MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Metodický návod pro ověřování platnosti uznávaných elektronických podpisů a elektronických pečetí.

Historie dokumentu:

Verze	*Vytvořeno*	*Autor*	*Poznámka*	*Status*
1	13.02.2016	FB	první draft	Návrh
2	14.03.2016	FB,MK	Přidán odstavec k ověření elektronických časových razítek, další úpravy	Návrh
3	10.04.2016	FB	Dokument upraven na základě komentářů členů pracovní skupiny č. 1	Návrh
4	25.04.2016	Kolektiv EG	Finalizace úprav, jazyková korektura, sladění textu. Verze před schválením řídícím výborem nařízení eIDAS.	Návrh
5	24.10.2016	FB	Aktualizace vzhledem k zák. 297/2016 Sb.	Řídící výbor vzal materiál na vědomí.

Obsah

1. Účel dokumentu

Dokument slouží jako metodický návod pro ověřování platnosti uznávaných elektronických podpisů a uznávaných elektronických pečetí. Podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „zák. č. 297/2016 Sb.“) se uznávaným elektronickým podpisem rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis (§ 6 odst. 2 zák. č. 297/2016 Sb.). Uznávanou elektronickou pečetí se rozumí zaručená elektronická pečeť založená na kvalifikovaném certifikátu pro elektronickou pečeť nebo kvalifikovaná elektronická pečeť (§ 9 odst. 2 zák. č. 297/2016 Sb.).

V úvodu je třeba říci, že tento návod nemá zavazující povahu, jedná se o výklad jednotlivých požadavků stanovených v nařízení eIDAS Ministerstvem vnitra. Legislativně je oblast ověřování platnosti uznávaných elektronických podpisů a uznávaných elektronických pečetí zakotvena zejména v:

- 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 (dále jen „nařízení eIDAS“),
- zák. č. 297/2016 Sb. - http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38075,
- prováděcím 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.

Metodický návod má za cíl rozvést obecné požadavky nařízení na ověřování platnosti kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí vzhledem k tomu, že požadavky stanovené v nařízení eIDAS jsou pouze obecného charakteru. Jak je stanoveno v zák. č. 297/2016 Sb., ustanovení čl. 32 odst. 1 písm. a) až e), g) a h) nařízení eIDAS se použijí na ověřování platnosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu pro elektronický podpis a na ověřování platnosti zaručené elektronické pečetě založené na kvalifikovaném certifikátu pro elektronické pečetě obdobně.

2. Články 32 a 40 nařízení eIDAS

Článek 32 - Požadavky na ověřování platnosti kvalifikovaných elektronických podpisů

1. Postup ověření platnosti kvalifikovaného elektronického podpisu potvrdí platnost kvalifikovaného elektronického podpisu, pokud:

a) certifikát, na němž je podpis založen, byl v okamžiku podpisu kvalifikovaným certifikátem pro elektronický podpis, jenž je v souladu s přílohou I;

b) kvalifikovaný certifikát byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a v okamžiku podpisu byl platný;

c) data pro ověřování platnosti podpisu odpovídají datům poskytnutým spoléhající se straně;

d) spoléhající se straně je řádně poskytnut jedinečný soubor dat identifikujících podepisující osobu v certifikátu;

e) pokud byl v okamžiku podpisu použit pseudonym, je jeho použití jednoznačně sděleno spoléhající se straně;

f) elektronický podpis byl vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů;

g) nebyla ohrožena integrita podepsaných dat;

h) v okamžiku podpisu byly splněny požadavky stanovené v článku 26.

2. Systém použitý k ověření platnosti kvalifikovaného elektronického podpisu musí poskytovat spoléhající se straně řádný výsledek postupu ověření platnosti a umožňovat jí zjistit jakékoli problémy týkající se bezpečnosti.

3. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro ověřování platnosti kvalifikovaných elektronických podpisů. Pokud ověřování platnosti kvalifikovaných elektronických podpisů vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Článek 40 - Ověřování platnosti a uchovávání kvalifikovaných elektronických pečetí

Na ověřování platnosti a uchovávání kvalifikovaných elektronických pečetí se použijí přiměřeně články 32, 33 a 34.

