolné zásahy nebo přírodní jevy, za účelem řízení rizik pro bezpečnost sítí a informačních systémů, které tito poskytovatelé používají při poskytování svých služeb, jakož i oznamování významných incidentů a kybernetických hrozeb v souladu s touto směrnicí. Požadavky na řízení kybernetických bezpečnostních rizik a oznamovací povinnosti podle směrnice NIS2 by měly být považovány za doplňkové k požadavkům uloženým poskytovatelům služeb vytvářejících důvěru podle nařízení eIDAS.

Problematika řízení kybernetické bezpečnosti pro QTSP nyní tak spadá pod směrnici NIS2 jakožto horizontální právní předpis pro oblast řízení kybernetické bezpečnosti. V České republice byla směrnice NIS2 transponována prostřednictvím zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „zákon č. 264/2025 Sb.“).

V souladu se směrnicí NIS2 se považuje QTSP za poskytovatele regulované služby v režimu vyšších povinností (viz čl. 3 směrnice NIS2 – „základní subjekt“ a přílohy vyhlášky č. 408/2025 Sb., o regulovaných službách, vydaná k zákonu č. 264/2025 Sb.).

QTSP je dle § 18 odst. 1 zákona č. 264/2025 Sb. ve vztahu k poskytovaným službám povinen v rámci stanoveného rozsahu zavádět a provádět vhodná a přiměřená bezpečnostní opatření zahrnující alespoň řízení rizik, řízení bezpečnostní politiky a bezpečnostní dokumentace, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, řízení dodavatelů, bezpečnou akvizici, vývoj a údržbu, aplikační bezpečnost, bezpečnost lidských zdrojů, kryptografické algoritmy, řízení přístupu a správu a ověřování identit, a to v míře a způsobem stanoveným CIR 2024/2690[4] , pokud jde o technické a metodické požadavky opatření, která jsou uvedení QTSP povinni přijímat; § 13 odst. 2 zákona č. 264/2025 Sb. se ve vztahu k těmto regulovaným službám nepoužije. Pokud jde o výčet použitelných požadavků dle CIR 2024/2690 týkající se řízení kybernetické bezpečnosti QTSP, jedná se o čl. 2 (a odkazovaná příloha), čl. 3, čl. 4 a čl. 14.

Výčet norem a standardů viz další kapitoly.

3.6. Oznamování o narušení bezpečnosti

V případě, kdy se jedná o významný incident týkající se kybernetické bezpečnosti, QTSP jej primárně hlásí NÚKIB (kritéria pro určení, kdy se incident považuje za významný jsou uvedena v čl. 3, 4 a 14

[4] Prováděcí nařízení Komise (EU) 2024/2690 ze dne 17. října 2024, kterým se stanoví pravidla pro uplatňování směrnice (EU) 2022/2555, pokud jde o technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik a bližší upřesnění případů, v nichž se incident považuje za významný, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru

CIR 2024/2690). V příslušných případech dotčené subjekty oznámí bez zbytečného odkladu příjemci svých služeb významné incidenty, které by mohly negativně ovlivnit poskytování těchto služeb. Viz směrnice NIS2 a zákon č. 264/2025 Sb.

Oznámení o narušení bezpečnosti nebo narušení poskytování služby nebo provádění opatření ve smyslu čl. 24 odst. 2 písm. fb) nařízení eIDAS se činní vůči orgánu dohledu v oblasti eIDAS (Digitální a informační agentura), dále vůči identifikovatelným dotčeným osobám, případně dalším relevantním příslušným orgánům a na žádost orgánu dohledu veřejnosti, pokud je to ve veřejném zájmu.

Jak je uvedeno v recitálu č. 50 revize nařízení eIDAS, tak nařízením eIDAS není dotčena povinnost oznamovat porušení zabezpečení osobních údajů podle GDPR (viz čl. 33 a 34 tohoto nařízení).

3.7. Používání kryptografických algoritmů při poskytování QTS

Digitální a informační agentura vydala separátní upřesnění k DKP s názvem Používání kryptografických algoritmů při poskytování kvalifikovaných služeb vytvářejících důvěru s ohledem na problematiku používání algoritmu RSA s délkou klíče 2048 bitů.

Subjekty posuzování shody při auditech (jak iniciačních, tak i dozorových) kvalifikovaných poskytovatelů služeb vytvářejících důvěru a jimi poskytovaných kvalifikovaných služeb vytvářejících důvěru ověří, zda kvalifikovaný poskytovatel služeb vytvářejících důvěru implementuje opatření uvedená v tomto upřesnění:

Kvalifikovaní poskytovatelé služeb vytvářejících důvěru musí zahájit nebo pokračovat v činnostech vedoucích k přechodu na silnější kryptografické algoritmy (zejména ECC) nebo RSA s délkou klíče alespoň 3072 bitů využívané v rámci poskytování kvalifikovaných služeb vytvářejících důvěru koncovým zákazníkům tak, aby do konce roku 2026 bylo dosaženo stavu, kdy nově vydané kvalifikované certifikáty nebo kvalifikovaná elektronická časová razítka byly založeny na ECC nebo RSA s délkou klíče alespoň 3072 bitů. Stran kvalifikovaných certifikátů založených na RSA s délkou klíče 2048 bitů, které budou na začátku roku 2027 stále platné a využívané pro vytváření (resp. ověřování) uznávaných elektronických podpisů/pečetí, musí kvalifikovaní poskytovatelé služeb vytvářejících důvěru zajistit jejich "pře-vydání" nejpozději do poloviny roku 2027.

3.8. Požadavky pro všechny QTSP při poskytování QTS

Společné požadavky pro všechny QTSP poskytující kvalifikované služby vytvářející důvěru (dále jen „QTS") jsou reglementovány ve článku 24.2 nařízení eIDAS, podle kterého má QTSP:

- oznámit orgánu dohledu případné změny v poskytování svých kvalifikovaných služeb vytvářejících důvěru (alespoň jeden měsíc před provedením) a záměr ukončit své činnosti (tři měsíce před ukončením) – blíže upřesněno ve čl. 1 CIR 2025/2530. Dále musí QTSP tyto informace oznámit také příslušnému CAB a to na základě čl. 6 odst. 6 CIR 2025/2162.
- zaměstnávat pracovníky a případně subdodavatele, kteří mají potřebné odborné znalosti, zkušenosti a kvalifikace, jsou spolehliví a absolvovali odpovídající odbornou přípravu týkající se bezpečnosti a pravidel ochrany osobních údajů, a používat správní a řídicí postupy, které odpovídají evropským nebo mezinárodním normám
- v souladu s článkem 13 eIDAS udržovat dostatečné finanční prostředky nebo uzavřít vhodné pojištění odpovědnosti v souladu s vnitrostátním právem s ohledem na odpovědnost za škodu

- před uzavřením smluvního vztahu informovat jasným, srozumitelným a jednoduše přístupným způsobem, ve veřejně dostupném prostoru a individuálně každou osobu, která chce využít kvalifikovanou službu vytvářející důvěru, o přesných podmínkách používání této služby, včetně případných omezení jejího využívání
- používat důvěryhodné systémy a produkty, které jsou chráněny proti pozměnění, a zajišťovat technickou bezpečnost a spolehlivost procesů, které podporují, včetně použití vhodných kryptografických technik
- používat důvěryhodné systémy k uchovávání dat, která jsou mu poskytnuta, v ověřitelné podobě tak, aby byla veřejně přístupná pro účely vyhledávání pouze se souhlasem osoby, jíž se data týkají, záznamy a změny v uložených datech mohly provádět pouze oprávněné osoby a bylo možno ověřit pravost dat;
- bez ohledu na článek 21 směrnice (EU) 2022/2555 mít vhodné politiky a přijímat odpovídající opatření pro řízení právních, obchodních, provozních a jiných přímých nebo nepřímých rizik poskytování kvalifikované služby vytvářející důvěru zahrnující alespoň opatření týkající se registrace ke službě a zapojení do jejího používání, procesních nebo správních kontrol, řízení a provádění služeb – podle CIR 2025/2530 se požadavky stanovené v článcích 2, 3 a 4 CIR 2025/2160 použijí obdobně na kvalifikované poskytovatele služeb vytvářejících důvěru, pokud jde o požadavek mít rámec pro řízení rizik stanovený v čl. 24 odst. 2 písm. fa) nařízení (EU) č. 910/2014. Relevantní normou v této oblasti je ČSN ETSI EN 319 401.
- oznámit orgánu dohledu, identifikovatelným dotčeným osobám, případně dalším relevantním příslušným orgánům a na žádost orgánu dohledu veřejnosti, pokud je to ve veřejném zájmu, veškerá narušení bezpečnosti nebo narušení poskytování služby nebo provádění opatření uvedených v předchozím bodě, která mají významný dopad na poskytovanou službu vytvářející důvěru nebo na osobní údaje v ní uchovávané, ve lhůtách stanovených nařízením eIDAS
- přijímat vhodná opatření proti padělání, odcizení nebo zneužití dat nebo neoprávněnému vymazání, pozměnění nebo znepřístupnění dat
- po přiměřenou dobu, i poté, co ukončil svou činnost kvalifikovaného poskytovatele služeb vytvářejících důvěru, evidovat a zpřístupňovat veškeré příslušné informace týkající se dat, která vydal a obdržel, zejména pro účely poskytnutí důkazů v soudním a správním řízení a pro účely zajištění kontinuity služby. Tato evidence může mít elektronickou podobu
- mít k dispozici aktualizovaný plán ukončení činnosti k zajištění kontinuity služby v souladu s ustanoveními ověřenými orgánem dohledu – blíže upřesněno ve čl. 3 CIR 2025/2530

Pozn. Nařízení eIDAS rovněž ve článku 20 definuje režim auditů nad QTSP a ve článku 21 definuje postup pro zahájení poskytování kvalifikované služby vytvářející důvěru.

