2025/1942

30.9.2025

# 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**

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. 33 odst. 2 a článek 40 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí zajišťují integritu, pravost a správnost procesu a výsledků ověřování platnosti kvalifikovaných elektronických podpisů, resp. kvalifikovaných elektronických pečetí. Tyto kvalifikované služby vytvářející důvěru hrají v digitálním podnikatelském prostředí klíčovou roli, neboť podporují přechod od tradičních postupů založených na papírových dokumentech k rovnocenným elektronickým postupům.

(2) Předpoklad shody stanovený v čl. 33 odst. 2 a článku 40 nařízení (EU) č. 910/2014 by měl platit pouze tehdy, pokud kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí splňují technické 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, jakož i možnost ověřit kvalifikovaný status a technickou platnost kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí.

(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.

([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).

(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]).

(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**

Referenční normy a specifikace uvedené v čl. 33 odst. 2 a článku 40 nařízení (EU) č. 910/2014 jsou stanoveny v příloze 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

([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).

([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*

**Seznam referenčních norem a specifikací pro kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pro kvalifikované služby ověřování platnosti kvalifikovaných elektronických pečetí**

Normy ETSI TS 119 441 V1.2.1 (2023-10) ([1]) (dále jen „ETSI TS 119 441“) a ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) (dále jen „ETSI TS 119 172-4“) se použijí s těmito úpravami:

1. Pro normu ETSI TS 119 441

1) 2.1 Normativní odkazy

— [1] ETSI TS 119 101 V1.1.1 (2016-03) „Elektronické podpisy a infrastruktury (ESI); Politické a bezpečnostní požadavky na aplikace pro vytváření podpisů a ověřování platnosti podpisů“.

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

— [3] ETSI EN 319 102-1 V1.4.1 (2024-06) „Elektronické podpisy a infrastruktury (ESI); Postupy pro vytváření a ověřování platnosti digitálních podpisů AdES; Část 1: Vytvoření a ověření platnosti“.

— [4] ISO/IEC 15408-1:2022 – Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Kritéria hodnocení bezpečnosti IT.

— [5] neplatné.

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

— [7] 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) ([3]).

— [8] ETSI TS 119 172-4 V1.1.1 (2021-05) „Elektronické podpisy a infrastruktury (ESI); Podpisová politika; Část 4: Pravidla použitelnosti podpisu (politika ověřování platnosti) pro evropské kvalifikované elektronické podpisy / pečetě používající důvěryhodné seznamy“.

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) „Elektronické podpisy a infrastruktury (ESI); Postupy pro vytváření a ověřování platnosti digitálních podpisů AdES; Část 2: Zpráva o ověření platnosti podpisu“.

— [10] Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování: „Dohodnuté kryptografické mechanismy“ zveřejněné Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) ([4]).

— [11] Prováděcí nařízení Komise (EU) 2024/3144, kterým se mění prováděcí nařízení (EU) 2024/482, pokud jde o použitelné mezinárodní normy, a kterým se uvedené prováděcí nařízení opravuje ([5]).

— [12] ETSI EN 319 411-1 „Elektronické podpisy a infrastruktury (ESI); Politické a bezpečnostní požadavky na poskytovatele služeb vytvářejících důvěru vydávající certifikáty; Část 1: Obecné požadavky“.

([1]) ETSI TS 119 441 – Elektronické podpisy a infrastruktury (ESI); Politické požadavky na poskytovatele služeb vytvářejících důvěru poskytující služby ověřování platnosti podpisu, V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 – Elektronické podpisy a infrastruktury (ESI); Podpisová politika; Část 4: Pravidla použitelnosti podpisu (politika ověřování platnosti) pro evropské kvalifikované elektronické podpisy / pečetě používající důvěryhodné seznamy, V1.1.1 (2021-05).
([3]) Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([5]) Úř. věst. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Informativní odkazy

— [i.11] neplatné.

3) 3.3 Zkratky

— EUCC Evropský systém certifikace kybernetické bezpečnosti založený na společných kritériích.

4) 4.3.3 Postup

— POZNÁMKA Pokyny – viz norma ETSI EN 319 102-1 [3]; další pokyny pro případ kvalifikovaného podpisu nebo pečetě EU – viz norma ETSI TS 119 172-4 [8].

5) 6.1 Prohlášení o postupech služby ověřování platnosti podpisů

— OVR-6.1-02 Prohlášení o postupech služby ověřování platnosti podpisů je strukturováno tak, jak je uvedeno v příloze A.

