Elektronické podpisy v elektronických nástrojích po jejich certifikaci

Michaela Poremská*

Úvod

Co je to elektronický podpis se lze srozumitelně dočíst v nejrůznějších odborných článcích[1] a samozřejmě v zákoně o elektronickém podpisu (zákon č. 227/2000 Sb.) a ostatních publikacích.[2] Tento článek se vysvětlením, co je to elektronický podpis nebude zabývat. Jeho cílem je zamyslet se nad používáním elektronických podpisů v elektronických nástrojích pro zadávání veřejných zakázek. Touto problematikou, si dovoluji uvést, se zabývá praxe provozovatelů elektronických nástrojů každý den, leč nikdo z praxe k ní prozatím nenapsal nic, co by ji činilo srozumitelnější. Jsem názoru, že používání elektronických podpisů v elektronických nástrojích je specifikou problematikou, ostatně jako všechno co se týká elektronizace veřejného zadávání.

Úvodem je však třeba si uvědomit, že elektronické nástroje pro zadávání veřejných zakázek využívají v souladu se zákonem č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále také „zákon o veřejných zakázkách" nebo „ZVZ") platný zaručený elektronický podpis založený na kvalifikovaném certifikátu (dále také „zaručený podpis"), ale provozovatelé elektronických nástrojů jsou osoby odlišné od akreditovaných certifikačních autorit vydávajících zaručené podpisy, takže nemají na podpisy vliv.

Tento článek je pouhou úvahou nad elektronickými podpisy ve veřejných zakázkách a nemá ambice tuto oblast zcela zmapovat.

Úvaha nad použitím elektronických podpisů v elektronických nástrojích podle předcházející právní úpravy

Otázka, která při používání elektronického nástroje, dle mého názoru, zůstává, je, zda nepodepsaná zadávací dokumentace byla platným dokumentem či nikoliv. Dovolím si nyní v krátkosti uvést, ve kterém případě jsem názoru, že ano.

Jednalo se především o případ, kdy se dokumentace uveřejnila přímým a neomezeným dálkovým přístupem či zpřístupnila v elektronickém nástroji. Uvedená úvaha však **ne**reflektuje právní úpravu účinnou k 1. 7. 2011, od kdy je nutné používat certifikovaný elektronický nástroj a nikoliv již atestovaný.

Před certifikací nebylo totiž striktně stanoveno, že je nutné používat elektronický podpis na zadávací doku-

* JUDr. Michaela Poremská, odborná asistentka na Ústavu práva a humanitních věd Provozně-ekonomické fakulty Mendelovy univerzity v Brně.

[1] Např. Matejka, J, Chum, V. K právní úpravě elektronického podpisu. Bulletin advokacie, 2002, č. 3, s. 27 an., Černý, P. Procesní účinky elektronického podání v občanském soudním řízení. [citováno 27. června 2011]. Dostupný z:http://www.ipravnik.cz/cz/clanky/civilni-proces/art_4986/procesni-ucinky-elektronickeho-podani-v-obcanskem-soudnim-rizeni.aspx. Dále viz poznámku 8 pod čarou.

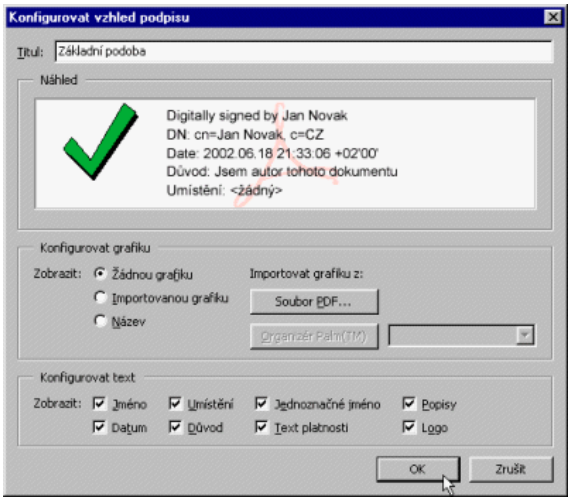
[2] Např. Budiš, P. Elektronický podpis a jeho aplikace v praxi. 1. vydání. Olomouc: ANAG, 2008, 153 s.

mentaci jako je tomu v příloze vyhlášky č. 9/2011 Sb. – viz T7 Neomezené poskytování zabezpečeného dokumentu dálkovým přístupem.

