MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

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

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

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) 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. Nutno podotknout, že některé požadavky nařízení nejsou pokryty stávajícími technickými normami, standardy a specifikacemi. 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.

Požadavky vychází z normy **ČSN EN ISO/IEC 17065 (CONFORMITY ASSESSMENT -- REQUIREMENTS FOR BODIES CERTIFYING PRODUCTS, PROCESSES AND SERVICES)** 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 EN 319 403 (ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); TRUST SERVICE PROVIDER CONFORMITY ASSESSMENT - REQUIREMENTS FOR CONFORMITY ASSESSMENT BODIES ASSESSING TRUST SERVICE PROVIDERS)** a specifikují jak obecné požadavky na CABy, tak i obecná pravidla pro provádění příslušných auditů. Součástí ČSN EN 319 403 jsou rovněž výše uvedené aplikovatelné požadavky norem ČSN EN ISO/IEC 17021-1 a ČSN ISO/IEC 27006[1].

[1] Viz ustanovení z ČSN EN 319 403: „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].“

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 by mělo probíhat samotné posuzování shody ze strany CABů u QTSP. Podle normy **ČSN EN 319 403** 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 EU 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** je rovněž umožnit posouzení shody podle osvědčených postupů z praxe a stejně také podle technických požadavků nařízení eIDAS.

2. Požadavky na poskytovatele služeb vytvářejících důvěru (trust service provider, dále jen „TSP“)

2.1. Společné požadavky pro všechny TSP

Zpracování a ochrana údajů:

eIDAS - článek 5.1: Zpracování osobních údajů se provádí v souladu s nařízením (EU) 2016/679 (známé pod zkratkou GDPR)[2].

eIDAS - článek 5.2: Aniž jsou dotčeny právní účinky, které vnitrostátní právo přiznává pseudonymům, není používání pseudonymů v elektronických transakcích zakázáno.

eIDAS článek 5(1)	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. Poznámka: Soulad s EN 319 411-2 (QTSP vydávající QCs) a soulad s EN 319 421 (QTSP vydávající kvalifikovaná elektronická časová razítka) vyžaduje rovněž soulad s kapitolou 7.13, REQ-7.13-05 EN 319 401.

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.

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

[2] Nařízení eIDAS obsahuje odkaz na původní směrnici 95/46/ES, která se s účinkem ode dne 25. května 2018 zrušila. Odkazy na zrušenou směrnici se považují za odkazy na 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). Z tohoto důvodu text požadavku čl. 5 již obsahuje přímo odkaz na GDPR i když normativní text nařízení eIDAS se odvolává ještě na původní směrnici.

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

- 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.

eIDAS článek 13(2)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Kapitola 6.2 Pozn.: Soulad s EN 319 411-2 (QTSP vydávající QCs) a soulad s EN 319 421 (QTSP vydávající kvalifikované elektronické časové razítka) vyžaduje rovněž soulad s kapitolou 6.2 v EN 319 401.
	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.

Přístupnost pro osoby se zdravotním postižením:

eIDAS - článek 15: Je-li to proveditelné, měly by být poskytované služby vytvářející důvěru a konečné uživatelské produkty používané při poskytování těchto služeb dostupné osobám se zdravotním postižením.

eIDAS článek 15	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Kapitola REQ-7.13-03vyžaduje, 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). Pozn: Soulad s EN 319 411-2 (QTSP vydávající QCs) a soulad s EN 319 421 (QTSP vydávající kvalifikované elektronické časové razítka) vyžaduje rovněž soulad s kapitolami REQ-7.13-03 a kap. REQ-7.13-04 EN 319 401.
	Accessibility requirements suitable for public procurement of ICT products and services in Europe (ETSI EN 301 549) Design for All - Accessibility following a Design for All approach in products, goods and services - Extending the range of users (EN 17161)	

<u>Bezpečnostní požadavky vztahující se na poskytovatele služeb vytvářejících důvěru:</u>

<u>eIDAS - článek 19.1:</u> Poskytovatel služeb vytvářejících důvěru musí

- přijmout vhodná technická a organizační opatření k řízení rizik ohrožujících bezpečnost jím poskytovaných služeb vytvářejících důvěru,
- s ohledem na nejnovější technologický vývoj musí tato opatření zajišťovat úroveň bezpečnosti, která je přiměřená míře rizika,
- přijmout opatření k zabránění bezpečnostním incidentům, k minimalizaci jejich dopadů a k informování zúčastněných stran o nepříznivých dopadech těchto incidentů.

