Úřední věstník
Evropské unie

CS
Řada L

2025/1943

30.9.2025

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

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na 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 ([1]), a zejména na čl. 28 odst. 6 a čl. 38 odst. 6 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Kvalifikované certifikáty pro elektronické podpisy a kvalifikované certifikáty pro elektronické pečetě hrají v digitálním podnikatelském prostředí klíčovou roli, neboť podporují přechod od tradičních postupů založených na papírových dokumentech k rovnocenným elektronickým postupům. Tím, že spojují data pro ověřování platnosti elektronických podpisů nebo data pro ověřování platnosti elektronických pečetí s fyzickou nebo právnickou osobou a potvrzují jméno této osoby, zvyšují kvalifikované certifikáty jistotu ohledně totožnosti podepisující osoby a pečetící osoby.

(2) Předpoklad shody stanovený v čl. 28 odst. 6 a čl. 38 odst. 6 nařízení (EU) č. 910/2014 by měl platit pouze tehdy, pokud kvalifikované služby vytvářející důvěru pro vydávání kvalifikovaných certifikátů pro elektronické podpisy a kvalifikované služby vytvářející důvěru pro vydávání kvalifikovaných certifikátů pro elektronické pečetě splňují normy stanovené v tomto nařízení. Tyto normy by měly odrážet zavedené postupy a měly by být v příslušných odvětvích široce uznávány. Měly by být upraveny tak, aby zahrnovaly další kontroly zajišťující bezpečnost a důvěryhodnost kvalifikovaných služeb vytvářejících důvěru a obsahu kvalifikovaných certifikátů.

(3) Pokud poskytovatel služeb vytvářejících důvěru splňuje požadavky stanovené v příloze tohoto nařízení, měly by orgány dohledu předpokládat shodu s příslušnými požadavky nařízení (EU) č. 910/2014 a tento předpoklad řádně zohlednit při udělování nebo potvrzování statusu kvalifikované služby vytvářející důvěru. Kvalifikovaný poskytovatel služeb vytvářejících důvěru však může při prokazování shody s požadavky nařízení (EU) č. 910/2014 nadále využívat i jiných postupů.

(4) Komise pravidelně posuzuje nové technologie, postupy, normy nebo technické specifikace. V souladu se 75. bodem odůvodnění nařízení Evropského parlamentu a Rady (EU) 2024/1183 ([2]) by Komise měla toto nařízení přezkoumávat a v případě potřeby ho aktualizovat, aby bylo v souladu s globálním vývojem, novými technologiemi, normami nebo technickými specifikacemi a aby byly dodržovány osvědčené postupy na vnitřním trhu.

(5) Na všechny činnosti zpracování osobních údajů podle tohoto nařízení se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ([3]) a v příslušných případech směrnice Evropského parlamentu a Rady 2002/58/ES ([4]).

([1]) Úř. věst. L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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 (Úř. věst. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) 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) (Úř. věst. L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(6) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([5]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 6. června 2025.

(7) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného článkem 48 nařízení (EU) č. 910/2014,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Referenční normy a specifikace pro kvalifikované certifikáty pro elektronické podpisy a kvalifikované certifikáty pro elektronické pečetě

1. Referenční normy a specifikace uvedené v čl. 28 odst. 6 nařízení (EU) č. 910/2014 jsou stanoveny v příloze I tohoto nařízení.

2. Referenční normy a specifikace uvedené v čl. 38 odst. 6 nařízení (EU) č. 910/2014 jsou stanoveny v příloze II tohoto nařízení.