Funkce elektronického nástroje jsou nastaveny tak, že po vložení zadávacích podmínek do nástroje a následně zahájení zakázky již není možné se zadávacími podmínkami manipulovat, tzn. je mazat či měnit. Na tuto transparentnost „měl dohlížet“ atestovaný (poznámka autorky – připomínám, že úvaha se týká právního stavu před 1. 7. 2011) elektronický nástroj. Kdo dokumentaci (podmínky) vložil a kdy lze z nástroje zjistit. Vzhledem k tomu, že dokumentaci je možné uveřejnit „neomezeným a přímým dálkovým přístupem“ v síti Internet, tzn. může si ji prohlédnout a stáhnout kdokoliv, striktně bych nedoporučila uveřejňovat vlastnoručním podpisem podepsané zadávací podmínky. Mohlo by se tak jednoduše stát, například že naše příští kontrola bankovního účtu bude spojena s nepříjemným zjištěním, že na účtu nemáme finanční prostředky či dokonce jsme „v mínusu,“ a to proto, že někdo zkopíroval náš podpis a použil jej na listinný platební příkaz.

Nutnou podmínkou pro platnost zadávací dokumentace, podle mého názoru, bylo, že vložení (nahrání) dokumentu do elektronického nástroje provedla osoba oprávněná.

U elektronických podpisů je, podle mého názoru, prozatím situace jiná. Elektronicky se nepodepisujeme „vizuelně,“ ale jedná se o data, a tudíž zneužití „obrázku“ podpisu je v tomto případě, podle mého názoru, podstatně menší.



Orázek: Krejčí, R. Elektronický podpis v pdf. [citováno 7. listopadu 2011]. Dostupný z: http://www.grafika.cz/art/pdf/pdfpodmis.html.

Podle platné právní úpravy použití elektronického podpisu na zadávací dokumentaci explicitně stanovuje již zmíněná vyhláška č. 9/2011 Sb. První problém, který se, podle mého názoru,v tomto případě objevuje je ten, že stále málo lidí má elektronický podpis.

Způsoby podepisování v elektronickém nástroji

Způsoby podepisování v elektronickém nástroji bychom mohli identifikovat několikeré. Reagujeme tak na skutečnost, že prozatím velmi málo osob má zaručený podpis a tudíž se významně uplatňuje kombinace vlastnoručního podpisu, zaručeného podpisu či zastoupení (viz dále).

Můžeme, dle mého soudu, definovat následující přípustné základní způsoby podepisování v elektronickém nástroji (a věřím, že existují další):

1. **Podepíše-li návrh smlouvy (nabídku) elektronicky platným zaručeným podpisem založeným na kvalifikovaném certifikátu nebo vlastnoručně osoba(y) oprávněná(é) jednat jménem uchazeče** (statutární orgán, resp. člen/členové dle výpisu z OR či jiné evidence), tj. příslušné soubor/y elektronicky/ vlastnoručně podepíše (vložit do elektronického nástroje E-ZAK a odeslat je již následně přes svůj uživatelský účet nemusí – viz variantu 2.) nebo soubory vloží **přes svůj uživatelský účet** do elektronického nástroje E-ZAK osoba(y) oprávněné jednat jménem uchazeče a soubory odešle (podá nabídku) a podepíše elektronický úkon v elektronickém nástroji E-ZAK (vlastní soubory **musí** být elektronicky podepsány) – není potřeba doložit žádnou plnou moc.

2. **Podepsaný platným zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu nebo vlastnoručně návrh smlouvy (nabídka) osobou(ami) oprávněnými jednat jménem uchazeče** (státutární orgán, resp. člen/členové dle výpisu z OR či jiné evidence), tj. příslušné soubor/y vloží a soubory odešle (podá nabídku) a elektronický úkon **ve svém uživatelském účtu** podepíše v elektronickém nástroji E-ZAK jiná osoba dodavatele, např. zaměstnanec dodavatele – není nutné doložit plnou moc pro osobu, která zaručeným elektronickým podpisem podepsala odeslanou zprávu s nabídkou.