- Pravidelný audit: kvalifikovaní poskytovatelé služeb vytvářejících důvěru se na vlastní náklady alespoň jednou za 24 měsíců podrobí auditu ze strany subjektu posuzování shody. Účelem auditu je potvrzení toho, že kvalifikovaní poskytovatelé služeb vytvářejících důvěru i jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení a v článku 21 směrnice (EU) 2022/2555. Poskytovatelé předloží výslednou zprávu o posouzení shody do tří pracovních dnů od jejího obdržení orgánu dohledu (tj. Digitální a informační agentuře).
- Kvalifikovaní poskytovatelé služeb vytvářejících důvěru informují orgán dohledu o plánovaných auditech alespoň jeden měsíc předem a na požádání umožní účast orgánu dohledu jako pozorovatele.

- Ad-hoc audit: orgán dohledu může u QTSP na jejich náklady kdykoli provést audit nebo požádat subjekt posuzování shody o provedení posouzení shody za účelem potvrzení, že oni sami i jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení.
- V případě zjištění porušení pravidel týkajících se ochrany osobních údajů, informuje dozorový úřad zřízený podle článku 51 nařízení (EU) 2016/679 (v ČR Úřad pro ochranu osobních údajů) příslušný orgán dohledu (v ČR Digitální a informační agentura o tomto. Stejně tak DIA bezodkladně vyrozumí Úřad pro ochranu osobních údajů o zjištěních učiněných v souvislosti s plněním úkolů orgánu dohledu (vyplývá ze zákona č. 297/2016 Sb.).
- Pokud QTSP nenapraví neplnění požadavků nařízení eIDAS nebo článku 21 směrnice (EU) 2022/2555 (po oznámení od orgánu stanoveného v § 1 odst. 1 zákona č. 264/2025 Sb.) nebo nařízení (EU) 2016/679 (po oznámení od orgánu dohledu dle § 51 odst. 1 zákona č. 110/2019 Sb.) do (případně) stanovené lhůty orgánem dohledu (tj. Digitální a informační agenturou), může orgán dohledu zejména s přihlédnutím k rozsahu, délce trvání a důsledkům daného neplnění odejmout danému poskytovateli.
  a jím poskytované dotčené službě status kvalifikovaného poskytovatele nebo kvalifikované služby. Orgán dohledu vyrozumí daného kvalifikovaného poskytovatele služeb vytvářejících důvěru o odnětí statusu kvalifikovaného poskytovatele nebo kvalifikované služby.

<u>Postup pro zahájení poskytování kvalifikované služby vytvářející důvěru:</u>

- Pokud poskytovatelé služeb vytvářejících důvěru hodlají začít poskytovat kvalifikovanou službu vytvářející důvěru, oznámí orgánu dohledu svůj úmysl spolu se zprávou o posouzení shody vydanou subjektem posuzování shody, která potvrzuje splnění požadavků stanovených v tomto nařízení a v článku 21 směrnice (EU) 2022/2555. Orgán dohledu ověří, zda poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení, zejména požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru a na jimi poskytované kvalifikované služby vytvářející důvěru. Zároveň dne 19. srpna 2026 nabývá účinnosti prováděcí nařízení Komise (EU) 2025/1572 ze dne 29. července 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o formát a postupy pro oznamování úmyslu a ověřování s ohledem na zahájení poskytování kvalifikovaných služeb vytvářejících důvěru. Toto prováděcí nařízení mimo jiné stanovuje požadavky na obsah oznámení o úmyslu zahájení poskytování kvalifikovaných služeb vytvářejících důvěru zasílaného orgánu dohledu od poskytovatele služeb vytvářejících důvěru, který chce začít poskytovat kvalifikovanou službu vytvářející důvěru.
- Za účelem ověření, zda poskytovatel služeb vytvářejících důvěru splňuje požadavky stanovené v článku 21 směrnice (EU) 2022/2555, požádá orgán dohledu příslušné orgány určené nebo zřízené podle čl. 8 odst. 1 uvedené směrnice (v ČR Národní úřad pro kybernetickou a informační bezpečnost), aby k tomu provedly opatření dohledu a poskytly informace o výsledku bez zbytečného odkladu a v každém případě do dvou měsíců od obdržení této žádosti. Není-li ověření dokončeno do dvou měsíců od oznámení, vyrozumí uvedené příslušné orgány orgán dohledu a uvedou důvody prodlení a dobu, v níž bude ověřování dokončeno.
- Dospěje-li orgán dohledu k závěru, že poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení, udělí orgán dohledu tomuto poskytovateli služeb vytvářejících důvěru a jím

poskytovaným službám vytvářejícím důvěru status kvalifikovaného poskytovatele a kvalifikované služby a uvědomí o tom subjekt uvedený v čl. 22 odst. 3 (v ČR Digitální a informační agentura) za účelem aktualizace důvěryhodných seznamů podle čl. 22 odst. 1, a to nejpozději do tří měsíců od obdržení oznámení podle odstavce 1 tohoto článku. Není-li ověření dokončeno do tří měsíců od oznámení, vyrozumí orgán dohledu poskytovatele služeb vytvářejících důvěru a uvede důvody prodlení a dobu, v níž bude ověřování dokončeno.

- Kvalifikovaní poskytovatelé služeb vytvářejících důvěru mohou začít danou kvalifikovanou službu vytvářející důvěru poskytovat poté, co byl status kvalifikovaného poskytovatele a kvalifikované služby vyznačen v důvěryhodných seznamech.

Příslušné referenční normy pro režimy posuzování shody jsou stanoveny v příloze II CIR 2025/2162.

Soulad s požadavky uvedenými ve čl. 24 odst. 2 je možné prokázat pomocí shody s CIR 2025/2530 pro jednotlivé typy kvalifikovaných služeb vytvářejících důvěru (QTSP však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů):

Typ kvalifikované služby	Seznam referenčních norem a specifikací
Kvalifikovaná služba vytvářející důvěru pro vydávání kvalifikovaných certifikátů pro elektronické podpisy	body 5.2, 6.1, 6.4, 6.5, 6.8 a 6.9 normy ETSI EN 319 411-2, jak na ni odkazuje a jak ji upravuje bod 1 přílohy I prováděcího nařízení Komise (EU) 2025/1943
Kvalifikovaná služba vytvářející důvěru pro vydávání kvalifikovaných certifikátů pro elektronické pečetě	body 5.2, 6.1, 6.4, 6.5, 6.8 a 6.9 normy ETSI EN 319 411-2, jak na ni odkazuje a jak ji upravuje bod 1 přílohy II prováděcího nařízení (EU) 2025/1943.
Kvalifikovaná služba vytvářející důvěru pro vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek	body 5.2, 6.1, 6.4, 6.5, 6.8 a 6.9 normy ETSI EN 319 411-2, jak na ni odkazuje a jak ji upravuje příloha prováděcího nařízení (EU) 2025/1943
Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů	body 5, 6 a 7 normy ETSI TS 119 441, jak na ni odkazuje a jak ji upravuje bod 1 přílohy prováděcího nařízení Komise (EU) 2025/1942
Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických pečetí	body 5, 6 a 7 normy ETSI TS 119 441, jak na ni odkazuje a jak ji upravuje bod 1 přílohy prováděcího nařízení (EU) 2025/1942
Kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů	body 5, 6 a 7 normy ETSI TS 119 511, jak na ni odkazuje a jak ji upravuje bod 1 přílohy prováděcího nařízení Komise (EU) 2025/1946
Kvalifikovaná služba uchovávání kvalifikovaných elektronických pečetí	body 5, 6 a 7 normy ETSI TS 119 511, jak na ni odkazuje a jak ji upravuje bod 1 přílohy prováděcího nařízení (EU) 2025/1946