Článek 2

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 29. září 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

([5]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PŘÍLOHA I

Seznam referenčních norem a specifikací pro kvalifikované certifikáty pro elektronické podpisy

Normy ETSI EN 319 411-2 V2.6.1 (dále jen „ETSI EN 319 411-2“), ETSI EN 319 412-1 V1.6.1 (dále jen „ETSI EN 319 412-1“), ETSI EN 319 412-2 V2.4.1 (dále jen „ETSI EN 319 412-2“) a ETSI EN 319 412-5 V2.5.1 (dále jen „ETSI EN 319 412-5“) se použijí s těmito úpravami:

1. Pro normu ETSI EN 319 411-2

1) 2.1 Normativní odkazy

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Obecné politické požadavky na poskytovatele služeb vytvářejících důvěru“.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Politické a bezpečnostní požadavky na poskytovatele služeb vytvářejících důvěru vydávající certifikáty; Část 1: Obecné požadavky“ s těmito úpravami:

Bod 2.1 „Normativní odkazy“ normy ETSI EN 319 411-1 V1.5.1 se mění takto:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Obecné politické požadavky na poskytovatele služeb vytvářejících důvěru“.

— [10] ETSI EN 319 412-2 V2.4.1 „Elektronické podpisy a infrastruktury (ESI); Profily certifikátů; Část 2: Profil certifikátu pro certifikáty vydávané fyzickým osobám“;

— [14] ETSI EN 319 412-1 V1.6.1 „Elektronické podpisy a infrastruktury (ESI); Profily certifikátů; Část 1: Přehled a společné datové struktury“.

— [3] ETSI EN 319 412-5 V2.5.1 „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Profily certifikátů; Část 5: Prohlášení „QCStatements“.

— [5] ETSI EN 319 412-1 V1.6.1 „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Profily certifikátů; Část 1: Přehled a společné datové struktury“.

— [6] CEN/TS 419261:2015 „Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty a časová razítka“.

— [7] Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování: „Dohodnuté kryptografické mechanismy“ zveřejněné Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) ([1]).

— [8] Prováděcí nařízení Komise (EU) 2024/482 ([2]), kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC).

— [9] Prováděcí nařízení Komise (EU) 2024/3144 ([3]), kterým se mění prováděcí nařízení (EU) 2024/482, pokud jde o použitelné mezinárodní normy, a kterým se uvedené prováděcí nařízení opravuje.

— [10] ISO/IEC 15408:2022 (části 1 až 5): „Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Kritéria hodnocení bezpečnosti IT“.

— [11] FIPS PUB 140-3 (2019) „Bezpečnostní požadavky na kryptografické moduly“.

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) Úř. věst. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 5.2 Požadavky na prohlášení o certifikačních postupech

— OVR-5.2-02 Certifikační postupy uvedené v dokumentaci poskytovatele služeb vytvářejících důvěru specifikují požadavky na profily certifikátů, které mají být použity.

3) 5.3 Název a identifikace certifikační politiky

— OVR-5.3-01 Pokud jsou v certifikačních postupech provedeny jakékoli změny popsané v bodě 4.2.2, které mají vliv na použitelnost, musí být změněn identifikátor politiky.

4) 6.1 Povinnosti v oblasti zveřejňování a úložišť

— OVR-6.1-02 Informace uvedené v ustanovení DIS-6.1-04 normy ETSI EN 319 411-1 [2] musí být veřejně a mezinárodně dostupné.

5) 6.2.2 Počáteční ověření totožnosti

— REG-6.2.2-01A Shromažďování atributů a důkazů o totožnosti subjektu, jakož i jejich ověřování se provádí v souladu s prováděcími akty přijatými podle čl. 24 odst. 1c nařízení (EU) č. 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] a [QCP-n-qscd] Totožnost fyzické osoby a v příslušných případech zvláštní atributy této osoby se ověřují v souladu s prováděcími akty přijatými podle čl. 24 odst. 1c nařízení (EU) č. 910/2014 [i.1];

— POZNÁMKA 1 neplatné.

6) 6.3.3 Vydávání certifikátů

— GEN-6.3.3-01 Použijí se požadavky GEN-6.3.3-01 až GEN-6.3.3-10 uvedené v normě ETSI EN 319 411-1 [2], bodě 6.3.3.