3. **Návrh smlouvy nebo Doklady o kvalifikaci (nabídku) v listinné nebo elektronické podobě podepíše jiná osoba než osoba(y) oprávněná jednat jménem dodavatele** (statutární orgán, resp. člen/členové dle výpisu z OR či jiné evidence) – neskenovaný dokument (soubor např. ve formátu PDF), tj. příslušné soubor/y podá **přes svůj uživatelský účet** jiná osoba než osoba(y) oprávněná jednat jménem dodavatele – je nutné doložit plnou moc pro osobu, která podepsala listinné nebo elektronické dokumenty. Zadavatel uvádí, že postačí prostá kopie zmíněné plné moci, tj. nedisponuje-li statutární orgán dodavatele (členové statutárního orgánu) platným zaručeným podpisem založeným na kvalifikovaném certifikátu, je možné doložit naskenovanou listinnou podobu plné moci (např. ve formátu PDF), z níž bude patrný vlastnoruční podpis osob(y)

oprávněné(ých) jednat jménem dodavatele (udělující plnou moc).

Ve všech výše uvedených případech je možné místo plné moci užít pověření apod.

Zastoupení

Prozatím obtížnou otázkou k zodpovězení je, podle mého názoru, zda zástupce (nejčastěji smluvní podle § 31 an.zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů; dále jen „OZ“) může činit úkony v elektronickém nástroji v uživatelském účtu dodavatele čili zastoupeného (zmocnitele). Jsem názoru, že obdobně jako činit operace pomocí přímého bankovnictví (dnes nejčastěji internetového) nemůže v uživatelském účtu dělat nikdo jiný než oprávněný (přihlášený) uživatel, tak nemůže za zástupce (nejčastěji právního; zmocněnce) činit úkony sám zastoupený (zmocnitel). Pokud by je činil sám zastoupený (zmocnitel), nejednalo by se, dle mého názrou, o zastoupení zastoupeného (zmocnitele), ale o zastoupení zástupce (nejjednodušší výklad je, že by činil úkony zastoupený sám, a tudíž by nebyl zastoupen), neboť zástupce (zmocněnec) je povinen jednat osobně (§ 24 OZ).

Vzhledem k tomu, že dodavatel sám má většinou možnost spravovat uživatelské účty, a tudíž i zřizovat účty pro další uživatele, měl by vytvořit i účet zástupci (zmocněnci), pokud chce, aby jej zastupoval, anebo se může zástupce (zmocněnec) zaregistrovat do elektronického nástroje sám.

Představíme-li si danou situaci tak, že by se realizovala v listinné podobě, pak ten, kdo by dával listinu zástupce do listinné obálky, by nebyl identifikován na rozdíl od odesílatele přípisu v elektronické podobě, který činí elektronický úkon, např. odesílá-li námitky datovou zprávou (viz § 149 odst. 4 ZVZ).

Pokud bychom označili odesílatele za „pouhého pošťáka,“ jak by se odlišovaly úkony zástupce (zmocněnce) a jednání zastoupeného (zmocnitele čili dodavatele)? Podle mého názoru, nijak, a tím by se zcela popřela elektronizace a výhody z ní plynoucí, např. padělání listin, kdy není zřejmé, kdo listinu padělal a kdo ji „pouze“ odeslal.

Uživatelské účty

Další úzce související problematikou s problematikou podepisování „pouhého pošťáka“ nebo zástupce či dodavatele, je užívání jednoho uživatelského účtu více osobami, a to především v situaci, kdy je podávána (odesílána) nabídka. Při odesílání nabídky je třeba daný elektronický úkon (datovou zprávu) podepsat zaručeným podpisem. Často dochází v praxi k situaci, že z uživatelského účtu osoby A je odeslána nabídka a datová zpráva (elektronický úkon) s nabídkou je podepsán osobou B a samotná nabídka osobou C.

Podle mého názoru se jedná o rozpor, na který se okamžitě přijde při otevírání nabídek. Podle § 71 odst. 8 písm. b) ZVZ komise pro otevírání nabídek kontroluje podpis oprávněné osoby na návrhu smlouvy. Jedná se o podpis oprávněné osoby, jestliže samotnou nabídku podepsala osoba oprávněná, ale odlišná od vlastníka daného uživatelského účtu? Podle mého názoru ano. Problém nastává až v případě, jestliže nabídku podepíše osoba, která není oprávněna podle výpisu z obchodního rejstříku či jiné evidence a navíc je nabídka odeslána z uživatelského účtu třetí osoby. Podle mého názoru, chyby, které mohou nastat, a tudíž není možné konstatovat, že návrh smlouvy je podepsán osobou oprávněnou, jsou minimálně tyto:

1. Uživatelský účet osoby A – datová zpráva podepsána osobou B, která není osobou oprávněnou jednat jménem ani za dodavatele a není doložena plná moc či jiné oprávnění – nabídka je podepsána osobou C, která není osobou oprávněnou jednat jménem ani za dodavatele a není doložena plná moc či jiné oprávnění
2. Uživatelský účet osoby A – datová zpráva podepsána osobou B, která není osobou oprávněnou jednat jménem ani za dodavatele a není doložena plná moc či jiné oprávnění – nabídka není podepsána vůbec
3. Uživatelský účet osoby A – datová zpráva podepsána osobou B, která je zaměstnancem dodavatele, ale není doloženo žádné oprávnění – nabídka není podepsána vůbec

Nabízí se otázka, zda by si zadavatel měl či neměl vyžádat vysvětlení o oprávněnosti podpisu.[3] Podle mého názoru nikoliv, pokud datová zpráva byla podepsána v účtu jiné (třetí osoby), navíc vlastní nabídka není podepsána, a tudíž je otázkou, zda nedošlo ke zneužití informací v souvislosti s vyhotovením a podáním nabídky, a zároveň přihlašovacích údajů k uživatelskému účtu. Úvaha se může dokonce rozvíjet tak dalece, zda nenastaly trestněprávní důsledky takového jednání. Celou situaci bych zjednodušeně přirovnala k užívání přímého bankovnictví, tzn. zda by banka akceptovala v účtu osoby A (například manžel), aby podepisovala osoba B (například manželka) a činila tak (platné) bankovní operace, aniž by osoba A zřídila oprávněný přístup (další uživatelský účet) osobě B?

[3] Srov. Jednání dodavatele. [citováno 10. září 2011]. Dostupný z:http://www.compet.cz/fileadmin/user_upload/Sekce_VZ/Metodiky/jednani_dodavatele.pdf

Nová právní úprava

Podle přechodných ustanovení zákona (novely) č. 179/2010 Sb. elektronické nástroje atestované podle dosavadních předpisů byli zadavatelé oprávněni používat do 30. června 2011. Od 1. července 2011 se proto nevydává atest, ale vydává se certifikát shody.

Posuzování shody a vydávání certifikátu se řídí vyhláškou č. 9/2011 Sb., kterou se stanoví podrobnější podmínky týkající se elektronických nástrojů a úkonů učiněných elektronicky při zadávání veřejných zakázek a podrobnosti týkající se certifikátu shody (dále jen „vyhl.9/11" nebo „vyhláška"), která nabyla účinnosti dne 20. ledna 2011.[4]

Podle § 9 odst. 1 vyhl. 9/11 žádost o vydání certifikátu shody podává žadatel certifikačnímu orgánu. Žadatel prokazuje v žádosti a následném certifikačním auditu shodu elektronického nástroje s požadavky stanovenými právními předpisy **za prvé ve vztahu kfunkcionalitě elektronického nástroje a za druhé ve vztahu k prostředí, v němž je elektronický nástroj provozován**.

Co je to **funkcionalita** definuje vyhláška v § 2 písm. f) takto: souhrn funkčních vlastností, které elektronický nástroj má. **Prostředím** jsou podle § 2 písm. g) podmínky, za kterých je elektronický nástroj provozován.

Shodu elektronického nástroje prokáže žadatel, pokud elektronický nástroj splňuje požadavky stanovené v příloze této vyhlášky.[5]

Provozovatel x žadatel

Podle § 9 odst. 2 vyhl.9/11 pokud má elektronický nástroj platný certifikát shody ve vztahu k funkcionalitě a je provozován jinou osobou než žadatelem, kterému byl certifikát shody vydán, prokazuje tato jiná osoba jako žadatel certifikačnímu orgánu pouze splnění požadavků **ve vztahu k provoznímu prostředí, v němž je elektronický nástroj provozován**, ve smyslu přílohy vyhlášky.

Vyhláška pracuje se dvěma subjekty – provozovatel elektronického nástroje a žadatel. **Provozovatelem** elektronického nástroje je fyzická nebo právnická osoba, která konkretizuje provozníparametry a zajišťuje provoz elektronického nástroje, jehož prostřednictvím jsou nebo mají býtprováděny elektronické úkony za účelem zadávání veřejných zakázek nebo za účelem získání návrhuv soutěži o návrh a který splňuje požadavky stanovené zákonem a touto vyhláškou (§ 2 písm. h) vyhl. 9/11).