eIDAS článek 19(1)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Kapitola 5 (hodnocení rizik) však neobsahuje striktní požadavky na implementaci vybraných opatření(“select” to become “implement”). Kapitola 6.3 týkající se politiky informační bezpečnosti. Kapitola 7 (s výjimkou 7.1.1 & 7.13). Další požadavky stanovené v kapitole 6.4 (zařízení, management a provozní kontroly) a v kapitole 6.5 (technické bezpečnostní kontroly) normy EN 319 411-1 se považují za nutné (obecně pro všechny TSP pokryté nařízením eIDAS) vzhledem k povinnosti splnění požadavků stanovených ve článku 19.1 nařízení eIDAS. Z tohoto důvodu je vyžadováno: - Pro TSP vydávající certifikáty soulad s normou EN 319 411-1 kapitolami 6.4 a 6.5. - Pro TSP vydávající časová razítka soulad s příslušnými kapitolami EN 319 421.
	Pro TSP vydávající certifikáty: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (EN 319 411-1)	Jednou z možností, jak demonstrovat soulad požadavků čl. 19(1) pro TSP vydávající certifikáty, je splnění požadavků kapitol 6.4 a 6.5 ETSI EN 319 411-1.

	Pro TSP vydávající elektronická časová razítka: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (ETSI EN 319 421)	Jednou z možností, jak demonstrovat soulad požadavků čl. 19(1) pro TSP vydávající elektronická časová razítka, je splnění požadavků kapitol 7.8, 7.9, 7.10, 7.12, a 7.13 ETSI EN 319 421.

Oznamování o narušení bezpečnosti a porušení ochrany osobních údajů:

eIDAS - článek 19.2: TSP musí:

- vyrozumět orgán dohledu a případné další příslušné subjekty, jako jsou příslušný vnitrostátní orgán pro bezpečnost informací nebo orgán pro ochranu údajů, o každém narušení bezpečnosti nebo ztrátě integrity, jež mají významný dopad na poskytovanou službu vytvářející důvěru nebo na uchovávané osobní údaje, a to bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy toto narušení zjistili.
- vyrozumět o daném narušení bezpečnosti nebo dané ztrátě integrity bez zbytečného odkladu také tuto fyzickou nebo právnickou osobu, může-li mít narušení bezpečnosti nebo ztráta integrity nepříznivý dopad na tuto osobu.
- informovat veřejnost, pokud je zveřejnění informací o narušení bezpečnosti nebo ztrátě integrity ve veřejném zájmu a byl o to požádán orgánem dohledu.

eIDAS článek 19(2)	General Policy Requirements for Trust Service Providers (ETSI EN 319 401)	Kapitola 7.9 (zejména REQ-7.9-07 a REQ-7.9-08) Pozn: Soulad s EN 319 411-2 (QTSP vydávající kvalifikované certifikáty) a soulad s EN 391 421 (QTSP vydávající kvalifikovaná elektronická časová razítka) vyžaduje soulad s EN 319 401 kapitolou 7.9.

Neexistují žádné konkrétní ETSI standardy určené speciálně pro řešení problematiky řízení rizik a přijmutí technických a organizačních opatření, které musí TSP implementovat a jenž zaručí bezpečnost poskytovaných služeb. Lze se nicméně např. řídit normou ČSN ISO 31000 obsahující směrnice pro řízení rizik, kterým jsou organizace vystaveny. Aplikování těchto směrnic může být přizpůsobeno pro jakoukoli organizaci a její kontext. Norma poskytuje společný přístup pro řízení jakéhokoliv typu rizika a není specifický ani pro průmysl, ani pro sektory. Normu lze využívat po celou dobu života organizace a může se použít na jakoukoliv činnost, včetně rozhodování na všech

úrovních. Jako další příklad obecné normy, kterou se lze řídit, lze uvést normu ČSN ISO/IEC 27005 obsahující směrnice pro řízení rizik bezpečnosti informací s podporou obecných konceptů specifikovaných v ISO/IEC 27001 a v ISO/IEC 27002. Norma je navržena tak, aby podporovala úspěšnou implementaci bezpečnosti informací na základě přístupu k řízení přístupu.

Neexistují ani standardy obsahující požadavky na formáty a postupy, včetně lhůt, použitelné pro účely oznámení o narušení bezpečnosti a oznámení o narušení bezpečnosti osobních údajů. Nicméně dokument od agentury ENISA [6] rozpracovává tuto oblast - obsahuje užitečné informace popisující jednotlivé toky informací v případě oznamování bezpečnostních incidentů, navrhuje věcný obsah reportů, „číselník“ aktiv i hodnocení závažnosti s ohledem na integritu, dostupnost a důvěrnost.