— GEN-6.3.3-02 [PODMÍNĚNÉ] Pokud je certifikát vydán fyzické osobě identifikované ve spojení s právnickou osobou, pak atributy subjektu identifikující organizaci v certifikátu představují právnickou osobu nebo dílčí subjekt této právnické osoby a identifikátor subjektu v certifikátu představuje fyzickou osobu.

— GEN-6.3.3-03 Identifikátor certifikační politiky je [VOLBA]:

a) [QCP-n]

— jak je uvedeno v bodě 5.3 písm. a), a/nebo

— identifikátor objektu přidělený poskytovatelem služeb vytvářejících důvěru, jinou příslušnou zúčastněnou stranou nebo další normalizací v oblasti certifikační politiky, která rozšiřuje příslušné platné požadavky na politiku vymezené v tomto dokumentu;

b) [QCP-n-qscd]

— jak je uvedeno v bodě 5.3 písm. c), a/nebo

— identifikátor objektu přidělený poskytovatelem služeb vytvářejících důvěru, jinou příslušnou zúčastněnou stranou nebo další normalizací v oblasti certifikační politiky, která rozšiřuje příslušné platné požadavky na politiku vymezené v tomto dokumentu.

7) 6.3.5 Použití párů klíčů a certifikátů

— SDP-6.3.5-02A [PODMÍNĚNÉ] Pokud poskytovatel služeb vytvářejících důvěru spravuje pro subjekt kvalifikovaný prostředek pro vytváření elektronických podpisů, musí být kvalifikovaným poskytovatelem služeb vytvářejících důvěru, který poskytuje kvalifikovanou službu vytvářející důvěru pro správu kvalifikovaného prostředku pro vytváření elektronických podpisů na dálku v souladu s nařízením (EU) č. 910/2014 [i.1].

— SDP-6.3.5-11A Povinnosti držitele certifikátu (viz bod 6.3.4), pokud držitel nebo subjekt generuje klíče subjektu, zahrnují:

a) povinnost generovat klíče subjektu pomocí algoritmu, který je v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti [7] a zveřejněnými agenturou ENISA pro použití certifikovaného klíče, jak je uvedeno v certifikační politice;

b) povinnost používat délku klíče a algoritmus, které jsou v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti [7] a zveřejněnými agenturou ENISA pro použití certifikovaného klíče, jak je uvedeno v certifikační politice, po dobu platnosti certifikátu.

8) 6.3.10 Služby pro ověření statusu certifikátu

— CSS-6.3.10-08 [PODMÍNĚNÉ] Jsou-li poskytnuty seznamy zneplatněných certifikátů, poskytovatel služeb vytvářejících důvěru zajistí integritu a dostupnost posledního seznamu zneplatněných certifikátů alespoň po dobu stanovenou v prohlášení o certifikačních postupech, jak je požadováno v CSS-6.3.10-12.

9) 6.4.4 Kontroly personálu

— OVR-6.4.4-02 Pracovníci poskytovatele služeb vytvářejících důvěru na důvěryhodných pozicích a v příslušných případech jeho subdodavatelé na důvěryhodných pozicích musí být schopni splnit požadavek na „odborné znalosti, zkušenosti a kvalifikaci“ prostřednictvím formální odborné přípravy a pověření nebo skutečných zkušeností nebo kombinace obojího.

— OVR-6.4.4-03 Soulad s OVR-6.4.4-02 musí zahrnovat pravidelné (alespoň každých dvanáct měsíců) aktuální informace o nových hrozbách a stávajících bezpečnostních postupech.

— OVR-6.4.4-04 Kromě důvěryhodných pozic uvedených v normě ETSI EN 319 401 [1] (bodech 7.2-15) musí být podporovány důvěryhodné pozice úředníků pro registraci a zneplatnění s povinnostmi vymezenými v normě TS 419261 [6]. V případech, kdy je systém kvalifikovaných poskytovatelů služeb vytvářejících důvěru přímo spravován členským státem nebo subjektem veřejného sektoru nebo je provozován jejich jménem, může tyto další důvěryhodné pozice zastávat jeden nebo více formálních zástupců, kteří jednají jménem úředníků pro registraci a zneplatnění působících v místní nebo regionální správě.