Žadatelem je provozovatel, který požádá o posouzení shody a udělení certifikátu shody (§ 2 písm. i) vyhl. 9/11).

Provozní prostředí

Z uvedeného pojetí certifikace na rozdíl od atestace, podle mého názoru, vyplývá, že některé opatření si musí zadavatel, pokud není provozovatelem ani žadatelem o certifikát elektronického nástroje, zavést individuálně, i když se jedná o technické požadavky (nepočítaje požadavky na řízení lidských zdrojů) a v případě potřeby prokázání shody by měl být schopen doložit jejich dodržování. Jedná se, podle mého názoru, především o tyto úkony:

- Řízení přístupu k aktivům v rámci zadávacích postupů (T3)
- Použití otevřených formát řízení (T4)
- Archivace dokumentace o veřejné zakázce (T5)
- Odeslání datové zprávy v rámci organizace zadavatele (T9)
- Příjem datové zprávy v rámci organizace zadavatele (T10)
- Jednání komise/ poroty/ zadavatele (T19)
- Elektronický podpis dokumentu (T20).

Řízení přístupu k aktivům v rámci zadávacích postupů (T3)

Zadavatel zajistí, aby řízení přístupu k aktivům v rámci zadávacích postupů bylo provedeno jednou z následujících variant:

1. *autentizace a autorizace přistupující osoby je založena na zadání jména a hesla. Poskytovatel dokumentu musízajistit, aby distribuce jména a hesla přistupujícím osobám proběhla přiměřeně bezpečným způsobem,*
2. *autentizace a autorizace přistupující osoby je založena na certifikátu veřejného klíče přistupující osoby nebo*
3. *autentizace a autorizace přistupující osoby je založena i na jiných technologiích; vždy však musí probíhat přiměřeně bezpečným způsobem.*

Vyhláška definuje aktiva jako jakoukoli součást elektronického nástroje a provozního prostředí včetně zdrojů, která je nezbytná k provozování elektronického nástroje v zamýšleném rozsahu (§ 2 písm. p) vyhl. 9/11).

[4] Vyhláška č. 172/2011 Sb.zrušila ke dni 29. června 2011 vyhlášku č. 326/2006 Sb., o podrobnostech atestačního řízení pro elektronické nástroje, náležitostech žádosti o atest a o výši poplatku za podání žádosti o atest (vyhláška o atestačním řízení pro elektronické nástroje).

[5] Podrobněji viz Metodické stanovisko [citováno 10. září 2011]. Dostupný z:http://www.portal-vz.cz/CMSPages/GetFile.aspx?guid=7bd44d87-b58b-4643-8f6a-b2199180427e

Zadavatel, který není provozovatel elektronického nástroje, by měl mít stanoveny interní postupy, například vnitřní předpis, pro zakládání uživatelských účtů, distribuci přístupových údajů uživatelům a záznamy o zrušení přístupů.

Použití otevřených formátů dokumentů (T4)

Zadavatel zajistí, aby formátem datových zpráv, které jsou vyměňovány během zadávacích postupů, byl otevřený formát.

Co se rozumí „otevřeným formátem" není z vyhlášky známo. Měly by se zřejmě používat tzv. opensource software jako je pdf, tiff anebo zip a zadavatel by si to měl stanovit ve vnitřním předpise.

Archivace dokumentace o veřejné zakázce (T5)

Zadavatel zajistí, aby dokumentace o veřejné zakázce, ke které je vyžadováno připojení zaručeného elektronického podpisu, byla uchovávána v datovém úložišti s řízeným přístupem. Řízení přístupu se musí řídit pravidly dle oddílu 2.3 (poznámka – řízení přístupu k aktivům v rámci zadávacích postupů (T3). Elektronický nástroj musí zajistit, aby při uložení dokumentace do datového úložiště bylo připojeno k dokumentaci kvalifikované časové razítko. Dokumentace o veřejné zakázce, která obsahuje důvěrné informace, musí být uchovávána v datovém úložišti s řízeným přístupem. Řízení přístupu se musí řídit pravidly dle oddílu 2.3 Dokumentace může být uchovávána ve své šifrované podobě. Pokud je dokumentace uchovávána v šifrované podobě, musí zadavatel bezpečně uchovávat soukromý klíč zadavatele, odpovídající veřejnému klíči zadavatele, kterým byl dokument šifrován. Doba uchování soukromého klíče zadavatele musí odpovídat době uchování dokumentace.