Obě oblasti (řízení rizik a přijmutí technických a organizačních opatření) jsou nicméně řešeny v souvislosti s poskytováním konkrétních služeb vytvářejících důvěru. Aktuálně jsou k dispozici standardy pro vydávání kvalifikovaných certifikátů a pro vydávání kvalifikovaných elektronických časových razítek.

2.2. Společné požadavky pro všechny QTSP

Společné požadavky pro všechny QTSP se skládají jednak z požadavků na všechny poskytovatele služeb vytvářejících důvěru (viz kapitola 2.1) a dále také z požadavků stanovených ve článku 24.2 nařízení eIDAS:

- oznámit orgánu dohledu případné změny v poskytování svých kvalifikovaných služeb vytvářejících důvěru a záměr ukončit své činnosti (nový požadavek v porovnání se směrnicí 1999/93/EC)
- 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 (podobné požadavkům přílohy II písm. e) směrnice 1999/93/EC)
- udržovat dostatečné finanční prostředky nebo uzavřít vhodné pojištění odpovědnosti v souladu s vnitrostátním právem s ohledem na odpovědnost za škodu (podobné požadavkům přílohy II písm. h) směrnice 1999/93/EC)
- informovat jasným a srozumitelným způsobem osobu, která chce využít kvalifikovanou službu vytvářející důvěru před uzavřením smluvního vztahu, o přesných podmínkách používání této služby, včetně případných omezení jejího využívání (podobné požadavkům přílohy II písm. k) směrnice 1999/93/EC)
- používat důvěryhodné systémy a produkty, které jsou chráněny proti pozměnění, a zajišťovat technickou bezpečnost a spolehlivost procesů, které podporují (podobné

požadavkům přílohy II písm. f) směrnice 1999/93/EC a spolehlivosti podporovaných procesů)

- používat důvěryhodné systémy k uchovávání dat, která jsou mu poskytnuta, v ověřitelné podobě (nový požadavek v porovnání se směrnicí 1999/93/EC)
- přijímat vhodná opatření proti padělání a odcizení dat (zobecnění přílohy II písm. g) směrnice 1999/93/EC)
- 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 (zobecnění přílohy II písm. i) směrnice 1999/93/EC, nový požadavek na evidenci a zpřístupnění i po ukončení činnosti)
- mít k dispozici aktualizovaný plán ukončení činnosti k zajištění kontinuity služby (nový požadavek v porovnání se směrnicí 1999/93/EC)
- zajistit zákonné zpracovávání osobních údajů v souladu se směrnicí 95/46/ES (podobné požadavkům článku 8 směrnice 1999/93/EC)

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. Poskytovatelé předloží výslednou zprávu o posouzení shody do tří pracovních dnů od jejího obdržení orgánu dohledu (tj. Ministerstvu vnitra).
- 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.
- Pokud QTSP nenapraví neplnění požadavků nařízení eIDAS do (případně) stanovené lhůty orgánem dohledu, 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.

Postup pro zahájení poskytování kvalifikované služby vytvářející důvěru:

- Pokud mají poskytovatelé služeb vytvářejících důvěru bez statusu kvalifikovaného poskytovatele v úmyslu začít poskytovat kvalifikované služby vytvářející důvěru, předloží orgánu dohledu oznámení o svém úmyslu společně se zprávou o posouzení shody vydanou subjektem posuzování shody.
- Orgán dohledu ověří, zda poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru splňují požadavky stanovené v nařízení eIDAS.
- Dojde-li orgán dohledu k závěru, že poskytovatel služeb vytvářejících důvěru a jím poskytované služby vytvářející důvěru splňují požadavky, udělí orgán dohledu tomuto poskytovateli služeb vytvářejících důvěru a jím poskytovaným službám vytvářejícím důvěru status kvalifikovaného poskytovatele a kvalifikované služby, a to do tří měsíců od obdržení oznámení. Není-li ověření dokončeno do tří měsíců od oznámení, vyrozumí orgán dohledu poskytovatele 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.

eIDAS článek 20(1)	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Není řešeno v EN 319 411-2, odkazováno na požadavky EN 319 411-1 - kapitola 6.7. obsahuje pouze poznámku s odkazem na ČSN EN 319 403. Nicméně ČSN EN 319 403 se vztahuje na (akreditované) subjekty posuzování shody. Zajištění nápravy po nalezení neshody při auditu nebo náprava nesouladu nejsou těmito standardy řešeny. Není řešeno v EN 319 401.
	EN 319 421 (QTSP vydávající kvalifikovaná el. časová razítka)	Viz komentář výše.