10) 6.4.9 Ukončení činnosti certifikačním nebo registračním orgánem

— OVR-6.4.9-02 Plán ukončení činnosti poskytovatele služeb vytvářejících důvěru musí splňovat požadavky stanovené v prováděcích aktech přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014 [i.1].

11) 6.5.1 Generování a instalace párů klíčů

— OVR-6.5.1-01A Generování páru klíčů certifikačního orgánu se provádí pomocí algoritmu, který je v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [7] pro účely podepisování certifikačního orgánu.

— OVR-6.5.1-01B Zvolená délka klíče a algoritmus pro podpisový klíč certifikačního orgánu musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [7] pro účely podepisování certifikačního orgánu.

— OVR-6.5.1-01C [PODMÍNĚNÉ] Pokud klíče subjektu generuje certifikační orgán, musí být klíče subjektu generované certifikačním orgánem v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou agentury ENISA [7] pro účely uvedené v certifikační politice po dobu platnosti certifikátu.

12) 6.5.2 Ochrana soukromého klíče a technické kontroly kryptografického modulu

— GEN-6.5.2-01 Použijí se všechny požadavky uvedené v normě ETSI EN 319 411-1 [2], bodě 6.5.2, kromě požadavků OVR-6.5.2-01, OVR-6.5.2-03 a OVR-6.5.2-04.

— GEN-6.5.2-02 Generování párů klíčů poskytovatele služeb vytvářejících důvěru, včetně klíčů používaných službami zneplatnění a registrace, se provádí v rámci bezpečného kryptografického prostředku, který představuje důvěryhodný systém certifikovaný v souladu s/se:

— společnými kritérii pro hodnocení bezpečnosti informačních technologií stanovenými v normě ISO/IEC 15408 [10] nebo ve společných kritériích pro hodnocení bezpečnosti informačních technologií, verzi CC:2002, části 1 až 5, zveřejněných účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT a certifikovaných na úrovni EAL 4 nebo vyšší, nebo

— evropským systémem certifikace kybernetické bezpečnosti založeným na společných kritériích (EUCC) [8][9] a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

— do 31. 12. 2030 s normou FIPS PUB 140-3 [11] úrovně 3.

Tato certifikace musí odpovídat bezpečnostnímu cíli nebo profilu ochrany nebo dokumentaci návrhu modulu a jeho bezpečnosti, která splňuje požadavky tohoto dokumentu na základě analýzy rizik a s přihlédnutím k fyzickým a jiným netechnickým bezpečnostním opatřením.

Pokud je bezpečný kryptografický prostředek certifikován podle EUCC [8][9], musí být tento prostředek nakonfigurován a používán v souladu s touto certifikací.

— GEN-6.5.2-03 Soukromý podpisový klíč certifikačního orgánu musí být uložen a používán v rámci bezpečného kryptografického prostředku, který splňuje požadavky GEN-6.5.2-01 a GEN-6.5.2-02.

13) 6.5.7 Bezpečnostní kontroly sítě

— OVR-6.5.7-02 Skenování zranitelnosti požadované v rámci požadavku REQ-7.8-13 normy ETSI EN 319 401 [1] se provádí nejméně jednou za čtvrtletí.

— OVR-6.5.7-03 Penetrační test požadovaný v rámci požadavku REQ-7.8-17X normy ETSI EN 319 401 [1] se provádí nejméně jednou ročně.

— OVR-6.5.7-04 Firewally musí být nakonfigurovány tak, aby zabránily veškerým protokolům a přístupům, které nejsou nezbytné pro provoz poskytovatele služeb vytvářejících důvěru.