Kvalifikované služby vytvářející důvěru pro vytváření kvalifikovaných elektronických časových razítek	body 5, 6 a 7 normy ETSI EN 319 421, jak na ni odkazuje a jak ji upravuje bod 1 přílohy prováděcího nařízení Komise (EU) 2025/1929
Kvalifikovaná služba elektronického doporučeného doručování	body 4, 6 a 7 normy ETSI EN 319 521, jak na ni odkazuje a jak ji upravuje příloha I prováděcího nařízení Komise (EU) 2025/1944 ETSI EN 319 531 (QTSP poskytující QREMS)
Kvalifikovaná služba správy kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku	body 5, 6.1, 6.4, 6.5, 6.7 a 6.8 normy ETSI TS 119 431-1, jak na ni odkazuje a jak ji upravuje příloha prováděcího nařízení Komise (EU) 2025/1567
Kvalifikovaná služba správy kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku	body 5, 6.1, 6.4, 6.5, 6.7 a 6.8 normy ETSI TS 119 431-1, jak na ni odkazuje a jak ji upravuje příloha prováděcího nařízení (EU) 2025/1567

4. Požadavky pro QTSP vydávající kvalifikované certifikáty

Požadavky pro QTSP vydávající kvalifikované certifikáty se skládají jednak z požadavků pro všechny QTSP (viz kapitola 3) a následujících:

eIDAS - článek 24.1: *Při vydávání kvalifikovaného certifikátu nebo kvalifikovaného elektronického potvrzení atributů ověří kvalifikovaný poskytovatel služeb vytvářejících důvěru totožnost a případně zvláštní atributy fyzické nebo právnické osoby, jimž se má kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů vydat.*

eIDAS - článek 24.1a: *Kvalifikovaný poskytovatel služeb vytvářejících důvěru provede ověření totožnosti uvedené v odstavci 1 vhodným způsobem buď přímo, nebo prostřednictvím třetí strany, a to na základě jedné z těchto metod nebo případně jejich kombinace a v souladu s prováděcími akty uvedenými v odstavci 1c:*

a) prostřednictvím evropské peněženky digitální identity nebo oznámených prostředků pro elektronickou identifikaci, které splňují požadavky stanovené v článku 8 eIDAS, pokud jde o vysokou úroveň záruky;

b) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaných v souladu s písmeny a), c) nebo d);

c) použitím jiných metod identifikace, které zajišťují identifikaci osoby s vysokou úrovní spolehlivosti, jejichž shodu potvrdí subjekt posuzování shody;

d) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby pomocí vhodných důkazů a postupů v souladu s vnitrostátním právem.

eIDAS - článek 24.1b: *Kvalifikovaný poskytovatel služeb vytvářejících důvěru provede ověření atributů uvedené v odstavci 1 vhodným způsobem buď přímo, nebo prostřednictvím třetí strany, a to na základě jedné z těchto metod nebo případně jejich kombinace a v souladu s prováděcími akty uvedenými v odstavci 1c:*

a) prostřednictvím evropské peněženky digitální identity nebo oznámených prostředků pro elektronickou identifikaci, které splňují požadavky stanovené v článku 8, pokud jde o vysokou úroveň záruky;

b) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaných v souladu s odst. 1a písm. a), c) nebo d);

c) pomocí kvalifikovaného elektronického potvrzení atributů;

d) použitím jiných metod, které zajišťují ověření atributů s vysokou úrovní spolehlivosti, jejichž shodu potvrdí subjekt posuzování shody;

e) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby pomocí vhodných důkazů a postupů v souladu s vnitrostátním právem.

eIDAS - článek 24.1c: *Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely ověřování totožnosti a atributů v souladu s odstavci 1, 1a a 1b tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.*

Na základě tohoto zmocnění bylo vydáno prováděcí nařízení Komise (EU) 2025/1566 ze dne 29. července 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční standardy pro ověřování totožnosti a atributů osob, jimž mají být vydány kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů (dále jen „CIR 2025/1566“). S ohledem na potřebu poskytnout dostatek času na přizpůsobení QTSP požadavkům prováděcího aktu, má tento prováděcí akt odloženou účinnost, přičemž se má použít od 19. srpna 2027.

Do doby použitelnosti CIR 2025/1566 je tak nutné se řídit požadavky článku 24 odst. 1, 1a a 1b nařízení eIDAS, ale není nutné se výlučně řídit požadavky uvedenými v CIR 2025/1566 (QTSP se nicméně musí na tyto požadavky dopředu připravit).

Pokud jde o ověření totožnosti/atributů žadatelů o vydání kvalifikovaného elektronického potvrzení atributů pomocí prostředků pro elektronickou identifikaci v souladu s článkem 24 odst. 1a písm. c) a 24 odst. 1b písm. d) nařízení eIDAS, uplatní se do doby použitelnosti CIR 2025/1566 požadavky uvedené v dokumentu Upřesnění ke kap. 2.3. a kap. 3 dokumentu DKP verze 4.

eIDAS - článek 24.2 písm. k): QTSP vydávající kvalifikované certifikáty vede a aktualizuje databázi certifikátů.

eIDAS - článek 24.3: Jestliže se QTSP vydávající kvalifikované certifikáty rozhodne určitý certifikát zneplatnit, zaeviduje toto zneplatnění ve své databázi certifikátů a zneplatnění certifikátu včas a v každém případě do 24 hodin od obdržení žádosti zveřejní. Zneplatnění nabývá účinku okamžitě po zveřejnění.

eIDAS - článek 24.4: Pokud jde o odstavec 3, kvalifikovaní poskytovatelé služeb vytvářejících důvěru vydávající kvalifikované certifikáty poskytnou kterékoli spoléhající se straně informace o platnosti nebo o zneplatnění kvalifikovaných certifikátů, které vydali. Tyto informace se poskytnou alespoň

na základě certifikátu, a to kdykoli i po skončení doby platnosti certifikátu, automatizovaným způsobem, který je spolehlivý, bezplatný a účinný.

4.1. Požadavky pro QTSP vydávající kvalifikované certifikáty pro elektronické podpisy a pečetě

Články 28.3, 38.3: Kvalifikované certifikáty pro elektronický podpis / pečeť mohou obsahovat nepovinné atributy. Těmito atributy nesmějí být dotčeny interoperabilita a uznávání kvalifikovaných elektronických podpisů.

Článek 28.4, 38.4: Pokud byl kvalifikovaný certifikát po počáteční aktivaci zneplatněn, ztrácí okamžikem zneplatnění platnost a jeho status se nemůže v žádném případě změnit zpět.

Požadavky na obsah kvalifikovaných certifikátů:

- Příloha I. nařízení eIDAS pro kvalifikované certifikáty pro elektronické podpisy podle článku 28.1
- Příloha III. nařízení eIDAS pro kvalifikované certifikáty pro elektronické pečeti podle článku 38.1

Bylo vydáno prováděcí nařízení Komise (EU) 2025/1943 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy pro kvalifikované certifikáty pro elektronické podpisy a kvalifikované certifikáty pro elektronické pečetě (dále jen „CIR 2025/1943“). CIR 2025/1943 odkazuje na ETSI EN 319 411-2, ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-5 a EN 319 412-3 (čistě jen pro QC pro el. pečeť) a zároveň modifikuje některá ustanovení těchto standardů.

Pokud QTSP při vydávání kvalifikovaných certifikátů pro el. podpisy / pečetě dodržuje normy, specifikace a postupy dle CIR 2025/1943, předpokládá se shoda s požadavky stanovenými v příloze I / III. nařízení eIDAS. Nicméně QTSP však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů.

V případě, kdy QTSP vydává spolu s kvalifikovanými certifikáty pro el. podpisy nebo el. pečetě rovněž i kvalifikované prostředky pro vytváření el. podpisů nebo pečetí, pak musí být zajištěno, aby tyto prostředky splňovaly požadavky přílohy II. nařízení eIDAS a rovněž, aby byly certifikovány v souladu s čl. 30 nařízení eIDAS příslušnými soukromými nebo veřejnými subjekty, které určily členské státy. Případně se musí jednat o prostředky, které se považují za kvalifikované prostředky pro vytváření elektronických podpisů do 21.května 2027 na základě přechodného opatření stanoveného ve článku 51(1) nařízení eIDAS.