— OVR-6.1-03 Prohlášení o postupech služby ověřování platnosti podpisů obsahuje seznam podporovaných politik ověřování platnosti podpisů (např. prostřednictvím identifikátorů objektu) nebo odkaz na ně a jejich stručný popis.

6) 6.3 Politika v oblasti bezpečnosti informací

— OVR-6.3-02 Politika v oblasti bezpečnosti dokumentuje kontroly bezpečnosti a ochrany soukromí zavedené za účelem ochrany osobních údajů.

7) 7.2 Lidské zdroje

— OVR-7.2-02 Pracovníci poskytovatele služby ověřování platnosti podpisů 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-7.2-03 Shoda s požadavkem OVR-7.2-02 musí zahrnovat pravidelné aktuální informace (alespoň každých dvanáct měsíců) o nových hrozbách a stávajících bezpečnostních postupech.

8) 7.5 Kontroly šifrování

— OVR-7.5-02 [PODMÍNĚNÉ] Při podepisování zpráv o ověření platnosti musí být veřejný podpisový certifikát poskytovatele služby ověřování platnosti podpisů odpovídající soukromému podpisovému klíči poskytovatele služby ověřování platnosti podpisů vydán důvěryhodnou certifikační autoritou v souladu s normalizovanou certifikační politikou NCP+, jak je vymezeno v normě ETSI EN 319 411-1 [12]. Měl by být vydán v souladu s příslušnou certifikační politikou uvedenou v normě ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [PODMÍNĚNÉ] Při podepisování zpráv o ověření platnosti je soukromý podpisový klíč poskytovatele služby ověřování platnosti podpisů uchováván a používán v rámci bezpečného kryptografického prostředku, který je důvěryhodným systémem certifikovaným v souladu se:

a) společnými kritérii pro hodnocení bezpečnosti informačních technologií stanovenými v normě ISO/IEC 15408 [4] nebo ve společných kritériích pro hodnocení bezpečnosti informačních technologií, verzi CC:2022, 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

b) systémem EUCC [7][11] a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [6] 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 [7][11], musí být tento prostředek nakonfigurován a používán v souladu s touto certifikací.

— OVR-7.5-04 neplatné.

— OVR-7.5-06 Soukromý podpisový klíč poskytovatele služby ověřování platnosti podpisů lze exportovat a importovat do jiného bezpečného kryptografického prostředku pouze tehdy, pokud je tento export a import realizován bezpečně a v souladu s certifikací těchto zařízení.

9) 7.7 Bezpečnost provozu

— OVR-7.7-02 Aby bylo zajištěno, že systémy, na kterých je aplikace vyvíjena, používají vhodná bezpečnostní opatření a přizpůsobují se specifickým aplikačním prostředím, musí aplikace ověřování platnosti podpisů používat aplikační prostředí, které je vždy aktualizováno všemi bezpečnostními opravami.

— OVR-7.7-03 Na aplikaci ověřování platnosti podpisů se vztahují následující požadavky uvedené v normě ETSI TS 119 101 [1], bodě 5.2: GSM 1.3.

10) 7.8 Bezpečnost sítí

— OVR-7.8-02 Pokud je povolen vzdálený přístup k systémům uchovávajícím nebo zpracovávajícím důvěrné údaje, musí být jako součást prvků požadovaných v rámci požadavku OVR-6.3-02 přijata a popsána formální politika.

— OVR-7.8-04 Skenování zranitelnosti požadované v rámci požadavku REQ-7.8-13 normy ETSI EN 319 401 [1] se provádí nejméně jednou za čtvrtletí.

— OVR-7.8-05 Penetrační test požadovaný v rámci požadavku REQ-7.8-17X normy ETSI EN 319 401 [1] se provádí nejméně jednou ročně.

— OVR-7.8-06 Firewally musí být nakonfigurovány tak, aby zabránily veškerým protokolům a přístupům, které nejsou nezbytné pro provoz poskytovatele služby ověřování platnosti podpisů.

11) 7.12 Ukončení poskytování služby ověřování platnosti podpisů a plány ukončení poskytování služby ověřování platnosti podpisů

— OVR-7.12-02 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].

12) 7.14 Dodavatelský řetězec

— OVR-7.14-01 Uplatňují se požadavky uvedené v normě ETSI EN 319 401 [2], bodě 7.14.

13) 8.1 Postup ověřování platnosti podpisu

— VPR-8.1-07 Aplikace ověřování platnosti (SVA) musí splňovat požadavky normy ETSI TS 119 101 [1], bodu 7.4 SIA 1 až SIA 4.