Zadavatel, který není provozovatel elektronického nástroje, by měl mít stanoveny interní postupy pro elektronickou archivaci dokumentů, například ve vnitřním předpise.

Odeslání datové zprávy v rámci organizace zadavatele (T9)

Formát datové zprávy odesílané v rámci organizace zadavatele bude zvolen podle potřeb zadavatele. Zadavatel vždy zvolí takový formát, který ochrání dokument proti neoprávněné změně. Elektronický protokol použitý k přenosu datové zprávy bude zvolen podle potřeb zadavatele. Zadavatel určí, zda datová zpráva bude šifrována a určí pravidla, jaký klíč bude používán k šifrování.

Příjem datové zprávy v rámci organizace zadavatele (T10)

Při příjmu datové zprávy, přenášené v rámci organizace zadavatele, musí zadavatel respektovat formát a elektronický protokol příchozí zprávy. V případě šifrované datové zprávy zadavatel stanoví pravidla určující, zda bude datová zpráva dešifrována. Pravidla pro to, zda bude pro datovou zprávu ověřena platnost tohoto elektronického podpisu, resp. značky, stanoví zadavatel. O příjmu datové zprávy musí být pořízen záznam o elektronickém úkonu (T2).[6]

Vyhláška definuje nešifrovanou a šifrovanou datovou zprávu. Podle § 2 písm. j) se jedná o **nešifrovanou datovou zprávu** o takovou, ve které nejsou přenášené údaje skryty například šifrováním a jsou přímo čitelné. **Šifrovanou datovou zprávou** se zpráva, ve které jsou přenášené údaje skryty pomocí šifrování a nejsou tak přímo čitelné (§ 2 písm. k) vyhl. 9/11).

Základní otázkou je, které zprávy (poznámka autorky – nemyslí se nyní formát, zda datová, šifrovaná apod.) u zadavatele je třeba zahrnout do certifikace. Opět by měl mít zadavatel, který není provozovatel elektronického nástroje, ve vnitřním předpise nastavenu komunikaci mezi svými zaměstnanci.

Jednání komise/poroty/zadavatele (T19)

Zadavatel zajistí, aby součástí záznamu o jednání komise/poroty/zadavatele byl dokument zápisu z jednání. Musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2 (poznámka – pořízení záznamu o elektronickém úkonu (T2).

Elektronickým úkonem se rozumí úkon jednající osoby v zadávacím řízení provedený prostřednictvím elektronického nástroje (§ 2 písm. d) vyhl. 9/11).

Není tedy možné, podle mého názoru, mimo elektronický nástroj a certifikační pravidla[7] řešit pouze elektronicky jednání buď komise anebo poroty či zadavatele, a to například e-mailem.Zadavatel by měl mít ve vnitřním předpise stanoveno jednání komise/poroty/zadavatele osobně, a tudíž zápis/protokol o jednání vzniká v listinné podobě a pouze se elektronicky archivuje. Podmínky archivace byly uvedeny výše.

[6] Pořízení záznamu o elektronickém úkonu (T2): zadavatel zajistí, aby veškeré záznamy o elektronických úkonech obsahovaly 1. jednoznačné určení daného konkrétního úkonu v rámci organizace zadavatele; 2. identifikaci osoby, která elektronický úkon provedla v případě, že jde o úkon učiněný konkrétní fyzickou osobou a nejedná se o úkon provedený automaticky elektronickým nástrojem (např. příjem nabídek); 3. informaci o nestandardním výsledku úkonu, pokud nastala při provedení úkonu chyba a 4. Zaznamenání času elektronického úkonu.

[7] Podle vyhlášky se certifikačními pravidly se rozumí souhrn podmínek a předpokladů stanovených certifikačním orgánem (§ 2 písm. n) vyhl. 9/11).