eIDAS článek 21(1)	Žádné ETSI/CEN standardy nejsou dostupné nebo pokrývající formáty a postupy pro účely článku 21(1).	
eIDAS článek 21(2)	Žádné ETSI/CEN standardy nejsou dostupné nebo pokrývající formáty a postupy pro účely článku 21(2).	
eIDAS článek 24(2). a	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Řešeno v EN 319 411-2 prostřednictvím kapitoly 5.2 s odkazem na použitelné požadavky EN 319 411-1. Kapitola 5.2 EN 319 411-1 odkazuje na použitelné požadavky uvedené v kapitole 6.1 EN 319 401.
	EN 319 421 (QTSP vydávající kvalifikovaná el. časová razítka)	Řešeno v EN 319 421 prostřednictvím kapitoly 6.2, s odkazem na použitelné požadavky uvedené v kapitole 6.1 normy EN 319 401.
eIDAS článek 24(2). b	EN 319 401 (QTSP poskytující kvalifikované služby vytvářejcící důvěru)	Kap. REQ-7.1.2-01 a kap. 7.2 EN 319 401.
	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitola 6.4.4 s odkazem na 6.4.4 EN 319 411-1 na základě kapitoly 7.2 EN 319 401. Kapitola 6.9.1 s odkazem na 6.9.1 EN 319 411-1 na základě kapitoly 7.1. EN 319 401.

	EN 319 421 (QTSP vydávající kvalifikovaná el. časová razítka)	Kapitola 7.2 & 7.3 s odkazem na použitelné požadavky v EN 319 401 (kapitoly 7.1 a 7.2).
eIDAS článek 24(2).c	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitola 6.8.2 s odkazem na kapitolu 6.8.2 EN 319 411-1 na základě kapitoly REQ-7.1.1-04EN 319 401.
	EN 319 421 (QTSP vydávající kvalifikovaná el. časová razítka)	Kapitola 7.2 s odkazem na použitelné požadavky kapitoly 7.1. EN 319 401 (včetně kapitoly REQ-7.1.1-04).
eIDAS článek 24(2). d	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitoly 6.1, 6.3.4, 6.3.5 a 6.9.4 s odkazem na kapitoly 6.1, 6.3.4, 6.3.5 a 6.9.4 EN 319 411-1 (kapitola 6.9.4 navazuje na kapitolu 6.2. EN 319 401)
	EN 319 421 (QTSP vydávající kvalifikovaná el. časová razítka)	Kapitola 6.3 s odkazem na použitelné požadavky EN 319 401 (kapitola 6.2).

eIDAS články 24(2). e& 24(2).f	Zde záleží, jaký typ procesu v rámci konkrétního typu služby má být prostřednictvím důvěryhodného systému podporován stejně jako v případě různého způsobu poskytování služby vzdáleného podepisování (vytváření nebo správa dat pro vytváření elektronických podpisů), tj. podpora vzdáleného podepisování zaručeným či kvalifikovaným el. podpisem. Kandidátské standardy: - EN 419 221 (Security requirements for trustworthy systems managing certificates for electronic signatures)- profily ochrany pro kryptografické moduly používané poskytovateli, zejména část 5 - profil ochrany pro kryptografické moduly používané poskytovateli. - EN 419 231 profil ochrany pro důvěryhodné systémy podporující proces vydávání časových razítek. - EN 419 241-1 bezpečnostní požadavky a EN 419 241-2 profil ochrany pro zařízení QSCD pro serverový podpis. - CEN/TS 419 261 (původně prTS 419 221-1, původně prTS 14167-1) – bezpečnostní požadavky pro důvěryhodné systémy spravující certifikáty a časová razítka. EN 319 411-2 a EN 319 421 obsahují požadavky na QTSP na využívání důvěryhodných systémů odkazovaných prostřednictvím článku 24(2).e a 24(2).f . Splnění požadavků čl. 24(2) písm. e) může být prokázáno hodnocením systému řízení bezpečnosti informací dle ČSN ISO/IEC 27002 nebo jiného obdobného standardu. V případě, že systém není hodnocen, pak může být splnění požadavků čl. 24(2) písm. e) prokázáno rovněž splněním požadavků REQ-7.7-02 až REQ-7.7-09 EN 319 401. Soulad s požadavky čl. 24(2) písm. f) implikuje rovněž splnění požadavku REQ-7.3.2-01 EN 319 401 (zásada bezpečného zacházení s medii s ohledem na jejich obsah a případná likvidace, pokud nejsou zapotřebí).	
eIDAS článek 24(2). g	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitoly 6.4 a 6.5 s odkazem na EN 319 411-1 kapitoly 6.4 a 6.5, které navazují na EN 319 401.