3. Znění § 12 zák. č. 297/2016 Sb.

§ 12 - Ověřování platnosti zaručeného elektronického podpisu a zaručené elektronické pečetě

Ustanovení čl. 32 odst. 1 písm. a) až e), g) a h) Nařízení se na ověřování platnosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu pro elektronický podpis a na

ověřování platnosti zaručené elektronické pečetě založené na kvalifikovaném certifikátu pro elektronické pečetě použijí obdobně.

4. Výklad jednotlivých požadavků článku 32 nařízení eIDAS

Požadavky na ověření kvalifikovaných elektronických pečetí vycházejí z požadavků na ověření platnosti kvalifikovaných elektronických podpisů, proto níže v textu se mluví pouze o elektronickém podpisu. Z technického pohledu jsou zaručené elektronické podpisy a zaručené elektronické pečeti obdobné.

4.1 Požadavky písm. a) *„certifikát, na němž je podpis založen, byl v okamžiku podpisu kvalifikovaným certifikátem pro elektronický podpis, jenž je v souladu s přílohou I;“*

V prvé řadě je nutné určit čas vzniku elektronického podpisu – za okamžik vzniku elektronického podpisu MV doporučuje zvolit okamžik, kdy spoléhající se strana může prohlásit, že zaručený elektronický podpis již existoval:

a) datum a čas doručení elektronicky podepsaného dokumentu nebo
b) nejčasnější časový okamžik, ve kterém již prokazatelně existoval zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis, jehož platnost je ověřována (čas připojení důvěryhodného elektronického časového razítka, v případě existence více důvěryhodných elektronických časových razítek čas připojení nejstaršího z nich).

Není-li k zaručenému elektronickému podpisu založenému na kvalifikovaném certifikátu pro elektronický podpis připojeno či logicky spojeno platné důvěryhodné elektronické časové razítko, je nejčasnějším okamžikem, ve kterém již prokazatelně existoval zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis, jehož platnost je ověřována, okamžik, kdy došlo k doručení nebo jinému předání elektronického dokumentu podepsaného tímto podpisem.

Spoléhající se strany by tedy měly určit jako okamžik podpisu nejstarší časový okamžik, kdy mohou prohlásit, že elektronický podpis již existoval.

[pozn. modifikace §3 odst. 1 vyhlášky 212/2012 Sb. a odůvodnění]

Pod pojmem důvěryhodné elektronické časové razítko rozumíme buď kvalifikované elektronické časové razítko dle nařízení eIDAS nebo elektronické časové razítko vydané kvalifikovaným poskytovatelem služeb vytvářejících důvěru, kterému byl udělen kvalifikovaný status v souvislosti s jinou poskytovanou službou (za důvěryhodné elektronické časové razítko se tak považuje elektronické časové razítko vydané stávajícími akreditovanými poskytovateli certifikačních služeb vzhledem k tomu, že po 1. červenci 2016 se tito poskytovatelé stanou kvalifikovanými poskytovateli služeb vytvářejících důvěru nabízející službu vydávání kvalifikovaných certifikátů pro elektronický podpis).

Aplikace pro ověření platnosti by měla zkontrolovat, zda certifikát, na němž je zaručený elektronický podpis založen, byl vydán službou, která byla službou vydávání kvalifikovaných certifikátů pro elektronický podpis a byla poskytována kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Zde je nutné využít informací vedených v důvěryhodných seznamech podle článku 22 nařízení eIDAS, tj.:

- Zkontrolovat, zda služba, která posuzovaný certifikát vydala, je vedená v důvěryhodném seznamu některého ze členských států. Pokud ano, pak:
- Zkontrolovat, zda služba má v důvěryhodném seznamu přiřazen identifikátor služby (Service type identifier) „http://uri.etsi.org/TrstSvc/Svctype/CA/QC“,
- Zkontrolovat, zda služba je poskytována kvalifikovaným poskytovatelem služeb vytvářejících důvěru (Service current status) „http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted“,
- Zkontrolovat, zda čas v poli „Current status starting date and time“ je menší než čas ke kterému je zkoumán kvalifikovaný status certifikátu případně využít historické informace o službě, pokud byl kvalifikovaný status službě odebrán,
- Zkontrolovat, zda certifikát vyhovuje specifikům dané služby (Service information extensions).