14) 6.6.1 Profil certifikátu

— GEN-6.6.1-05 Certifikát musí obsahovat jeden z identifikátorů politiky uvedených v GEN-6.3.3-03 [VOLBA]. Certifikát může obsahovat další identifikátory objektu přidělené poskytovatelem služeb vytvářejících důvěru.

2. Pro normu ETSI EN 319 412-2

1) 2.1 Normativní odkazy

— [2] ETSI EN 319 412-5 V2.5.1 „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Profily certifikátů; Část 5: Prohlášení „QCStatements“.

— [9] Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování, „Dohodnuté kryptografické mechanismy“ zveřejněné agenturou ENISA.

2) 4.2.2 Podpis

— GEN-4.2.2-2 Podpisový algoritmus se zvolí v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [9];

— POZNÁMKA neplatné.

3) 4.2.3.1 Vydavatelé – právnické osoby

— GEN-4.2.3.1-3 Pokud je známa existence příslušného registračního čísla, pak identita vydavatele obsahuje atribut organizationIdentifier s hodnotou tohoto registračního čísla, jak je uvedeno v příslušném úředním záznamu, který toto registrační číslo stanoví.

4) 4.2.5 Informace o veřejném klíči subjektu

— GEN-4.2.5-2 Veřejný klíč subjektu se zvolí v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [9];

— POZNÁMKA neplatné.

5) 4.2.6 Sériové číslo

— GEN-4.2.6-01 Sériové číslo certifikátu (jak je uvedeno v normě IETF RFC 5280 [1], bodě 4.1.2.2) musí být jedinečné pro každý certifikát vydaný poskytovatelem služeb vytvářejících důvěru.

PŘÍLOHA II

Seznam referenčních norem a specifikací pro kvalifikované certifikáty pro elektronické pečetě

Normy ETSI EN 319 411-2 V2.6.1 (dále jen „ETSI EN 319 411-2“), ETSI EN 319 412-1 V1.6.1(dále jen „ETSI EN 319 412-1“), ETSI EN 319 412-3 V1.3.1 (dále jen „ETSI EN 319 412-3“), ETSI EN 319 412-2 V2.4.1 (dále jen „ETSI EN 319 412-2“), a ETSI EN 319 412-5 V2.5.1 (dále jen „ETSI EN 319 412-5“) se použijí s těmito úpravami:

1. Pro normu ETSI EN 319 411-2

1) 2.1 Normativní odkazy

— [1] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Obecné politické požadavky na poskytovatele služeb vytvářejících důvěru“.

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Politické a bezpečnostní požadavky na poskytovatele služeb vytvářejících důvěru vydávající certifikáty; Část 1: Obecné požadavky“ s těmito úpravami:

Bod 2.1 „Normativní odkazy“ normy ETSI EN 319 411-1 V1.5.1 se mění takto:

— [9] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Obecné politické požadavky na poskytovatele služeb vytvářejících důvěru“.

— [10] ETSI EN 319 412-2 V2.4.1 „Elektronické podpisy a infrastruktury (ESI); Profily certifikátů; Část 2: Profil certifikátu pro certifikáty vydávané fyzickým osobám“;

— [14] ETSI EN 319 412-1 V1.6.1 „Elektronické podpisy a infrastruktury (ESI); Profily certifikátů; Část 1: Přehled a společné datové struktury“.

— [3] ETSI EN 319 412-5 V2.5.1 „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Profily certifikátů; Část 5: Prohlášení „QCStatements“.

— [5] ETSI EN 319 412-1 V1.6.1 „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Profily certifikátů; Část 1: Přehled a společné datové struktury“.

— [6] CEN/TS 419261:2015 „Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty a časová razítka“, (vyhotovené Evropským výborem pro normalizaci).

— [7] Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování: „Dohodnuté kryptografické mechanismy“ zveřejněné agenturou ENISA.

— [8] Prováděcí nařízení Komise (EU) 2024/482, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC).