Prováděcí rozhodnutí Komise (EU) 2016/650

Dne 26. 4. 2016 bylo zveřejněno v Úředním věstníku EU prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení eIDAS, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1438256835547&uri=CELEX:32016D0650. Prováděcí rozhodnutí stanovuje ve své příloze normy pro posuzování bezpečnosti produktů informačních technologií, které se mají použít pro certifikaci kvalifikovaných prostředků pro vytváření elektronických podpisů nebo kvalifikovaných prostředků pro vytváření elektronických pečetí, pokud jsou data pro vytváření

elektronických podpisů nebo data pro vytváření elektronických pečetí uchovávána v prostředí spravovaném zcela, nikoli však nutně výhradně uživatelem. Odkazované normy se mají použít pro certifikaci těch prostředků, které jsou ve fyzickém držení podepisující nebo pečetící osoby (např. čipová karta, USB token). V tomto případě jsou tedy stanoveny normy, které se mají povinně použít při certifikaci těch prostředků, které jsou ve fyzickém držení podepisující nebo pečetící osoby. Komise v blízké době zveřejní seznam certifikovaných kvalifikovaných prostředků pro vytváření elektronických podpisů a kvalifikovaných prostředků pro vytváření elektronických pečetí dle článku 31, respektive článku 39 nařízení eIDAS. Na tomto seznamu budou rovněž uvedeny prostředky, které se považují za kvalifikované prostředky pro vytváření elektronických podpisů a to na základě přechodného opatření stanoveného ve článku 51(1) nařízení eIDAS (*Prostředky pro bezpečné vytváření podpisu, jejichž shoda byla stanovena podle čl. 3 odst. 4 směrnice 1999/93/ES, se považují za kvalifikované prostředky pro vytváření elektronických podpisů podle tohoto nařízení*). Seznam certifikovaných prostředků má pouze informativní, nikoliv konstitutivní charakter.

Do doby, než Komise stanoví seznam norem pro posuzování bezpečnosti produktů informačních technologií, které se použijí pro certifikaci kvalifikovaných prostředků pro vytváření elektronických podpisů nebo kvalifikovaných prostředků pro vytváření elektronických pečetí, pokud data pro vytváření elektronických podpisů nebo data pro vytváření elektronických pečetí spravuje QTSP jménem podepisující osoby nebo pečetící osoby, je certifikace takových produktů založena na alternativním postupu, který používá srovnatelné úrovně bezpečnosti s normami odkazovanými v příloze rozhodnutí a který byl Komisi oznámen příslušným veřejným nebo soukromým subjektem.

Kromě vydávání „vlastních“ kvalifikovaných prostředků, může QTSP také certifikovat kryptografické klíče s příslušnou informací o uložení na kvalifikovaném prostředku, které byly vygenerovány v kvalifikovaném prostředku, jímž už uživatel disponuje. V tomto případě musí být zajištěno, aby QTSP implementoval příslušné postupy a procedury, které zajistí, že kryptografické klíče byly skutečně vygenerovány v kvalifikovaném prostředku (tj. zajištění původu klíče).

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	**Příslušné normy**
Vydávání kvalifikovaných certifikátů pro elektronické podpisy	ETSI EN 319 411 -2 ETSI EN 301 549 ETSI EN 319 412 -1 ETSI EN 319 412 -2 ETSI EN 319 412 -5 ETSI TS 119 461 ETSI EN 319 401
Vydávání kvalifikovaných certifikátů pro elektronické pečetě	ETSI EN 319 411 -2 ETSI TS 119 495 ETSI EN 301 549 ETSI EN 319 412 -1 ETSI EN 319 412 -2

	ETSI EN 319 412 -3 ETSI EN 319 412 -5 ETSI TS 119 461 ETSI EN 319 401

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

V případě prohlášení o souladu s normami řady ETSI EN 319 412 ze strany QTSP, CAB ověří na vzorku vydávaných certifikátů, zda-li formát těchto certifikátů je v souladu s ETSI EN 319 412-2, ETSI EN 319 412-3 a ETSI EN 319 412-5.

V případě, že QTSP deklaruje, že vydává certifikáty ve shodě se standardem S/MIME (Secure/Multipurpose Internet Mail Extensions), provede CAB ověření plnění tohoto standardu vůči požadavkům normy ETSI 119 411-6.

4.2. Požadavky pro QTSP vydávající kvalifikované certifikáty pro autentizaci internetových stránek

Článek 45.1 a 45.1b: Kvalifikované certifikáty pro autentizaci internetových stránek musí splňovat požadavky stanovené v příloze IV. Hodnocení shody s těmito požadavky se provádí v souladu s CIR 2025/2527. Kvalifikované certifikáty pro autentizaci internetových stránek nepodléhají žádným jiným závazným požadavkům.

Požadavky na obsah kvalifikovaných certifikátů:

- Příloha IV. nařízení eIDAS pro kvalifikované certifikáty pro autentizaci internetových stránek podle článku 45.1

Bylo vydáno prováděcí nařízení Komise (EU) 2025/2527 ze dne 16. prosince 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy pro kvalifikované certifikáty pro autentizaci internetových stránek (dále jen „CIR 2025/2527“), které se použije od 6. ledna 2027. QTSP při vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek musí tak nejpozději od 6. ledna 2027 dodržovat normy, specifikace a postupy dle tohoto CIR 2025/2527 s ohledem na to, že podle čl. 45 odst. 1 se hodnocení shody s požadavky přílohy IV. provádí v souladu s normami, specifikacemi a postupy uvedenými v CIR 2025/2527.

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	**Příslušné normy**
Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek	ETSI EN 319 411 -2 ETSI TS 119 411 -5 ETSI TS 119 495 ETSI EN 301 549 ETSI EN 319 412 -1

	ETSI EN 319 412 -4 ETSI EN 319 412 -5 ETSI TS 119 461 ETSI EN 319 401

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

5. Požadavky pro QTSP poskytující kvalifikovanou službu ověřování platnosti kvalifikovaných elektronických podpisů a/nebo kvalifikovaných elektronických pečetí

Požadavky pro QTSP poskytující kvalifikovanou službu ověřování platnosti kvalifikovaných elektronických podpisů a/nebo kvalifikovaných elektronických pečetí (s odkazem na čl. 33 a 40 nařízení eIDAS) se skládají z požadavků stanovených pro všechny QTSP (viz kapitola 3) a následujících:

eIDAS - článek 33.1 písm. a) : QTSP zajišťuje ověřování platnosti v souladu s čl. 32 odst. 1

eIDAS - článek 33.1 písm. b) : QTSP umožňuje, aby spoléhající se strany obdržely výsledek postupu ověření platnosti automatizovaným způsobem, který je spolehlivý, účinný a je opatřen zaručeným elektronickým podpisem nebo zaručenou elektronickou pečetí poskytovatele kvalifikované služby ověřování platnosti. V souladu s čl. 32 odst. 2, služba musí umožňovat zjistit jakékoli problémy týkající se bezpečnosti.

Bylo vydáno prováděcí nařízení Komise (EU) 2025/1942 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a kvalifikované služby ověřování platnosti kvalifikovaných elektronických pečetí (dále jen „CIR 2025/1942“). Pokud QTSP při poskytování kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů/pečetí dodržuje normy, specifikace a postupy dle CIR 2025/1942, předpokládá se shoda s požadavky stanovenými ve článku 33 a 40 nařízení eIDAS. Nicméně QTSP však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů.

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	**Příslušné normy**
Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů	ETSI TS 119 441 ETSI TS 119 442 ETSI EN 319 102 -1 ETSI TS 119 102 -2 ETSI TS 119 172 -4 ETSI EN 301 549 ETSI EN 319 401

Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických pečetí	ETSI TS 119 441 ETSI TS 119 442 ETSI EN 319 102 -1 ETSI TS 119 102 -2 ETSI TS 119 172 -4 ETSI EN 301 549 ETSI EN 319 401

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

S problematikou ověřování platnosti kvalifikovaných elektronických podpisů a pečetí souvisí i otázka formátů zaručených elektronických podpisů a pečetí, viz PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2026/248 ze dne 2. února 2026, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o formáty zaručených elektronických podpisů a zaručených elektronických pečetí uznávaných subjekty veřejného sektoru, a zrušuje prováděcí rozhodnutí Komise (EU) 2015/1506. Prováděcí rozhodnutí specifikuje formáty zaručených elektronických podpisů a zaručených elektronických pečetí, které mají členské státy uznávat v případě, že požadují pro využití určité online služby nabízené subjektem veřejného sektoru elektronicky podepsané dokumenty nebo elektronické dokumenty opatřené elektronickými pečetěmi. Seznam technických specifikací pro zaručené elektronické podpisy a pro zaručené elektronické pečetě je uveden v příloze tohoto prováděcího rozhodnutí.

CAB má k dispozici vlastní předem připravený vzorek elektronicky podepsaných dokumentů, na kterém ověří kvalitu ověřování platnosti kvalifikovaných elektronických podpisů/pečetí. Tento vzorek si může předem ověřit např. pomocí aplikace ETSI Signature Conformance Checker (https://signatures-conformance-checker.etsi.org/pub/index.shtml - kontrola souladu formátu AdES s ETSI TS / EN a demo DSS (https://ec.europa.eu/cefdigital/DSS/webapp-demo/home).