Pokud certifikát vyhovuje všem požadavkům, pak jej lze považovat za kvalifikovaný certifikát pro elektronický podpis.

Soulad vydaného kvalifikovaného certifikátu pro elektronický podpis s požadavky stanovenými v příloze I. nařízení eIDAS lze předpokládat na základě skutečnosti, že byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru, jehož povinností a zodpovědností je, aby byly požadavky stanovené v příloze I. nařízení eIDAS dodrženy, tj.:

Kvalifikované certifikáty pro elektronické podpisy obsahují:

a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis;

b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen, a

— v případě právnické osoby: název a případné registrační číslo uvedené v úředních záznamech,

— v případě fyzické osoby: jméno osoby;

c) alespoň jméno podepisující osoby nebo pseudonym. Je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;

d) data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro vytváření elektronických podpisů;

e) označení začátku a konce doby platnosti certifikátu;

f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru;

g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;

h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g);

i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu;

j) pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.

4.2. Požadavky písm. b) *„kvalifikovaný certifikát byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a v okamžiku podpisu byl platný;“*

Kontrola, zda certifikát, na kterém je podpis založen, byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru, byla provedena v předchozím kroku oproti údajům vedeným v příslušném důvěryhodném seznamu, kde je služba vydávání kvalifikovaných certifikátů pro elektronické podpisy vedena.

Kontrola platnosti certifikátu, na kterém je podpis založen, by měla zahrnovat:

- Sestavení platné certifikační cesty posuzovaného certifikátu.
- Kontrola, zda okamžik podpisu (určení času viz předchozí bod) spadá do intervalu platnosti certifikátu,
- ověření platnosti zaručeného elektronického podpisu nebo zaručené elektronické pečeti poskytovatele, kterým je posuzovaný certifikát opatřen,
- kontrola zneplatnění posuzovaného certifikátu v souladu s certifikační politikou k okamžiku podpisu a za pomoci služby, která je uvedena v posuzovaném certifikátu (nejčastěji pomocí CRL nebo OSCP),
- ověření platnosti zaručeného elektronického podpisu nebo zaručené elektronické pečeti poskytovatele, kterým je opatřen seznam zneplatněných certifikátů (CRL) nebo informace o stavu certifikátu (např. OCSP odpověď),
- provedení kontroly platnosti certifikátu pro nadřazené certifikáty v platné certifikační cestě.

Informace o platnosti certifikátů mohu být buď získány od kvalifikovaného poskytovatele služeb vytvářejících důvěru „na dálku“ nebo mohou být rovněž součástí podepsaného dokumentu (v tomto

případě jsou k podpisu přidány všechny potřebné certifikáty včetně revokačních informací). Pokud jsou informace o platnosti certifikátů vzaty přímo z elektronicky podepsaného dokumentu, aplikace musí ověřit, že revokační informace jsou starší více než 24 hodin od okamžiku vzniku podpisu. Toto ověření se provádí buď oproti času připojeného důvěryhodného elektronického časového razítka, nebo oproti času, kdy spoléhající se strana může prohlásit, že zaručený elektronický podpis již existoval. V případě připojeného důvěryhodného elektronického časového razítka se jedná tedy o využití funkcionality vyšší úrovně zaručeného elektronického podpisu, kdy se k samotnému zaručenému elektronickému podpisu přidává rovněž podpisové časové razítko a validační informace (LT úroveň - Long Term level).