	EN 319 421 (QTSP vydávající kvalifikovaná el. časová razítka)	Kapitoly 6.1, 6.4 & 7 navazující na EN 319 401.
eIDAS článek 24(2). h	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitoly 6.2.2, 6.3.4, 6.3.8, 6.4.5, 6.4.6, a 6.4.9 s odkazem na EN 319 411-1 navazující na EN 319 401.
	EN 319 421 (QTSP vydávající kvalifikovaná el. časová razítka)	Kapitoly 7.6.5, 7.7.2, 7.8 a 7.12 navazující na EN 319 401.
eIDAS článek 24(2).i	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitola 6.4.9 s odkazem na kapitolu 6.4.9 EN 319 411-1 navazující na EN 319 401 kapitolu 7.12.
	EN 319 421 (QTSP vydávající kvalifikovaná el. časová razítka)	Kapitola 7.14 navazující na EN 319 401 kapitolu 7.12.
eIDAS článek 24(2).j	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitoly 6.8.4 a 6.8.15 s odkazem na kapitolu 6.8.4 a 6.8.15 EN 319 411-1 navazující na EN 319 401 kapitolu 7.13.
	EN 319 421 (QTSP vydávající kvalifikovaná el. časová razítka)	Kapitola 7.15 navazující na kapitolu 7.13 EN 319 401.

2.3. Požadavky pro QTSP vydávající kvalifikované certifikáty

Požadavky pro QTSP vydávající kvalifikované certifikáty se skládají jednak z požadavků na všechny poskytovatele služeb vytvářejících důvěru (viz kapitola 2.1), dále také z požadavků stanovených pro všechny QTSP (viz kapitola 2.2) a následujících:

eIDAS - článek 24.1:

> *Při vydávání kvalifikovaného certifikátu pro službu vytvářející důvěru ověří kvalifikovaný poskytovatel služeb vytvářejících důvěru pomocí vhodných prostředků a v souladu s vnitrostátním právem totožnost a případně zvláštní znaky fyzické nebo právnické osoby, jíž je kvalifikovaný certifikát vydáván.*
>
> *Kvalifikovaný poskytovatel služeb vytvářejících důvěru ověří informace uvedené v prvním pododstavci přímo nebo tím, že se v souladu s vnitrostátním právem spolehne na třetí osobu:*
>
> *a) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby; nebo*
> *b) na dálku s využitím prostředku pro elektronickou identifikaci, u něhož byla před vydáním kvalifikovaného certifikátu zajištěna fyzická přítomnost fyzické osoby nebo oprávněného zástupce právnické osoby a jenž splňuje požadavky stanovené v článku 8, pokud jde o značnou nebo vysokou úroveň záruky; nebo*
> *c) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti, vydaného v souladu s písmenem a) nebo b); nebo*
> *d) pomocí jiných identifikačních metod uznávaných na vnitrostátní úrovni, které poskytují záruku spolehlivosti rovnocennou fyzické přítomnosti. Tuto rovnocennou záruku musí potvrdit subjekt posuzování shody.*

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.

Požadavky na obsah kvalifikovaných certifikátů:

- Příloha I. nařízení eIDAS pro kvalifikované certifikáty pro elektronické podpisy podle článku 28.1
- Příloha II. nařízení eIDAS pro kvalifikované certifikáty pro elektronické pečeti podle článku 38.1
- Příloha IV. nařízení eIDAS pro kvalifikované certifikáty pro autentizaci internetových stránek podle článku 45.1

Článek 28.3, 38.3, recitál č. 65: Kvalifikované certifikáty mohou obsahovat nepovinné atributy. Těmito atributy nesmějí být dotčeny interoperabilita a uznávání kvalifikovaných elektronických podpisů.

Článek 28.4, 38.4, recitál č. 65: Pokud byl kvalifikovaný certifikát po počáteční aktivaci zneplatněn, ztrácí okamžikem zneplatnění platnost a jeho status se nemůže v žádném případě změnit zpět.