6. Požadavky pro QTSP poskytující kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů a/nebo kvalifikovaných elektronických pečetí

Požadavky pro QTSP poskytující kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů a/nebo kvalifikovaných elektronických pečetí (s odkazem na čl. 34 a 40 nařízení eIDAS) se skládají z požadavků stanovených pro všechny QTSP (viz kapitola 3) a následujících:

eIDAS - článek 34.1 : používání postupů a technologií, jež jsou s to zajistit důvěryhodnost kvalifikovaného elektronického podpisu i po uplynutí doby technické platnosti.

Bylo vydáno prováděcí nařízení Komise (EU) 2025/1946 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o kvalifikované služby uchovávání kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí (dále jen „CIR 2025/1946“). Pokud QTSP při poskytování kvalifikované služby uchovávání kvalifikovaných elektronických podpisů/pečetí dodržuje normy, specifikace a postupy dle

CIR 2025/1946, předpokládá se shoda s požadavky stanovenými ve článku 34 a 40 nařízení eIDAS. Nicméně QTSP však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů.

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	Příslušné normy
Kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů	ETSI TS 119 511 ETSI TS 119 172 -4 ETSI TS 119 512 ETSI EN 301 549 ETSI EN 319 401
Kvalifikovaná služba uchovávání kvalifikovaných elektronických pečetí	ETSI TS 119 511 ETSI TS 119 172 -4 ETSI TS 119 512 ETSI EN 301 549 ETSI EN 319 401

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

7. Požadavky pro QTSP vydávající kvalifikovaná elektronická časová razítka

Požadavky pro QTSP vydávající kvalifikovaná elektronická časová razítka (s odkazem na čl. 42 nařízení eIDAS) se skládají z požadavků stanovených pro všechny QTSP (viz kapitola 3) a následujících:

eIDAS - článek 42.1 : Kvalifikované elektronické časové razítko musí splňovat tyto požadavky:

- spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat;
- je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem; a
- je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou.

Bylo vydáno prováděcí nařízení Komise (EU) 2025/1929 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o spojení data a času s příslušnými daty a stanovení přesnosti zdrojů času pro poskytování kvalifikovaných elektronických časových razítek (dále jen „CIR 2025/1929“). Pokud QTSP při poskytování kvalifikovaných elektronických časových razítek dodržuje normy, specifikace a postupy dle CIR 2025/1929, předpokládá se shoda s požadavky stanovenými ve článku 42 nařízení eIDAS. Nicméně QTSP však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů.

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	Příslušné normy
Vytváření kvalifikovaných elektronických časových razítek	ETSI EN 319 421 ETSI EN 319 422 ETSI EN 301 549 ETSI EN 319 401

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

Soulad se standardem musí zajistit, že spojení data a času s daty je učiněno takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat a rovněž požadavky na zdroj přesného času, který je spojen s koordinovaným světovým časem.

8. Požadavky pro QTSP poskytující kvalifikovanou službu elektronického doporučeného doručování

Požadavky pro QTSP poskytující kvalifikovanou službu elektronického doporučeného doručování (s odkazem na čl. 44 nařízení eIDAS) se skládají z požadavků stanovených pro všechny QTSP (viz kapitola 3) a následujících:

eIDAS - článek 44.1 : Kvalifikované služby elektronického doporučeného doručování musí splňovat tyto požadavky:

- jsou poskytovány jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru;
- s vysokou úrovní spolehlivosti zajišťují identifikaci odesílatele;
- zajišťují identifikaci příjemce před doručením dat;
- odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat;
- odesílatel a příjemce dat jsou jednoznačně vyrozuměni o případných změnách dat potřebných za účelem odeslání nebo přijetí dat;
- datum a čas odeslání, přijetí a případná změna dat jsou označeny prostřednictvím kvalifikovaného elektronického časového razítka.

V případě přenosu dat mezi dvěma či více kvalifikovanými poskytovateli služeb vytvářejících důvěru se výše uvedené požadavky vztahují na všechny kvalifikované poskytovatele služeb vytvářejících důvěru.

Poskytovatelé kvalifikovaných služeb elektronického doporučeného doručování se mohou dohodnout na interoperabilitě mezi kvalifikovanými službami elektronického doporučeného doručování, které poskytují. Tento rámec interoperability musí splňovat požadavky stanovené ve článku 42 odstavci 1 a tato shoda musí být potvrzena subjektem posuzování shody.

Bylo vydáno prováděcí nařízení Komise (EU) 2025/1944 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy pro postupy odesílání a přijímání dat v rámci kvalifikovaných služeb elektronického doporučeného doručování a pokud jde o interoperabilitu těchto služeb (dále jen 2025/1944“). Pokud QTSP při poskytování kvalifikované služby elektronického doporučeného doručování dodržuje normy, specifikace a postupy dle CIR 2025/1944, předpokládá se shoda s požadavky stanovenými ve článku 44 nařízení eIDAS. Nicméně QTSP však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů.

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	Příslušné normy
Poskytování kvalifikovaných služeb elektronického doporučeného doručování	ETSI EN 319 521 ETSI EN 319 522 ETSI EN 319 531 ETSI EN 319 532 ETSI EN 301 549 ETSI TS 119 461 ETSI EN 319 401

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

V rámci vydaných ETSI standardů je definována obecná služba elektronického doporučeného doručování „Electronic Registered Delivery Service“ (dále jen „ERDS“) a dále specifický typ této služby založený na formátech, protokolech a mechanismech, které se běžně používají při výměně e-mailových zpráv, ale nabízející zvýšenou bezpečnost a průkaznost zpracování - Registered Electronic Mail Service (dále jen „REMS“). Pro účely kvalifikované služby elektronického doporučeného doručování, jsou stěžejní kvalifikované formy ERDS a REMS, tedy qualified ERDS (dále jen „QERDS“) a qualified REMS (dále jen „QREMS“).

V rámci technických specifikací řady TS 119 524 jsou pak definovány postupy kontrol, které mají být provedeny pro testování shody při poskytování ERDS podle specifických technických požadavků definovaných v řadě EN 319 522:

ETSI TS 119 524-1 Electronic Signatures and Infrastructures (ESI);Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 1: Testing conformance

ETSI TS 119 524-2 Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 2: Test suites for interoperability testing of Electronic Registered Delivery Service Providers

V rámci technických specifikací řady TS 119 534 jsou pak definovány postupy kontrol, které mají být provedeny pro testování shody při poskytování REMS podle specifických technických požadavků definovaných v řadě EN 319 532:

ETSI TS 119 534-1 Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 1: Testing conformance

ETSI TS 119 534-2 Electronic Signatures and Infrastructures (ESI);Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 2: Test suites for interoperability testing of providers using same format and transport protocols

9. Požadavky pro QTSP poskytující kvalifikovanou službu správy kvalifikovaných prostředků pro vytváření elektronických podpisů a/nebo pečetí na dálku

Požadavky pro QTSP poskytující kvalifikovanou službu správy kvalifikovaných prostředků pro vytváření elektronických podpisů a/nebo pečetí na dálku (s odkazem na čl. 29a a 39a nařízení eIDAS) se skládají z požadavků stanovených pro všechny QTSP (viz kapitola 3) a následujících:

eIDAS - článek 29a odst. 1 písm. a) / článek 39a: QTSP vytváří nebo spravuje data pro vytváření elektronických podpisů/pečetí jménem podepisující/pečetící osoby,

eIDAS - článek 29a. odst. 1 písm. b) / článek 39a: QTSP bez ohledu na přílohu II nařízení eIDAS bod 1 písm. d) kopíruje data pro vytváření elektronických podpisů/pečetí pouze pro účely zálohování, za splnění požadavků na stejnou úroveň bezpečnosti zkopírovaných souborů dat a původních souborů dat a zároveň počet zkopírovaných souborů dat nesmí přesáhnout minimum potřebné pro zajištění kontinuity služby,

eIDAS - článek 29a. odst. 1 písm. c) / článek 39a : QTSP splňuje všechny požadavky uvedené v certifikační zprávě konkrétního kvalifikovaného prostředku pro vytváření elektronických podpisů/pečetí na dálku vydané podle článku 30 eIDAS.

Bylo vydáno prováděcí nařízení Komise (EU) 2025/1567 ze dne 29. července 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o správu kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku a kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku jako služeb vytvářejících důvěru (dále jen „CIR 2025/1567“), které se použije od 19. srpna 2027. QTSP při poskytování služby správy kvalifikovaných prostředků pro vytváření elektronických podpisů/pečetí na dálku musí tak nejpozději od 19. srpna 2027 dodržovat normy, specifikace a postupy dle tohoto CIR 2025/1567 s ohledem na čl. 29a odst. 2 nařízení eIDAS.