4.3. Požadavky písm. c) „data pro ověřování platnosti podpisu odpovídají datům poskytnutým spoléhající se straně;“

Zajistit, aby aplikace pro kontrolu platnosti elektronického podpisu použila pro ověření platnosti elektronického podpisu data, která se mají použít pro ověření platnosti podpisu (pro dešifrování elektronického podpisu použít příslušný veřejný klíč, který je uveden v certifikátu a tento certifikát je obsažen v atributu elektronického podpisu nebo na který je odkazováno v atributech podpisu případně v certifikátu, který je poskytnut aplikaci externě). Podpisový certifikát musí být zkontrolován oproti referencím uvedeným v atributech elektronického podpisu. Například kontrola otisku odkazovaného certifikátu – zda otisk certifikátu uvedený v atributech certifikátu souhlasí s vypočítaným otiskem za použití příslušného algoritmu.

Pokud jsou v atributech podpisu uvedeny informace např. o vydavateli certifikátu, sériové číslo certifikátu, zkontrolovat jej rovněž oproti podpisovému certifikátu.

4.4. Požadavky písm. d) „spoléhající se straně je řádně poskytnut jedinečný soubor dat identifikujících podepisující osobu v certifikátu;“

Uživateli jsou přehledným způsobem zobrazeny údaje obsažené v kvalifikovaném certifikátu pro elektronický podpis – jméno a příjmení podepisující osoby, případně další atributy z předmětu certifikátu, sériové číslo certifikátu, údaje jednoznačně identifikující kvalifikovaného poskytovatele služeb vytvářejících důvěru,…

4.5. Požadavky písm. e) „pokud byl v okamžiku podpisu použit pseudonym, je jeho použití jednoznačně sděleno spoléhající se straně;“

Navazuje na požadavky z bodu d), v případě použití pseudonymu v certifikátu musí být uživateli jasně sděleno, že certifikát obsahuje pseudonym podepisující osoby místo pravého jména podepisující osoby.

4.6. Požadavky písm. f) *„elektronický podpis byl vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů;“*

Na základě údajů získaných z kvalifikovaného certifikátu pro elektronický podpis, na kterém je elektronický podpis založen, určit, zda data pro vytváření elektronických podpisů (soukromý klíč) spojená s daty pro ověřování platnosti elektronických podpisů jsou bezpečně uložena v kvalifikovaném prostředku pro vytváření elektronických podpisů. Pokud jsou data pro vytváření elektronických podpisů uložena v kvalifikovaném prostředku pro vytváření elektronických podpisů, kvalifikovaný certifikát pro elektronický podpis má obsahovat příslušnou informaci (např. ve standardu ETSI EN 319 412-5 vyjádřeno pomocí Qualified Certificate Statement vkládaného do kvalifikovaného certifikátu).

Údaj, zda data pro vytváření elektronických podpisů jsou obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů, je možné určit i na základě informací z důvěryhodného seznamu, pokud je příslušný kvalifikátor použit u dané služby. Viz technické specifikace ETSI TS 119 612 v 2.1.1:

- ***QCWithSSCD ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD")**: to indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being qualified, have their private key residing in an SSCD;*
- ***QCNoSSCD ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoSSCD")**: to indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being qualified, do not have their private key residing in an SSCD;*
- ***QCSSCDStatusAsInCert ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCSSCDStatusAsInCert")**: to indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being qualified, do contain proper machine processable information about whether or not their private key residing in an SSCD;*
- ***QCWithQSCD ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD")**: to indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being qualified, have their private key residing in a QSCD;*
- ***QCNoQSCD ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD")**: to indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being qualified, do not have their private key residing in a QSCD;*
- ***QCQSCDStatusAsInCert ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDStatusAsInCert")**: to indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being qualified, do contain proper machine processable information about whether or not their private key residing in a QSCD;*
- ***QCQSCDManagedOnBehalf ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf")**: to*

indicate that all certificates identified by the applicable list of criteria, when they are claimed or stated as being qualified, have their private key residing in a QSCD for which the generation and management of that private key is done by the qualified TSP on behalf of the entity whose identity is certified in the certificate;

4.7. Požadavky písm. g) *„nebyla ohrožena integrita podepsaných dat;“*

Provedení kontroly, zda nedošlo ke změně podepsaných dat po jejich elektronickém podepsání:

- Vypočítat otisk (hash) podepsaných dat podle stejného algoritmu, kterým byl spočítán otisk na straně podepisujícího.
- Dešifrovat elektronický podpis a získaný otisk porovnat s vypočteným otiskem podepsaných dat, zda se otisky shodují.