— [9] Prováděcí nařízení (EU) 2024/3144, kterým se mění prováděcí nařízení (EU) 2024/482, pokud jde o použitelné mezinárodní normy, a kterým se uvedené prováděcí nařízení opravuje.

— [10] ISO/IEC 15408:2022 (části 1 až 5) „Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Kritéria hodnocení bezpečnosti IT“.

— [11] FIPS PUB 140-3 (2019) „Bezpečnostní požadavky na kryptografické moduly“.

2) 5.2 Požadavky na prohlášení o certifikačních postupech

— OVR-5.2-02 Certifikační postupy uvedené v dokumentaci poskytovatele služeb vytvářejících důvěru specifikují požadavky na profily certifikátů, které mají být použity.

3) 5.3 Název a identifikace certifikační politiky

— OVR-5.3-01 Pokud jsou v certifikačních postupech provedeny jakékoli změny popsané v bodě 4.2.2, které mají vliv na použitelnost, musí být změněn identifikátor politiky.

4) 6.1 Povinnosti v oblasti zveřejňování a úložišť

— OVR-6.1-02 Informace uvedené v ustanovení DIS-6.1-04 normy ETSI EN 319 411-1 [2] musí být veřejně a mezinárodně dostupné.

5) 6.2.2 Počáteční ověření totožnosti

— REG-6.2.2-01A Shromažďování atributů a důkazů o totožnosti subjektu, jakož i jejich ověřování se provádí v souladu s prováděcími akty přijatými podle čl. 24 odst. 1c nařízení (EU) č. 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] a [QCP-l-qscd] Totožnost právnické osoby a v příslušných případech zvláštní atributy této osoby se ověřují v souladu s prováděcími akty přijatými podle čl. 24 odst. 1c nařízení (EU) č. 910/2014 [i.1];

— POZNÁMKA 3 viz poznámka 2.

6) 6.3.3 Vydávání certifikátů

— GEN-6.3.3-01 Použijí se požadavky GEN-6.3.3-01 až GEN-6.3.3-10 uvedené v normě ETSI EN 319 411-1 [2], bodě 6.3.3.

— GEN-6.3.3-02 Identifikátor certifikační politiky je [VOLBA]:

a) [QCP-l]

— jak je uvedeno v bodě 5.3 písm. b), a/nebo

— identifikátor objektu přidělený poskytovatelem služeb vytvářejících důvěru, jinou příslušnou zúčastněnou stranou nebo další normalizací v oblasti certifikační politiky, která rozšiřuje příslušné platné požadavky na politiku vymezené v tomto dokumentu;

b) [QCP-l-qscd]

— jak je uvedeno v bodě 5.3 písm. d), a/nebo

— identifikátor objektu přidělený poskytovatelem služeb vytvářejících důvěru, jinou příslušnou zúčastněnou stranou nebo další normalizací v oblasti certifikační politiky, která rozšiřuje platné požadavky na politiku vymezené v tomto dokumentu.

7) 6.3.5 Použití párů klíčů a certifikátů

— SDP-6.3.5-02A [PODMÍNĚNÉ] Pokud poskytovatel služeb vytvářejících důvěru spravuje pro subjekt kvalifikovaný prostředek pro vytváření elektronických pečetí, musí být kvalifikovaným poskytovatelem služeb vytvářejících důvěru, který poskytuje kvalifikovanou službu vytvářející důvěru pro správu kvalifikovaného prostředku pro vytváření elektronických pečetí na dálku v souladu s nařízením (EU) č. 910/2014 [i.1].

— SDP-6.3.5-11A Povinnosti držitele certifikátu (viz bod 6.3.4), pokud držitel nebo subjekt generuje klíče subjektu, zahrnují:

a) povinnost generovat klíče subjektu pomocí algoritmu, který je v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [7] pro použití certifikovaného klíče, jak je uvedeno v certifikační politice; a

b) povinnost používat délku klíče a algoritmus, které jsou v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [7] pro použití certifikovaného klíče, jak je uvedeno v certifikační politice, po dobu platnosti certifikátu.