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 a 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 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. 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).

eIDAS článek 24(1)	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitoly 6.2.2 a 6.2.3 s odkazem na související kapitoly 6.2.2 a 6.2.3 EN 319 411-1. Pozn.*: S ohledem na požadavky stanovené ve článku 24.1.(b) nařízení eIDAS je nutné použít prostředek pro elektronickou identifikaci, u kterého byla před vydáním QC zajištěna fyzická přítomnost fyzické osoby nebo oprávněného zástupce právnické osoby, bez ohledu na to, zda se jedná o prostředek se značnou nebo vysokou úrovní záruky.*
eIDAS článek 24(2).k	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitola 6.1 s odkazem na související kapitolu 6.1. EN 319 411-1.

eIDAS článek 24.3	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitola 6.2.4 s odkazem na související kapitolu 6.2.4. EN 319 411-1.
eIDAS článek 24.4	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitola 6.3.10 s odkazem na související kapitolu 6.3.10 EN 319 411-1. Pozn.: požadavek na bezplatné poskytování informací o platnosti QC není řešen v normě EN 319 411-2 –mimo rozsah normy.
Pozn: S ohledem na soulad s články 24.3 a 24.4 nařízení eIDAS, předpokládá se, že norma EN 319 411-2 neobsahuje dostatečné opatření, pokud jde o CRL a OCSP profily a proces jejich tvorby a dodržení požadavků stanovených ve zmíněných článcích. Tabulka A.1 v příloze A (informativní) EN 319 411-2 obsahuje check list týkají se požadavků na QTSP vydávající QC dle politiky QCP z nařízení eIDAS vůči požadavkům této technické normy. Tabulka neobsahuje mapování všech požadavků nařízení eIDAS kladené na QTSP vydávající QC dle politiky QCP, jelikož některé požadavky nařízení eIDAS nejsou technické povahy a nespadají do oblasti působnosti EN 319 411-2.		

eIDAS článek 28(1) & Příloha I eIDAS článek 38(1) & Příloha III eIDAS články 28(3) & 38(3) eIDAS články 28(4) & 38(4) eIDAS článek 45(1) & Příloha IV	EN 319 411-2 (QTSP vydávající kvalifikované certifikáty)	Kapitola 6.6.1 s odkazem na související kapitolu 6.6.1 EN 319 411-1 a vyžadující soulad s příslušnou normou řady EN 319 412 (profil certifikátu) v závislosti na typu QC. Kapitola 6.3.9 s odkazem na souvisící kapitolu 6.3.9. EN 319 411-1. *Pozn.: Namísto vydávání nového kvalifikovaného prostředku pro vytváření el. podpisů, může chtít QTSP certifikovat veřejné klíče, které byly vygenerovány ve kvalifikovaném prostředku, který je již v rukou uživatele, případně je provozovaný vzdáleně v souladu s přílohou II. odst. 3. V tomto případě musí QTSP pomocí příslušných prostředků před vydáním kvalifikovaného certifikátu ověřit, že související soukromý klíč k veřejnému klíči byl vygenerován v kvalifikovaném prostředku (viz článek 3(12) nařízení eIDAS). EN 319 411-2 kapitoly SDP-6.5.1-02, SDP-6.5.1-03, SDP-6.5.1-07, 6.5.2, 6.3.5, a 6.3.12.*
eIDAS článek 28(5) eIDAS článek 38(5)		Dočasné pozastavení platnosti kvalifikovaných certifikátů pro elektronický podpis a pro elektronickou pečeť může být specifikováno na národní úrovni.

ETSI EN 319 412 by měla obsahovat dostatečné požadavky na zajištění, aby QTSP vydávající kvalifikované certifikáty splňoval použitelné požadavky nařízení eIDAS na obsah certifikátů.

Řada norem **ETSI EN 319 412** se skládá z celkem pěti částí:

ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

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

2.3.1 Požadavky pro QTSP vydávající kvalifikované certifikáty pro autentizaci internetových stránek

eIDAS článek 45(2)	Baseline requirements for the issuance and management of publicly-trusted certificates (CAB Forum CAB BR)	Částečně pokryto, viz níže.
	EV SSL certificate guidelines (CAB Forum CAB EVSSL)	Částečně pokryto, viz níže.
	Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates (ETSI TR 103 123)	Dokument s pokyny pro auditory (menší rozsah požadavků než je předpokládán v nařízení eIDAS)

Technical report TR 101 564 on guidance on ETSI TS 102 042 for issuing EV certificates for auditors and CSPs	Určeno pro použití auditory jako metodické pokyny pro posouzení, zda je CA v souladu s TS 102 042 a použití rovněž pro CA k osvětlení požadavků.
Electronic Signatures and Infrastructures (ESI);Certificate Profiles;Part 4: Certificate profile for web site certificates ETSI EN 319 412-4	

Částečně pokryto: Dokumenty pocházející od sdružení CAB Forum představují průmyslové standardy, používané nejvýznamnějšími tvůrci webových prohlížečů. Nicméně požadavky stanovené v těchto standardech jsou zaměřeny zejména na zaručení identity webových stránek a jejich vlastníka a neodpovídají plně požadavkům na kvalifikované certifikáty pro autentizaci internetových stránek dle nařízení eIDAS. ETSI normy se na tyto standardy odvolávají a doplňují k nim další specifické požadavky.