4.8. Požadavky písm. h) *„ v okamžiku podpisu byly splněny požadavky stanovené v článku 26.“*

Písmeno h) odkazuje na článek č. 26 nařízení eIDAS, který definuje požadavky na zaručené elektronické podpisy:

Zaručený elektronický podpis musí splňovat tyto požadavky:

a) je jednoznačně spojen s podepisující osobou;

b) umožňuje identifikaci podepisující osoby;

c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a

d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Tato kontrola souvisí se samotným formátem zaručeného elektronického podpisu – nejčastěji používanými formáty u nás PAdES, CAdES, XAdES. Je možné rovněž využít kontejner s přidruženým obsahem (ASiC - Associated Signature Container), jehož výchozí profil je definovaný v technických specifikacích ETSI.

Podle vydaného 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 eIDAS mají členské státy vyžadující zaručený elektronický podpis nebo zaručený elektronický podpis založený na kvalifikovaném certifikátu, jak je stanoveno v čl. 27 odst. 1 a 2 nařízení eIDAS, uznávat zaručený elektronický podpis XML, CMS nebo PDF na úrovni shody B, T nebo LT nebo prostřednictvím kontejneru s přidruženým podpisem, pokud jsou tyto podpisy v souladu s technickými specifikacemi uvedenými v příloze I:

Seznam technických specifikací pro zaručené elektronické podpisy XML, CMS nebo PDF a kontejner s přidruženým podpisem

Zaručené elektronické podpisy uvedené v článku 1 rozhodnutí musí vyhovovat jedné z následujících technických specifikací ETSI, s výjimkou bodu 9 uvedených specifikací:

výchozí profil XAdES	*ETSI TS 103171 v.2.1.1 ([1]).*
výchozí profil CAdES	*ETSI TS 103173 v.2.2.1 ([2]).*
výchozí profil PAdES	*ETSI TS 103172 v.2.2.2 ([3]).*

Kontejner s přidruženým podpisem uvedený v článku 1 rozhodnutí musí vyhovovat následujícím technickým specifikacím ETSI:

výchozí profil kontejneru s přidruženým podpisem	*ETSI TS 103174 v.2.2.1 ([4])*

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf
([4]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

Podle prováděcího rozhodnutí Komise (EU) 2015/1506 členské státy akceptují i jiné formáty zaručených elektronických podpisů a pečetí za předpokladu splnění podmínek stanovených v odkazovaném nařízení.

4.9. Požadavky odstavce 2 *„Systém použitý k ověření platnosti kvalifikovaného elektronického podpisu musí poskytovat spoléhající se straně řádný výsledek postupu ověření platnosti a umožňovat jí zjistit jakékoli problémy týkající se bezpečnosti.“*

Aplikace by měla jednoduše uživateli zobrazit výsledek ověření platnosti kvalifikovaného elektronického podpisu, dále informaci, že došlo k ověření zneplatnění certifikátů, apod.

5. Požadavky na ověřování platnosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu pro elektronický podpis a zaručené elektronické pečetě založené na kvalifikovaném certifikátu pro elektronické pečetě

Jak plyne ze zák. č. 297/2016 Sb., požadavky na ověřování platnosti kvalifikovaných elektronických podpisů a pečetí by se měly obdobně použít také na ověřování platnosti zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu pro elektronický podpis a zaručené elektronické pečetě založené na kvalifikovaném certifikátu pro elektronické pečetě.

Při ověřování platnosti zaručených el. podpisů nebo pečetí není nutné kontrolovat, zda soukromý klíč (data pro vytváření el. podpisů/pečetí) je uložen v kvalifikovaném prostředku pro vytváření el. podpisů nebo pečetí jelikož pro vytvoření těchto druhů podpisů/pečetí není použití prostředku vyžadováno.