8) 6.3.10 Služby pro ověření statusu certifikátu

— CSS-6.3.10-08 [PODMÍNĚNÉ] Jsou-li poskytnuty seznamy zneplatněných certifikátů, poskytovatel služeb vytvářejících důvěru zajistí integritu a dostupnost posledního seznamu zneplatněných certifikátů alespoň po dobu stanovenou v prohlášení o certifikačních postupech, jak je požadováno v CSS-6.3.10-12.

9) 6.4.4 Kontroly personálu

— OVR-6.4.4-02 Pracovníci poskytovatele služeb vytvářejících důvěru na důvěryhodných pozicích a v příslušných případech jeho subdodavatelé na důvěryhodných pozicích musí být schopni splnit požadavek na „odborné znalosti, zkušenosti a kvalifikaci“ prostřednictvím formální odborné přípravy a pověření nebo skutečných zkušeností nebo kombinace obojího.

— OVR-6.4.4-03 Soulad s OVR-6.4.4-02 musí zahrnovat pravidelné (alespoň každých dvanáct měsíců) aktuální informace o nových hrozbách a stávajících bezpečnostních postupech.

— OVR-6.4.4-04 Kromě důvěryhodných pozic uvedených v normě ETSI EN 319 401 [1] (bodech 7.2-15) musí být podporovány důvěryhodné pozice úředníků pro registraci a zneplatnění s povinnostmi vymezenými v normě TS 419261 [6]. V případech, kdy je systém kvalifikovaných poskytovatelů služeb vytvářejících důvěru přímo spravován členským státem nebo subjektem veřejného sektoru nebo je provozován jejich jménem, může tyto další důvěryhodné pozice zastávat jeden nebo více formálních zástupců, kteří jednají jménem úředníků pro registraci a zneplatnění působících v místní nebo regionální správě.

10) 6.4.9 Ukončení činnosti certifikačním nebo registračním orgánem

— OVR-6.4.9-02 Plán ukončení činnosti poskytovatele služeb vytvářejících důvěru musí splňovat požadavky stanovené v prováděcích aktech přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014 [i.1].

11) 6.5.1 Generování a instalace párů klíčů

— OVR-6.5.1-01A Generování páru klíčů certifikačního orgánu se provádí pomocí algoritmu, který je v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [7] pro účely podepisování certifikačního orgánu.

— OVR-6.5.1-01B Zvolená délka klíče a algoritmus pro podpisový klíč certifikačního orgánu musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [7] pro účely podepisování certifikačního orgánu.

— OVR-6.5.1-01C [PODMÍNĚNÉ] Pokud klíče subjektu generuje certifikační orgán, musí být klíče subjektu generované certifikačním orgánem v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou agentury ENISA [7] pro účely uvedené v certifikační politice po dobu platnosti certifikátu.

12) 6.5.2 Ochrana soukromého klíče a technické kontroly kryptografického modulu

— GEN-6.5.2-01 Použijí se všechny požadavky uvedené v normě ETSI EN 319 411-1 [2], bodě 6.5.2, kromě požadavků OVR-6.5.2-01, OVR-6.5.2-03 a OVR-6.5.2-04.

— GEN-6.5.2-02 Generování párů klíčů poskytovatele služeb vytvářejících důvěru, včetně klíčů používaných službami zneplatnění a registrace, se provádí v rámci bezpečného kryptografického prostředku, který představuje důvěryhodný systém certifikovaný v souladu s/se:

  — společnými kritérii pro hodnocení bezpečnosti informačních technologií stanovenými v normě ISO/IEC 15408 [10] nebo ve společných kritériích pro hodnocení bezpečnosti informačních technologií, verzi CC:2002, části 1 až 5, zveřejněných účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT a certifikovaných na úrovni EAL 4 nebo vyšší, nebo

  — evropským systémem certifikace kybernetické bezpečnosti založeným na společných kritériích (EUCC) [8][9] a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

  — do 31. 12. 2030 s normou FIPS PUB 140-3 [11] úrovně 3.