V případném prováděcím aktu dle článku 45(2) nařízení eIDAS by bylo s velkou pravděpodobností odkazováno na normu **ETSI EN 319 412-4** ("Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates").

V případě prohlášení o souladu s normami řady ETSI EN 319 412 ze strany QTSP, CAB ověří na vzorku vydávaných certifikátů, zdali formát těchto certifikátů je v souladu s ETSI EN 319 412-4 a ETSI EN 319 412-5.

2.4. 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 jednak z požadavků na všechny poskytovatele služeb vytvářejících důvěru (viz kapitola 2.1), dále také z požadavků stanovených pro všechny QTSP (viz kapitola 2.2) 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.

eIDAS článek 32(1)	Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation EN 319 102-1, ETSI TS 119 102-1
eIDAS článek 32(2)	Policy and security requirements for applications for signature creation and signature validation (ETSI TS 119 101)
eIDAS článek 33(1)	General requirements on testing compliance and interoperability of signature creation and validation (ETSI TS 119 144)
	EN 319 102-1, ETSI TS 119 102-1
	Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report (ETSI TS 119 102-2)

ETSI publikovalo v únoru 2019 aktualizaci technických specifikací **TS 119 312 (ELECTRONIC SIGNATURES AND INFRASTRUCTURES ; CRYPTOGRAPHIC SUITES)** - jedná se o aktualizace původních specifikací **TS 102 176-1**, známých jako "Algo paper". Dokument obsahuje doporučení k výběru vhodných algoritmů, které zajistí bezpečnost a interoperabilitu elektronických podpisů v závislosti na požadované úrovni bezpečnosti.

S problematikou ověřování platnosti kvalifikovaných elektronických podpisů a pečetí souvisí i otázka formátů zaručených elektronických podpisů a pečetí, viz **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.**

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:

ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); XADES BASELINE PROFILE ETSI TS 103 171 V.2.1.1.

ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI);CADES BASELINE PROFILE ETSI TS 103 173 V.2.2.1.

ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI);PADES BASELINE PROFILE ETSI TS 103 172 V.2.2.2.

ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); ASIC BASELINE ETSI TS 103 174 V.2.2.1.

V roce 2016 byly přijaty EN normy, které nahrazují výše zmíněné technické specifikace (nicméně prováděcí rozhodnutí KOMISE (EU) 2015/1506 odkazuje na technické specifikace a to do doby, než dojde k jeho případné novelizaci).

ETSI EN 319 132-1 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); XADES DIGITAL SIGNATURES; PART 1: BUILDING BLOCKS AND XADES BASELINE SIGNATURES

ETSI EN 319 132-2 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); XADES DIGITAL SIGNATURES; PART 2: EXTENDED XADES SIGNATURES

ETSI EN 319 122-1 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); CADES DIGITAL SIGNATURES; PART 1: BUILDING BLOCKS AND CADES BASELINE SIGNATURES

ETSI EN 319 122-2 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); CADES DIGITAL SIGNATURES; PART 2: EXTENDED CADES SIGNATURES

ETSI EN 319 142-1 ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); PADES DIGITAL SIGNATURES; PART 1: BUILDING BLOCKS AND PADES BASELINE SIGNATURES

ETSI EN 319 142-2 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles

ETSI EN 319 162-1 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers

ETSI EN 319 162-2 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers

CAB má k dispozici předem připravený vzorek elektronicky podepsaných dokumentu, 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).

2.5. 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 jednak z požadavků na všechny poskytovatele služeb vytvářejících důvěru (viz kapitola 2.1), dále také z požadavků stanovených pro všechny QTSP (viz kapitola 2.2) 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.

eIDAS článek 34(2)	PDF/A Specifikace (ISO 19005-1, Adobe) Audit and Certification of Trustworthy Digital Repositories (ISO 16363:2012, CCSDS) Storage of electronic invoices (CWA 15580) Design Criteria Standard For Electronic Records Management Software Applications (DoD 5015.2) Data Preservation Systems Security; Parts 1-2 (ETSI/ TS 101 533) Policy requirements for trust service providers signing and/or storing data objects (ETSI/CEN TS 102 573)

	Evidence Record Syntax (ERS)(IETF RFC 4998)
	Electronic archiving - Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation (ISO/IEC ISO 14641-1:2012)
	Information and documentation – Records management (ISO/IEC ISO 15489-1:2001)
	Information technology – Metadata registries (MDR)(ISO/IEC ISO/IEC 11179)
	Space data and information transfer systems - Open archival information system (OAIS) - Reference model (ISO/IEC ISO 14721:2012)
	Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents
	International Standard for Archival Description (General)(ISAD(G))
	Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques (ETSI TS 119 511)
	DRAFT Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services protocols for long-term preservation (DRAFT ETSI TS 119 512 – předpoklad publikace schválené TS 04/2020)

Nařízení eIDAS neupřesňuje dále požadavky na postupy a technologie, které mohou být použity k zajištění důvěryhodnosti kvalifikovaného elektronického podpisu/kvalifikované elektronické pečeti i po uplynutí doby technické platnosti. Tudíž není možné posoudit soulad norem, standardů s nařízením eIDAS.