6. Požadavky na ověřování platnosti zaručené elektronické pečeti založené na certifikátu pro elektronické pečetě vydaného kvalifikovaným poskytovatelem služeb vytvářejících důvěru

Pro přechodnou dobu 2 let lze namísto zaručené elektronické pečetě založené na kvalifikovaném certifikátu pro elektronické pečetě nebo kvalifikované elektronické pečetě použít rovněž zaručenou elektronickou pečeť založenou na certifikátu pro elektronické pečetě. Certifikát pro elektronickou pečeť musí být vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru (kterému byl udělen kvalifikovaný status v souvislosti s jinou poskytovanou službou). Kontrola, zda certifikát pro elektronickou pečeť byl vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru, se provádí za pomoci informací uvedených v důvěryhodných seznamech, tj. provede se kontrola, zda vydavatel certifikátu pro elektronickou pečeť, je uveden v některém z důvěryhodných seznamů jako kvalifikovaný poskytovatel služeb vytvářejících důvěru poskytující jinou kvalifikovanou službu vytvářející důvěru (např. vydávání kvalifikovaných certifikátů pro elektronický podpis).

MV doporučuje nejdříve z posuzovaného certifikátu zjistit, kde je poskytovatel, který vydal certifikát, usazen (lze zjistit z informací uvedených v položce „Vystavovatel certifikátu“) a v příslušném důvěryhodném seznamu členského státu se pokusit vyhledat tohoto poskytovatele.

Seznam umístění (webových adres) jednotlivých důvěryhodných seznamů členských zemí lze získat z dokumentu „List of Trusted List information as notified by Member States“ na stránkách EC:

PDF verze: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf

XML verze: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

případně lze rovněž využít nástroj „EU Trust Service status List (TSL) Analysis Tool“ dostupný na adrese: http://tlbrowser.tsl.website/tools/index.jsp.

Jméno poskytovatele služeb vytvářejících důvěru je v důvěryhodných seznamech uvedeno podle technických specifikací ETSI TS 119 612 v2.1.1 v části „TrustServiceProviderList“, konkrétně v tagu „TSP name“, obchodní jméno uvedeno v tagu „TSP trade name“, adresa v tagu „TSP Address“.

Při ověřování platnosti není nutné v tomto případě kontrolovat, zda certifikát pro elektronickou pečeť byl vydán jako kvalifikovaný (stačí zkontrolovat, že poskytovateli byl udělen kvalifikovaný status v souvislosti s jinou poskytovanou kvalifikovanou službou):

Tag „Service type identifier“ některé z poskytovaných služeb, musí obsahovat „kvalifikovanou“ URI:

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q

http://uri.etsi.org/TrstSvc/Svctype/PSES/Q

http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q

Poskytovateli musí být alespoň u jedné z těchto poskytovaných služeb udělen kvalifikovaný status v tagu „Service current status“ – vyjádřeno pomocí URI: "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted". MV doporučuje z webových stránek poskytovatele ověřit (odkaz na webové stránky poskytovatele bývají uvedeny v tagu „TSP electronic address“), zda daný poskytovatel opravdu službu vydávání certifikátů pro elektronické pečetě nabízí, aby se předešlo možnosti, kdy se jeden subjekt vydává za jiného.

7. Ověřování platnosti elektronické značky

Ověřování platnosti elektronické značky se provádí stejným postupem jako před zrušením zákona č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a vyhlášky č. 212/2012 Sb. o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu).

Na stránkách MV bude stále k dispozici evidence systémových certifikátů, na kterých jsou založeny elektronické značky systémových certifikátů pro elektronické značky.

8. Ověřování elektronického časového razítka

Zák. č. 297/2016 Sb. stanovuje povinnost pro veřejnoprávního podepisujícího a pro osobu, která právně jedná při výkonu své působnosti, opatřit podepsaný či zapečetěný dokument, kterým právně jedná, kvalifikovaným elektronickým časovým razítkem. V přechodných ustanoveních zák. č. 297/2016 Sb. (§ 19) je stanovena přechodná lhůta dvou let, po kdy je možné místo kvalifikovaného elektronického časového razítka použít elektronické časové razítko, které bylo vydáno kvalifikovaným poskytovatelem služeb vytvářejících důvěru (jemuž byl udělen kvalifikovaný status v souvislosti s jinou poskytovanou službou) – zjištění této skutečnosti viz návodný postup z bodu 6. V případě, že dokument obsahuje jediné elektronické časové razítko, jeho platnost se ověřuje k aktuálnímu časovému okamžiku. Pokud dokument obsahuje více časových razítek, ověřuje se platnost elektronického časového razítka k okamžiku připojení nejbližšího „mladšího (novějšího)“ elektronického časového razítka.