— VPR-8.1-11 [PODMÍNĚNÉ] Pokud je cílem služby ověřování platnosti podpisů validovat kvalifikované elektronické podpisy nebo kvalifikované elektronické pečetě, jako je tomu v souladu s čl. 32 odst. 1 (resp. článkem 40) nařízení (EU) č. 910/2014 [i.1], musí se postup ověřování platnosti řídit požadavky normy ETSI TS 119 172-4 [8].

14) 8.2 Protokol ověřování platnosti podpisu

— SVP-8.2-03 Odpověď na ověření platnosti podpisu musí obsahovat identifikátor objektu politiky služby ověřování platnosti podpisu.

15) 8.4 Zpráva o ověření platnosti podpisu

— SVR-8.4-02 Zpráva o ověření platnosti musí být v souladu s normou ETSI TS 119 102-2 [9].

— SVR-8.4-07 [PODMÍNĚNÉ] Pokud není politika ověřování platnosti podpisu zcela zpracována službou ověřování platnosti podpisu, musí zpráva kromě informací o ověřených omezeních obsahovat i informace o omezeních, která byla ignorována nebo přepsána.

— SVR-8.4-15 Ve zprávě o ověření platnosti musí být jasně uveden původ každého vstupního bodu (z podpisu, od klienta, od serveru).

— SVR-8.4-16 Zpráva o ověření platnosti musí být opatřena podpisem zprávy o ověření platnosti, který je digitálním podpisem poskytovatele služby ověřování platnosti podpisů.

— SVR-8.4-17 [PODMÍNĚNÉ] Pokud jsou zprávy o ověření platnosti podepsány, musí formát a cíl podpisu odpovídat normě ETSI TS 119 102-2 [9].

16) 9 Rámec pro vymezení politik služeb ověřování platnosti opírající se o politiku služeb vytvářejících důvěru vymezenou v tomto dokumentu:

— OVR-9-05 [PODMÍNĚNÉ] Při vytváření politiky služby ověřování platnosti podpisů na základě politiky služeb vytvářejících důvěru vymezené v tomto dokumentu se provede posouzení rizik z účelem vyhodnocení obchodních požadavků a stanovení bezpečnostních požadavků, které mají být zahrnuty do politiky pro uvedenou komunitu a použitelnost.

— OVR-9-06 [PODMÍNĚNÉ] Při vytváření politiky služby ověřování platnosti podpisů na základě politiky služeb vytvářejících důvěru vymezené v tomto dokumentu se tato politika schvaluje a upravuje v souladu s vymezeným procesem přezkumu, včetně odpovědnosti za její udržování.

— OVR-9-07 [PODMÍNĚNÉ] Při vytváření politiky služby ověřování platnosti podpisů na základě politiky služeb vytvářejících důvěru vymezené v tomto dokumentu musí existovat vymezený proces přezkumu, který zajistí, že politika bude podpořena prohlášeními o postupech.

— OVR-9-08 [PODMÍNĚNÉ] Při vytváření politiky služby ověřování platnosti podpisů na základě politiky služeb vytvářejících důvěru vymezené v tomto dokumentu zpřístupní poskytovatel služeb vytvářejících důvěru své uživatelské komunitě zásady podporované poskytovatelem služeb vytvářejících důvěru.

— OVR-9-09 [PODMÍNĚNÉ] Při vytváření politiky služby ověřování platnosti podpisů na základě politiky služeb vytvářejících důvěru vymezené v tomto dokumentu se účastníkům zpřístupní revize zásad podporovaných poskytovatelem služeb vytvářejících důvěru.

17) Příloha B (normativní) Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů podle článku 33 nařízení (EU) č. 910/2014:

— VPR-B-02 [PODMÍNĚNÉ] Pokud je poskytovatel služby ověřování platnosti podpisů poskytovatelem služby ověřování platnosti kvalifikovaných podpisů, musí být provádění v souladu s normou ETSI TS 119 172-4 [8].

— POZNÁMKA 2 neplatné.

— OVR-B-04 [PODMÍNĚNÉ] Pokud je poskytovatel služby ověřování platnosti podpisů poskytovatelem služby ověřování platnosti kvalifikovaných podpisů, musí testy uvedené v OVR-B-03 kontrolovat různé případy použití, a to pozitivní a negativní.

— VPR-B-11 [PODMÍNĚNÉ] Pokud je poskytovatel služby ověřování platnosti podpisů poskytovatelem služby ověřování platnosti kvalifikovaných podpisů, musí poskytovatel služby ověřování platnosti podpisů řídit hašovací výpočet (buď provádět výpočet na straně serveru, nebo řídit klienta, pokud je výpočet povolen na straně klienta).