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	**Příslušné normy**
Kvalifikovaná služba správy kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku	ETSI TS 119 431 -1 ETSI EN 301 549 ETSI TS 119 461 ETSI EN 319 401
Kvalifikovaná služba správy kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku	ETSI TS 119 431 -1 ETSI EN 301 549

	ETSI TS 119 461 ETSI EN 319 401

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

Pokud poskytovatel splňuje požadavky CIR 2025/1567 již před datem účinnosti prováděcího nařízení, lze posouzení shody poskytovatele a služby provést v souladu s požadavky CIR 2025/1567. Pokud poskytovatel zatím nemůže prokázat splnění požadavků CIR 2025/1567, pak může CAB před datem účinnosti prováděcího nařízení pro účely posouzení shody využít alternativní postup spočívající v ověření:

- platného certifikátu kvalifikovaného prostředku pro vytváření elektronických podpisů na dálku nebo elektronických pečetí na dálku
- splnění podmínek uvedených v certifikačním reportu, případně v další dokumentaci výrobce / dodavatele, které musejí být dodrženy, aby daný prostředek mohl být považován za kvalifikovaný prostředek pro vytváření elektronických podpisů/pečetí na dálku
- poskytovatel má implementovány procesy za účelem průběžné kontroly platnosti certifikace daného prostředku
- souladu s požadavky na uložení, aktivaci, zpřístupnění a správu soukromých klíčů podle Přílohy II nařízení eIDAS

CAB může využít následující standardy a normy pro účely ověření výše uvedených požadavků:

- ETSI TS 119 431-1:
  - ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev **nebo novější**
  - ETSI TS 119 431-1 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev
- ETSI TS 119 432 Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation
- ČSN ETSI EN 319 102-1 Elektronické podpisy a infrastruktury (ESI) - Postupy pro vytváření a ověřování platnosti digitálních podpisů AdES - Část 1: Vytváření a ověřování platnosti, kapitola 4 Vytváření podpisu
- ČSN EN 419 221-5 Profily ochrany pro TSP kryptografické moduly - Část 5: Kryptografický modul pro důvěryhodné služby
- ČSN EN 419 241-2 Důvěryhodné systémy podporující podpisový server - Část 2: Profil ochrany pro zařízení QSCD pro serverový podpis

10. Požadavky pro QTSP vydávající kvalifikované elektronické potvrzení atributů

Požadavky pro QTSP vydávající kvalifikovaná elektronická potvrzení atributů (s odkazem na čl. 45d nařízení eIDAS a přílohu V.) se skládají z požadavků stanovených pro všechny QTSP (viz kapitola 3) a následujících:

eIDAS - článek 24.1: *Při vydávání kvalifikovaného certifikátu nebo kvalifikovaného elektronického potvrzení atributů ověří kvalifikovaný poskytovatel služeb vytvářejících důvěru totožnost a případně*

zvláštní atributy fyzické nebo právnické osoby, jimž se má kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů vydat.

eIDAS - článek 24.1a: *Kvalifikovaný poskytovatel služeb vytvářejících důvěru provede ověření totožnosti uvedené v odstavci 1 vhodným způsobem buď přímo, nebo prostřednictvím třetí strany, a to na základě jedné z těchto metod nebo případně jejich kombinace a v souladu s prováděcími akty uvedenými v odstavci 1c:*

a) prostřednictvím evropské peněženky digitální identity nebo oznámených prostředků pro elektronickou identifikaci, které splňují požadavky stanovené v článku 8 eIDAS, pokud jde o vysokou úroveň záruky;

b) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaných v souladu s písmeny a), c) nebo d);

c) použitím jiných metod identifikace, které zajišťují identifikaci osoby s vysokou úrovní spolehlivosti, jejichž shodu potvrdí subjekt posuzování shody;

d) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby pomocí vhodných důkazů a postupů v souladu s vnitrostátním právem.

eIDAS - článek 24.1b: *Kvalifikovaný poskytovatel služeb vytvářejících důvěru provede ověření atributů uvedené v odstavci 1 vhodným způsobem buď přímo, nebo prostřednictvím třetí strany, a to na základě jedné z těchto metod nebo případně jejich kombinace a v souladu s prováděcími akty uvedenými v odstavci 1c:*

a) prostřednictvím evropské peněženky digitální identity nebo oznámených prostředků pro elektronickou identifikaci, které splňují požadavky stanovené v článku 8, pokud jde o vysokou úroveň záruky;

b) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaných v souladu s odst. 1a písm. a), c) nebo d);

c) pomocí kvalifikovaného elektronického potvrzení atributů;

d) použitím jiných metod, které zajišťují ověření atributů s vysokou úrovní spolehlivosti, jejichž shodu potvrdí subjekt posuzování shody;

e) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby pomocí vhodných důkazů a postupů v souladu s vnitrostátním právem.

eIDAS - článek 24.1c: *Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely ověřování totožnosti a atributů v souladu s odstavci 1, 1a a 1b tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.*

Na základě tohoto zmocnění bylo vydáno prováděcí nařízení Komise (EU) 2025/1566 ze dne 29. července 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční standardy pro ověřování totožnosti a atributů osob, jimž mají být vydány kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů (dále jen „CIR

2025/1566“). S ohledem na potřebu poskytnout dostatek času na přizpůsobení QTSP požadavkům prováděcího aktu, má tento prováděcí akt odloženou účinnost, přičemž se má použít od 19. srpna 2027.

Do doby použitelnosti CIR 2025/1566 je tak nutné se řídit požadavky článku 24 odst. 1, 1a a 1b nařízení eIDAS, ale není nutné se výlučně řídit požadavky uvedenými v CIR 2025/1566 (QTSP se nicméně musí na tyto požadavky dopředu připravit).

Pokud jde o ověření totožnosti/atributů žadatelů o vydání kvalifikovaného elektronického potvrzení atributů pomocí prostředků pro elektronickou identifikaci v souladu s článkem 24 odst. 1a písm. c) a 24 odst. 1b písm. d) nařízení eIDAS, uplatní se do doby použitelnosti CIR 2025/1566 požadavky uvedené v dokumentu Upřesnění ke kap. 2.3. a kap. 3 dokumentu DKP verze 4.

eIDAS - článek 24.4a: Jestliže se QTSP vydávající kvalifikovaná elektronická potvrzení atributů (dále jen QEAA) rozhodne určité QEAA zneplatnit, zaeviduje toto zneplatnění a zneplatnění certifikátu včas a v každém případě do 24 hodin od obdržení žádosti zveřejní. Zneplatnění nabývá účinku okamžitě po zveřejnění. QTSP vydávající QEAA poskytnou kterékoli spoléhající se straně informace o platnosti nebo o zneplatnění QEAA, které vydal. Tyto informace se poskytnou automatizovaným způsobem, který je spolehlivý, bezplatný a účinný.

Článek 45d.1: QEAA musí splňovat požadavky stanovené v příloze V.

Článek 45d.2: QEAA nepodléhají žádným závazným požadavkům kromě požadavků stanovených v příloze V.

Článek 45d.4: Pokud bylo QEAA po počátečním vydání zneplatněno, ztrácí okamžikem zneplatnění platnost a jeho status nelze v žádném případě změnit zpět.

Článek 45h.1: Poskytovatelé elektronického potvrzování atributů nesmějí kombinovat osobní údaje týkající se poskytování těchto služeb s osobními údaji z jiných služeb, které nabízejí oni nebo jejich obchodní partneři.

Článek 45h.2: Osobní údaje týkající se poskytování služeb elektronického potvrzování atributů jsou uchovávány logicky odděleně od jiných dat uchovávaných poskytovatelem elektronického potvrzování atributů.

Článek 45h.3: Poskytovatelé QEAA zavedou poskytování těchto kvalifikovaných služeb vytvářejících důvěru způsobem, který je funkčně oddělen od jiných jimi poskytovaných služeb.

Bylo vydáno prováděcí nařízení Komise (EU) 2025/1569 ze dne 29. července 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o kvalifikovaná elektronická potvrzení atributů a elektronická potvrzení atributů poskytovaná subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem (dále jen „CIR 2025/1569“). Pokud QTSP při vydávání QEAA dodržuje normy, specifikace a postupy dle CIR 2025/1569.