2.6. 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 jednak z požadavků na všechny poskytovatele služeb vytvářejících důvěru (viz kapitola 2.1), dále také z požadavků stanovených pro všechny QTSP (viz kapitola 2.2) 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.

eIDAS článek 42(2)	Time-stamping System (CC3.1) (ANSSI DCSSI-PP 2008/07)	PP pro důvěryhodný produkt TST.
	Politique d'Horodatage Type (ANSSI RGS A5)	Posouzení.
	EESSI Conformity Assessment Guidance - Part 8 - Time-stamping Authority services and processes (CEN CWA 14172-8)	Posouzení.
	Policy and security requirements for TSPs providing time-stamping services (ETSI EN 319 421)	Posouzení, důvěryhodné systémy, správa času.
	Profiles for TSPs providing time-stamping services (ETSI EN 319 422)	Posouzení, důvěryhodné systémy.

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. Standard ETSI TS 102 023, který byl využíván pro certifikaci autorit časových razítek, byl aktualizován v rámci mandátu M460 a rozdělen do dvou standardů:

- *ETSI EN 319 421* specifikující požadavky politiky a bezpečnostní požadavky vztahující se na provoz a správu TSP vydávajícího časová razítka. *ANSSI RGS A5* dále posiluje tyto požadavky, ale obsahuje některé specifické francouzské požadavky, které nemusejí být kompatibilní s aktuální praxí v jiných státech.
- Soulad s *ETSI EN 319 422* zajišťuje spojení data a času s daty ve vydaných elektronických časových razítkách.

ANSSI DCSSI-PP 2008/07 a CEN EN 419 231 jsou vyhodnocené profily ochrany dle Common Criteria pro systém autority časových razítek.

3. 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“).

Poskytovatel služeb vytvářejících důvěru musí předložit orgánu dohledu (MV ČR) 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).

Obsahem zprávy o posouzení shody by mělo být zejména doporučení, zda je možné provést certifikační rozhodnutí, které bude uvádět výsledek auditu, tj. auditovaná služba je v souladu a splňuje požadavky nebo auditovaná služba nesplňuje požadavky, v takovém případě nemůže být vydán certifikát (viz 7.6 a 7.7 z ČSN EN ISO/IEC 17065:2013). To se netýká případu, pokud během auditu byly nalezeny neshody, které ale nemají vliv na splnění požadavků, resp. poskytování dotčené služby a které mají být odstraněny do 3 měsíců v závislosti na závažnosti chyby, viz kapitola 7.6 **ČSN EN 319 403**. V certifikačním rozhodnutí musí být uvedena minimálně identifikace subjektu posuzování shody, identifikace poskytovatele služeb vytvářejících důvěru, identifikace služby, která byla posuzována, datum zahájení a datum ukončení posuzování, výsledek posouzení a specifikace požadavků vůči kterým bylo posouzení shody provedeno (použitelné požadavky nařízení eIDAS). Ve zprávě o posouzení shody by mělo být specifikováno, jakým způsobem (např. dodržením určitých ustanovení konkrétních norem) poskytovatel splnil použitelné požadavky nařízení eIDAS, viz stanovené požadavky na obsah auditní zprávy v kapitole 7.4.4. **ČSN EN 319 403.**

4. Zkratky

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

[2] 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)

[3] CAB - subjekt posuzování shody (conformity assessment body)

[4] NAB - národní akreditační orgán (national accreditation body)

[5] QTSP - kvalifikovaný poskytovatel služeb vytvářejících důvěru (qualified trust service providers)

[6] TSP - poskytovatel služeb vytvářejících důvěru (trust service providers)

[7] REQ - značí konkrétní požadavek uvedený v dané normě (REQ - requirement)

[8] 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)

[9] AdES – advanced electronic signature

[10] DSS – Digital Signature Service

5. 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] ETSI TR 119 000 V1.2.1 Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview

[3] 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, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[4] 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.

[5] 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.

[6] ENISA: Article 19 Incident reporting, https://www.enisa.europa.eu/publications/article19-incident-reporting-framework