Problematikou ověřování časových razítek se zabývala již vyhláška o ověřování platnosti zaručeného elektronického podpisu. Ověřování platnosti elektronického časového razítka zahrnuje:

a) Ověření vazby mezi daty a připojeným elektronickým časovým razítkem. Ověření vazby mezi daty a připojeným elektronickým časovým razítkem se provádí podle standardu kryptografické hashovací funkce odpovídající funkci použité při výpočtu otisku dat uvedeného v elektronickém časovém razítku.

b) Ověření platnosti elektronického „instrumentu“, který zajišťuje neporušenost obsahu elektronického časového razítka, respektive zajišťuje možnost zjištění případného pozměnění. Tento elektronický instrument je obvykle zaručený elektronický podpis nebo zaručená elektronická pečeť nebo elektronická značka poskytovatele.

c) Ověření platnosti certifikátu, na kterém je založen elektronický „instrument“ z bodu b.

Při ověřování, zda se jedná o kvalifikované elektronické časové razítko, je nutné využít informace uvedené v důvěryhodném seznamu členského státu.

9. Kdy ověřovat finální platnost uznávaného elektronického podpisu nebo uznávané elektronické pečeti

Otázka platnosti uznávaného elektronického podpisu nebo uznávané elektronické pečeti úzce souvisí s otázkou platnosti samotného kvalifikovaného certifikátu, na kterém je podpis či pečeť založena.

Problematika zneplatnění kvalifikovaných certifikátů je řešena v nařízení eIDAS v odstavci 3 článku 24:

„Jestliže se kvalifikovaný poskytovatel služeb vytvářejících důvěru 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."

Je důležité zmínit, že zneplatnění certifikátu nabývá účinnosti až po zveřejnění informace o zneplatnění, čili až od doby, kdy spoléhající se strany mají možnost zjistit, že daný certifikát byl zneplatněn. Na rozhodnutí zneplatnit kvalifikovaný certifikát a na zveřejnění tohoto zneplatnění mají kvalifikovaní poskytovatelé služeb vytvářejících důvěru stanovenu lhůtu 24 hodin, která se počítá od okamžiku, kdy obdrželi žádost o zneplatnění. Není tedy možné tzv. zpětné zneplatnění kvalifikovaného certifikátu – například v případě CRL seznamů by se nemělo stávat, aby datum vydání prvního CRL seznamu, kde je konkrétní certifikát zneplatněn, bylo pozdější než datum zneplatnění konkrétního certifikátu uvedeného v detailech zneplatnění konkrétního certifikátu.

Aby spoléhající se strana měla jistotu, že kvalifikovaný certifikát, na kterém je založen uznávaný elektronický podpis nebo uznávaná elektronická pečeť, nebyl zneplatněn v době vytvoření podpisu nebo pečeti, měla by spoléhající se strana počkat s finálním ověřením platnosti uznávaného elektronického podpisu nebo uznávané elektronické pečeti až 24 hodin od okamžiku vzniku podpisu nebo okamžiku vzniku pečeti. V případě, kdy ověření probíhá minimálně 24 hodin po prokazatelném vzniku podpisu/pečeti, není nutné čekat 24 hodin. V certifikačních politikách pro vydávání kvalifikovaných certifikátů se kvalifikovaný poskytovatel může nicméně zavázat tento čas zkrátit.

10. Zdroje

[1] 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.

[2] Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce.

[3] VYHLÁŠKA č. 212/2012 Sb. ze dne 13. června 2012 o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka.

[4] ETSI TS 119 102-1 V1.0.1 (2015-07) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

[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.