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	**Příslušné normy**
Vydávání kvalifikovaných elektronických potvrzení atributů	ETSI TS 119 471 ETSI EN 301 549 ETSI TS 119 461 ETSI EN 319 401

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

CAB akreditovaný k posuzování této služby může rovněž vydávat zprávu o posouzení shody dle článku 45f odst. 3 nařízení eIDAS týkající se vydávání elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem. V případě, kdy CAB vydává zprávu o posouzení shody dle článku 45f odst. 3 nařízení Evropského Parlamentu a Rady (EU) č. 910/2014, v platném znění, týkající se vydávání elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem, posuzuje splnění požadavků dle odstavců 1, 2 a 6 článku 45f nařízení č. 910/2014.

11. Požadavky pro QTSP poskytující kvalifikovanou službu elektronické archivace

Požadavky pro QTSP poskytující kvalifikovanou službu elektronické archivace (s odkazem na čl. 45j nařízení eIDAS) se skládají z požadavků stanovených pro všechny QTSP (viz kapitola 3) a následujících:

eIDAS - článek 45j.1: Kvalifikované služby elektronické archivace musí splňovat tyto požadavky:

- jsou poskytovány kvalifikovanými poskytovateli služeb vytvářejících důvěru;
- používají postupy a technologie umožňující zajistit trvanlivost a čitelnost elektronických dat a elektronických dokumentů i po uplynutí doby technologické použitelnosti – a alespoň po zákonně či smluvně stanovenou dobu uchovávání a současně zachovat jejich integritu a přesnost původu;
- zajišťují, aby byla elektronická data a elektronické dokumenty uchovávány způsobem, který je chrání před ztrátou a pozměněním, s výjimkou změn jejich nosiče nebo elektronického formátu;
- oprávněným spoléhajícím se stranám umožňují obdržet automatizovaným způsobem zprávu, která potvrzuje, že u elektronických dat a elektronických dokumentů získaných z kvalifikovaného elektronického archivu platí předpoklad integrity dat od začátku doby uchovávání do doby jejich zpřístupnění. Zpráva se poskytne spolehlivým a účinným způsobem a musí být opatřena kvalifikovaným elektronickým podpisem nebo kvalifikovanou elektronickou pečetí poskytovatele kvalifikované služby elektronické archivace.

Bylo vydáno prováděcí nařízení Komise (EU) 2025/2532 ze dne 16. prosince 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy a specifikace pro kvalifikované služby elektronické archivace (dále jen „CIR 2025/2532“). Pokud QTSP při poskytování kvalifikované služby elektronické archivace dodržuje normy, specifikace a postupy dle CIR 2025/2532, předpokládá se shoda s požadavky stanovenými ve článku 45j nařízení eIDAS. Nicméně QTSP však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 využívat i jiných postupů.

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	Příslušné normy
Poskytování kvalifikovaných služeb elektronické archivace	ISO 14641 ISO 14721

	CEN/TS 18170 ETSI EN 301 549 ETSI EN 319 401 ETSI EN 119 511

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

12. Požadavky pro QTSP poskytující kvalifikovanou elektronickou knihu záznamů

Požadavky pro QTSP poskytující kvalifikovanou elektronickou knihy záznamů (s odkazem na čl. 45I nařízení eIDAS) se skládají z požadavků stanovených pro všechny QTSP (viz kapitola 3) a následujících:

eIDAS - článek 45I.1 : Kvalifikované elektronické knihy záznamů musí splňovat tyto požadavky:

- jsou vytvářeny a spravovány jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru;
- identifikují původ datových záznamů v knize záznamů;
- zajišťují jedinečné sekvenční chronologické řazení datových záznamů v knize záznamů;
- zaznamenávají data takovým způsobem, že je možné okamžitě zjistit jakoukoliv následnou změnu dat, čímž zajišťují jejich integritu v čase.

V případě distribuované elektronické knihy záznamů je předmětem posouzení shody kvalifikovaná služba poskytovaná konkrétním kvalifikovaným poskytovatelem služeb vytvářejících důvěru (nebo kvalifikovanými poskytovateli služeb vytvářejících důvěru) a její vymezené provozní, organizační a bezpečnostní hranice, přičemž do posouzení budou zpravidla spadat zejména ty komponenty infrastruktury a subjekty, které mají přímý vliv na poskytování kvalifikované služby, zejména na

- zajištění zápisu datových záznamů,
- ověřování / validaci záznamů,
- určení nebo ovlivnění chronologického pořadí a finality,
- aplikaci governing rules[5] a mechanismu konsenzu[6],
- zajištění bezpečnosti, integrity a kontinuity služby,

a to s přihlédnutím k použité technologii a samotného řešení služby elektronické knihy záznamů. Komponenty, které pouze uchovávají kopii (repliku) dat bez možnosti ovlivnit jejich vznik, obsah,

[5] Soubor protokolů, politik a mechanismů, které určují, jak distribuovaný systém elektronické knihy záznamů funguje, jak jsou data ověřována a zapisována do knihy záznamů a jak spolu účastníci systému interagují.
[6] Soubor pravidel a postupů, jejichž prostřednictvím je mezi uzly distribuované elektronické knihy záznamů dosaženo shody o platnosti záznamů a o udržování jednotné a chronologicky uspořádané množiny ověřených záznamů.

integritu nebo pořadí, nebo nemají rozhodovací pravomoci v konsensu, se zpravidla nepovažují za součást rozsahu posouzení shody.

Způsob posouzení shody, včetně technického ověřování a bezpečnostních testů, se stanovuje s ohledem na povahu, rozsah a složitost poskytované kvalifikované služby. Při stanovení způsobu posouzení se vychází z rizik a z relevance jednotlivých komponent pro poskytování služby. Posouzení se zaměřuje zejména na ty části systému, které mají přímý vliv na plnění požadavků nařízení eIDAS. CAB při posouzení shody ověřuje, že poskytovatel řídí bezpečnost a systém řízení kvalifikované služby vytvářející důvěru v rámci perimetru kvalifikované služby vytvářející důvěru, a dále ověřuje naplnění požadavků stanovených pro kvalifikovanou elektronickou knihu záznamů. Způsob posouzení splnění těchto požadavků se odvíjí od použité technologii a samotného řešení služby elektronické knihy záznamů.

Bylo vydáno prováděcí nařízení Komise (EU) 2025/2531 ze dne 16. prosince 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy a specifikace pro kvalifikované elektronické knihy záznamů (dále jen „CIR 2025/2531“). Pokud QTSP při poskytování kvalifikované elektronické knihy záznamů dodržuje normy, specifikace a postupy dle CIR 2025/2531, předpokládá se shoda s požadavky stanovenými ve článku 45l nařízení eIDAS. Nicméně QTSP však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 využívat i jiných postupů.

Referenční normy pro režimy posuzování shody dle CIR 2025/2162:

Typ služby	**Příslušné normy**
Zaznamenávání elektronických dat do kvalifikované elektronické knihy záznamů	ETSI EN 319 401 ETSI EN 301 549 CEN/TS 18170 ISO 23257 ISO/TS 23635 ETSI EN 319 122 -1 ETSI EN 319 132 -1 ETSI TS 119 182 -1

Konkrétní verze standardů, viz příloha č. 1 k DKP – verze standardů.

13. Požadavky na základní obsah zprávy o posouzení shody

Subjekt posuzování shody musí po proběhlém posouzení shody vydat tzv. zprávu o posouzení shody („conformity assessment report“). Povinností subjektu posuzování shody je rovněž minimálně dle čl. 5 odst. 1 CIR 2025/2162 zveřejnit vydaný certifikát shody ve veřejném úložišti, které daný subjekt posuzování shody za tímto účelem udržuje.

Poskytovatel služeb vytvářejících důvěru musí předložit orgánu dohledu (Digitální a informační agentura) tuto zprávu nejen v souvislosti s oznámením o svém úmyslu zahájit poskytování

kvalifikované služby vytvářející důvěru, ale rovněž v souvislosti s pravidelným auditem (kvalifikovaní poskytovatelé služeb vytvářejících důvěru se na vlastní náklady alespoň jednou za 24 měsíců podrobí auditu ze strany subjektu posuzování shody) nebo v souvislosti s ad-hoc auditem (orgán dohledu může u QTSP na jejich náklady kdykoli provést audit nebo požádat subjekt posuzování shody o provedení posouzení shody za účelem potvrzení, že oni sami i jimi poskytované kvalifikované služby vytvářející důvěru splňují požadavky stanovené v tomto nařízení).

Obsah a náležitosti zprávy o posouzení shody je definován v příloze III. CIR 2025/2162. Zároveň zpráva o posouzení shody musí obsahovat bližší informace o délce trvání samotného posouzení shody a identifikaci verze dokumentu DKP použitého v rámci certifikace dané kvalifikované služby vytvářející důvěru.

Výše uvedené požadavky se uplatní přiměřeně rovněž v případě, kdy CAB vydává zprávu o posouzení shody dle článku 45f odst. 3 nařízení eIDAS týkající se elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem.