Tato certifikace musí odpovídat bezpečnostnímu cíli nebo profilu ochrany nebo dokumentaci návrhu modulu a jeho bezpečnosti, která splňuje požadavky tohoto dokumentu na základě analýzy rizik a s přihlédnutím k fyzickým a jiným netechnickým bezpečnostním opatřením.

Pokud je bezpečný kryptografický prostředek certifikován podle EUCC [8][9], musí být tento prostředek nakonfigurován a používán v souladu s touto certifikací.

— GEN-6.5.2-03 Soukromý podpisový klíč certifikačního orgánu musí být uložen a používán v rámci bezpečného kryptografického prostředku, který splňuje požadavky GEN-6.5.2-01 a GEN-6.5.2-02.

13) 6.5.7 Bezpečnostní kontroly sítě

— OVR-6.5.7-02 Skenování zranitelnosti požadované v rámci požadavku REQ-7.8-13 normy ETSI EN 319 401 [1] se provádí nejméně jednou za čtvrtletí.

— OVR-6.5.7-03 Penetrační test požadovaný v rámci požadavku REQ-7.8-17X normy ETSI EN 319 401 [1] se provádí nejméně jednou ročně.

— OVR-6.5.7-04 Firewally musí být nakonfigurovány tak, aby zabránily veškerým protokolům a přístupům, které nejsou nezbytné pro provoz poskytovatele služeb vytvářejících důvěru.

14) 6.6.1 Profil certifikátu

— GEN-6.6.1-05 Certifikát musí obsahovat jeden z identifikátorů politiky uvedených v GEN-6.3.3-02 [VOLBA].

2. Pro normu ETSI EN 319 412-3

1) 2.1 Normativní odkazy

— [2] ETSI EN 319 412-2 V2.4.1 „Elektronické podpisy a infrastruktury (ESI); Profily certifikátů; Část 2: Profil certifikátu pro certifikáty vydávané fyzickým osobám“.

2) 4.2.1 Subjekt

— LEG-4.2.1-6 Atribut organizationIdentifier musí obsahovat identifikaci organizace subjektu odlišnou od názvu organizace. Pokud je známa existence příslušného registračního čísla, pak atribut organizationIdentifier obsahuje hodnotu tohoto registračního čísla uvedenou v příslušném úředním záznamu, který toto registrační číslo stanoví.

3. Pro normu ETSI EN 319 412-2

1) 2.1 Normativní odkazy

— [2] ETSI EN 319 412-5 V2.5.1 „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Profily certifikátů; Část 5: Prohlášení „QCStatements“.

— [9] Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování: „Dohodnuté kryptografické mechanismy“ zveřejněné agenturou ENISA.

2) 2.2 Informativní odkazy

— [i.7] neplatné.

3) 4.2.2 Podpis

— GEN-4.2.2-2 Podpisový algoritmus se zvolí v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [9];

— POZNÁMKA neplatné.

4) 4.2.3.1 Vydavatelé – právnické osoby

— GEN-4.2.3.1-3 Pokud je známa existence příslušného registračního čísla, pak identita vydavatele obsahuje atribut organizationIdentifier s hodnotou tohoto registračního čísla, jak je uvedeno v příslušném úředním záznamu, který toto registrační číslo stanoví.

5) 4.2.5 Informace o veřejném klíči subjektu

— GEN-4.2.5-2 Veřejný klíč subjektu se zvolí v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [9];

— POZNÁMKA neplatné.

6) 4.2.6 Sériové číslo

— GEN-4.2.6-01 Sériové číslo certifikátu (jak je uvedeno v normě IETF RFC 5280 [1], bodě 4.1.2.2) musí být jedinečné pro každý certifikát vydaný poskytovatelem služeb vytvářejících důvěru.