— POZNÁMKA 5 neplatné.

— POZNÁMKA 6 neplatné.

— VPR-B-15 [PODMÍNĚNÉ] Pokud je poskytovatel služby ověřování platnosti podpisů poskytovatelem služby ověřování platnosti kvalifikovaných podpisů, musí být validační zpráva v souladu s normou ETSI TS 119 102-2 [9], aby splňovala požadavky VPR-B-13 až VPR-B-14.

— VPR-B-16 [PODMÍNĚNÉ] Pokud je poskytovatel služby ověřování platnosti podpisů poskytovatelem služby ověřování platnosti kvalifikovaných podpisů, musí být provádění v souladu s dohodnutými kryptografickými mechanismy, které přijala Evropská skupina pro certifikaci kybernetické bezpečnosti a zveřejnila agentura ENISA [10] pro použití vhodných šifrovacích technik při poskytování kvalifikovaných služeb ověřování platnosti kvalifikovaných elektronických podpisů.

18) Příloha C (informativní) Mapování požadavků na nařízení (EU) č. 910/2014, oddíl „Poskytování ověření platnosti v souladu s čl. 32 odst. 1“, druhý odstavec:

— Aby bylo zajištěno, že jsou ověřeny všechny podmínky požadované v čl. 32 odst. 1 a článku 40 nařízení (EU) č. 910/2014 [i.1], je zapotřebí správný ověřovací algoritmus. Poskytuje stejný deterministický výsledek pro podpis nebo pečeť podrobené ověření platnosti. Politika ověřování platnosti podpisu je pro tento účel klíčová. S ohledem na to byla vydána norma ETSI TS 119 172-4 [8] založená na algoritmu ověřování platnosti stanoveném v normě ETSI EN 319 102-1 [3].

2. Pro normu ETSI TS 119 172-4

1) 2.1 Normativní odkazy:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) „Elektronické podpisy a důvěryhodné infrastruktury (ESI); Postupy pro vytváření a ověřování platnosti digitálních podpisů AdES; Část 1: Vytvoření a ověření platnosti“.

— Všechny odkazy na normu „ETSI TS 119 102-1 [1]“ se považují za odkazy na normu „ETSI EN 319 102-1 [1]“.

— [2] ETSI TS 119 612 V2.3.1 (2024-11) „Elektronické podpisy a infrastruktury (ESI); Důvěryhodné seznamy“.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) „Elektronické podpisy a infrastruktury (ESI); Politické a bezpečnostní požadavky na aplikace pro vytváření podpisů a ověřování platnosti podpisů“.

2) 4.2 Omezení ověřování a ověřovací postupy, požadavek REQ-4.2-03, oddíl „X.509 omezení ověřování“, písm. c):

— i) pokud certifikát koncového subjektu představuje zdroj důvěry, omezení RevocationCheckingConstraints se nepoužijí;

— ii) pokud certifikát koncového subjektu nepředstavuje zdroj důvěry, nastaví se omezení RevocationCheckingConstraints na hodnotu „eitherCheck“, jak je vymezeno v normě ETSI TS 119 172-1 [3], bodě A.4.2.1, tabulce A.2, řádcích (m)2.1;

— iii) pokud certifikát koncového subjektu představuje zdroj důvěry, omezení RevocationFreshnessConstraints vymezená v normě ETSI TS 119 172-1 [3], bodě A.4.2.1, tabulce A.2, řádcích (m)2.2 se nepoužijí;

— iv) pokud certifikát koncového subjektu nepředstavuje zdroj důvěry, omezení RevocationFreshnessConstraints vymezená v normě ETSI TS 119 172-1 [3], bodě A.4.2.1, tabulce A.2, řádcích (m)2.2 se použijí s maximální hodnotou 24 hodin pro podpisový certifikát. Pro jiné certitikáty než podpisový certifikát, včetně certifikátů podporujících časová razítka, se hodnota RevocationFreshnessConstraints nenastavuje.

3) 4.4 Proces kontroly technické použitelnosti (pravidel)

— REQ-4.4.2-03 Pokud některá z kontrol uvedených v požadavku REQ-4.4.2-01 selže, pak:

a) proces se zastaví;

b) podpis je technicky určen jako neurčitý, tj. ani jako kvalifikovaný elektronický podpis EU, ani jako kvalifikovaná elektronická pečeť EU;

c) výše uvedený výsledek a výsledky procesů všech meziprocesů se promítnou do zprávy o kontrole pravidel použitelnosti podpisu.