14. Přehled článků nařízení eIDAS při posuzování shody

Níže uvedená tabulka obsahuje seznam článků, jejichž splnění je předmětem posuzování shody konkrétní kvalifikované služby vytvářející důvěru ze strany subjektu posuzování shody.

Typ kvalifikované služby vytvářející důvěru	Seznam článků nařízení eIDAS
Vydávání kvalifikovaných certifikátů pro elektronické podpisy	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 28. Příloha I.
Vydávání kvalifikovaných certifikátů pro elektronické pečetě	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 38.

	Příloha III.
Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 45. Příloha IV.
Vydávání kvalifikovaných elektronických časových razítek	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 42.
Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a/nebo kvalifikovaných elektronických pečetí	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 32. článek 33. článek 40 (ověřování kvalifikovaných elektronických pečetí).
Kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů a/nebo kvalifikovaných elektronických pečetí	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24.

	článek 34. článek 40 (uchování kvalifikovaných elektronických pečetí).
Kvalifikovaná služba elektronického doručování	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 44.
Kvalifikovaná služba správy kvalifikovaných prostředků pro vytváření elektronických podpisů a/nebo pečetí na dálku	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 29a článek 39a (správa kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku).
Vydávání kvalifikovaných elektronických potvrzení atributů Subjekt posuzování shody akreditovaný k této činnosti může rovněž vydávat zprávu o posouzení shody dle článku 45f odst. 3 nařízení eIDAS, týkající se vydávání elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem.	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 45d článek 45h. článek 45g. V případě, kdy subjekt posuzování shody (certifikační orgán) vydává zprávu o posouzení shody dle článku 45f odst. 3 nařízení eIDAS týkající se vydávání elektronických potvrzení atributů vydaných subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho

	jménem, posuzuje splnění požadavků dle odstavců 1, 2 a 6 článku 45f nařízení č. 910/2014.
Kvalifikovaná služba elektronické archivace	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 45j.
kvalifikovaná elektronická kniha záznamů (zaznamenávání elektronických dat do kvalifikované elektronické knihy záznamů)	článek 2 odst. 4. článek 5. článek 13. článek 15. článek 20. článek 24. článek 45l.

15. Přílohy

Příloha	Popis
Příloha č. 1	V souladu s CIR 2025/2162 příloha obsahuje upřesnění verze norem standardů pro účely režimu posuzování shody.

16. Zkratky

Zkratka	Význam
DKP	Dokument konkretizující požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru.
Nařízení eIDAS	Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES), v platném znění.
QTS	Kvalifikovaná služba vytvářející důvěru.
CIR 2025/2162	Prováděcí nařízení Komise (EU) 2025/2162 ze dne 27. října 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o akreditaci subjektů posuzování shody provádějících posuzování kvalifikovaných poskytovatelů služeb vytvářejících důvěru a jimi poskytovaných kvalifikovaných služeb vytvářejících důvěru, zprávu o posouzení shody a režim posuzování shody.
CAB	Subjekt posuzování shody (conformity assessment body).
NAB	Národní akreditační orgán (national accreditation body).
Směrnice NIS2	Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148.
Zákon č. 264/2025 Sb.	Zákon č. 264/2025 Sb., o kybernetické bezpečnosti.
CIR 2024/2690	Prováděcí nařízení Komise (EU) 2024/2690 ze dne 17. října 2024, kterým se stanoví pravidla pro uplatňování směrnice (EU) 2022/2555, pokud jde o technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik a bližší upřesnění případů, v nichž se incident považuje za významný, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru.
CIR 2025/1566	prováděcí nařízení Komise (EU) 2025/1566 ze dne 29. července 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a

	Rady (EU) č. 910/2014, pokud jde o referenční standardy pro ověřování totožnosti a atributů osob, jimž mají být vydány kvalifikovaný certifikát nebo kvalifikované elektronické potvrzení atributů.
QTSP	Kvalifikovaný poskytovatel služeb vytvářejících důvěru (qualified trust service provider).
QTS	Kvalifikovaná služba vytvářející důvěru (qualified trust service).
TSP	Poskytovatel služeb vytvářejících důvěru (trust service provider).
REQ	Značí konkrétní požadavek uvedený v dané normě (REQ - requirement).
GDPR	Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), v platném znění.
CIR 2025/2160	Prováděcí nařízení Komise (EU) 2025/2160 ze dne 27. října 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy, specifikace a postupy pro řízení rizik spojených s poskytováním nekvalifikovaných služeb vytvářejících důvěru.
CIR 2025/2530	Prováděcí nařízení Komise (EU) 2025/2530 ze dne 16. prosince 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru poskytující kvalifikované služby vytvářející důvěru pro jednotlivé typy kvalifikovaných služeb vytvářejících důvěru.
CIR 2025/2527	Prováděcí nařízení Komise (EU) 2025/2527 ze dne 16. prosince 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy pro kvalifikované certifikáty pro autentizaci internetových stránek (dále jen „CIR 2025/2527“).
CIR 2025/1942	Prováděcí nařízení Komise (EU) 2025/1942 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a kvalifikované služby ověřování platnosti kvalifikovaných elektronických pečetí.
CIR 2025/1929	nařízení Komise (EU) 2025/1929 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o spojení data a času s příslušnými daty a stanovení přesnosti zdrojů času pro poskytování kvalifikovaných elektronických časových razítek.
AdES	Zaručený elektronický podpis / pečeť (Advanced electronic signature/seal).

DSS	Digital Signature Service.
CIR 2025/1943	prováděcí nařízení Komise (EU) 2025/1943 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy pro kvalifikované certifikáty pro elektronické podpisy a kvalifikované certifikáty pro elektronické pečetě.
CIR 2025/1946	prováděcí nařízení Komise (EU) 2025/1946 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o kvalifikované služby uchovávání kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí.
CIR 2025/1944	prováděcí nařízení Komise (EU) 2025/1944 ze dne 29. září 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy pro postupy odesílání a přijímání dat v rámci kvalifikovaných služeb elektronického doporučeného doručování a pokud jde o interoperabilitu těchto služeb.
CIR 2025/1567	prováděcí nařízení Komise (EU) 2025/1567 ze dne 29. července 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o správu kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku a kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku jako služeb vytvářejících důvěru.
ERDS	Electronic Registered Delivery Service.
QERDS	[Qualifed Electronic Registered Delivery Service.
REMS	Registered Electronic Mail Service.
QREMS	Qualified Registered Electronic Mail Service.
QEAA	Kvalifikovaná elektronická potvrzení atributů.
CIR 2025/1569	prováděcí nařízení Komise (EU) 2025/1569 ze dne 29. července 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o kvalifikovaná elektronická potvrzení atributů a elektronická potvrzení atributů poskytovaná subjektem veřejného sektoru odpovědným za autentický zdroj nebo jeho jménem.
CIR 2025/2532	Bylo vydáno prováděcí nařízení Komise (EU) 2025/2532 ze dne 16. prosince 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy a specifikace pro kvalifikované služby elektronické archivace.

17. Zdroje

[1]	ENISA: Analysis of standards related to Trust Service Providers Mapping of requirements of eIDAS to existing standards, https://www.enisa.europa.eu/publications/tsp_standards_2015.
[2]	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění. Konsolidované informativní znění: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:02014R0910-20241018.
[3]	PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1438256835547&uri=CELEX:32016D0650.
[4]	PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2015/1506 ze dne 8. září 2015, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru podle čl. 27 odst. 5 a čl. 37 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006.
[5]	ENISA: Article 19 Incident reporting, https://www.enisa.europa.eu/publications/article19-incident-reporting-framework.
[7]	Prováděcí akty vydané v souvislosti s revidovaným nařízením eIDAS jsou k dispozici na: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931811/The+European+Digital+Identity+Regulation?all=1#sec-6-regulations.
[8]	ověření totožnosti/atributů žadatelů o vydání kvalifikovaného certifikátu/kvalifikovaného elektronického potvrzení atributů pomocí prostředků pro elektronickou identifikaci uvedené v dokumentu Upřesnění ke kap. 2.3. a kap. 3 dokumentu DKP verze 4, https://www.dia.gov.cz/media/2203/download/Upresneni_ke_kapitole_2-3_a_kapitole_3_dokumentu_DKP_-_20220921.pdf?v=1.
[9]	upřesnění k DKP s názvem Používání kryptografických algoritmů při poskytování kvalifikovaných služeb vytvářejících důvěru s ohledem na

	problematiku používání algoritmu RSA s délkou klíče 2048 bitů, https://www.dia.gov.cz/media/3157/download/Up%C5%99esn%C4%9Bn%C3%AD%20ke%20kap.%202.2%20dokumentu%20DKP.pdf?v=1.

Filip Bílek

Digitálně podepsal Filip Bílek
Datum: 2026.05.15 07:38:06 +02'00'