Elektronický podpis dokumentu (T20)

Zadavatel zajistí, aby elektronický podpis dokumentu byl proveden jedním z následujících způsobů:

1. *Formát dokumentu musí odpovídat požadavkům dle oddílu 2.4 (poznámka – použití otevřených formátů dokumentů T4). Dokument musí být podepsán připojením zaručeného elektronického podpisu nebo zaručené elektronické značky k dokumentu. Po připojení elektronického podpisu nebo elektronické značky zadavatele musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2 (poznámka – pořízení záznamu o elektronickém úkonu (T2) nebo*
2. *U vícestranného zaručeného elektronického podpisu bude dokument oboustranně podepsán postupnou výměnnou zpráv. V tomto případě zadavatel musí odeslat datovou zprávu s dokumentem s připojeným zaručeným elektronickým podpisem dodavateli způsobem dle oddílu 2.11 (poznámka – odeslání šifrované datové zprávy opatřené elektronickým podpisem T11). Dodavatel musí při příjmu datové zprávy respektovat formát dle příchozí zprávy. V případě, že byla datová zpráva šifrována, provede dodavatel její dešifrování. Dodavatel ověří platnost připojeného zaručeného elektronického podpisu. Dodavatel musí datovou zprávou odmítnout v případě, kdy zaručený elektronický podpis není platný nebo jeho kvalifikovaný certifikát byl zneplatněn. Dále dodavatel musí k dešifrování dokumentu připojit vlastní zaručený elektronický podpis a odeslat jej v datové zprávě v souladu s od-dílem 2.11. Zadavatel při příjmu této zprávy musí postupovat dle oddílu 2.14 (příjem šifrované datové zprávy opatřené elektronickým podpisem T14). Postup vícestranného elektronického podpisu lze realizovat v opačném pořadí, tj. dokument nejdříve podepíše dodavatel a následně ho předá zadavateli. Veškeré výše uvedené požadavky se použijí obdobně.*

Dlouhodobě řešená otázka v rámci elektronizace je, zda podepsat úkon či dokument,[8] se ve vyhlášce, dle mého názoru, začíná „rozšifrovávat." Vyhláška jednoznačně definuje podpis dokumentu a odlišuje tak tento úkon od podpisu úkonu, který je stanoven v § 149 odst. 4 ZVZ: *Zadavatel je oprávněn požadovat opatření datové zprávy elektronickým podpisem založeným na kvalifikovaném certifikátu či elektronickou značkou založenou na kvalifikovaném systémovém certifikátu u jakýchkoliv datových zpráv zasílaných elektronickými prostředky.*

[8] Podrobněji viz například Peterka, J., Podaný, J. Problematika elektronického podpisu v soudní praxi. Právní rozhledy, 2010, č. 19, s. 689 an.

Co se týká praxe, nastanou (a nastávají) problémy, že osoby oprávněné jednat nemají elektronické podpisy, a tudíž se omezuje, dle mého názoru, využívání elektronického zadávání veřejných zakázek anebo bude (a je) třeba začít využívat zástupců, kteří mají elektronický podpis.

Závěr

Shrneme-li úvahy z tohoto textu, je otázkou, zda nová právní úprava podpořila elektronizaci veřejného investování anebo naopak podpořila nedůvěru v používání elektronických nástrojů díky složitému procesu prokazování shody včetně požadavků na používání zaručených podpisů.

Zákon o veřejných zakázkách umožňuje používání „pouze" nástrojů (nikoliv tedy jen certifikovaných), které prokazatelně splňují požadavky stanovené zákonem o veřejných zakázkách a jeho prováděcími právními předpisy

Použití necertifikovaných elektronických nástrojů umožňuje § 149 odst. 2 ZVZ, podle kterého je možné užívat takové nástroje, které neporušují zákaz diskriminace, jsou s ohledem na předmět veřejné zakázky obecně dostupné a slučitelné s běžně užívanými informačními a komunikačními technologiemi.

S necertifikovanými nástroji se ovšem pojí mnohem více otázek než s certifikovanými, které byly nastoleny v tomto článku výše, protože v případě jakýchkoli pochybností, například při podání námitek v zadávacím řízení, musí být zadavatel schopen prokázat, že jím použitý elektronický nástroj prokazatelně splňuje požadavek na zákaz diskriminace a slučitelnost s běžně dostupnými informačními a komunikačními technologiemi Požadavky prokáže pravděpodobně formou znaleckého posudku, což považuji za velmi rizikové, protože v praxi se používají elektronické nástroje, které byly certifikovány jak na funkčnost, tak na prostředí a podle zákona o veřejných zakázkách splnění požadavků na elektronické nástroje lze **vždy** prokázat certifikátem shody (§ 149 odst. 9 ZVZ).

Summary

The aim of the article is to think about usage of electronic signatures in electronic tools for public procurement according the previous and contemporary legal regulation, particularly in connection with certification of electronic tools after the 1st July 2011. According to the Act No. 137/2006 Coll. electronic tools for public procurement are usingvalid advanced electronic signature based on a qualified certificatebut this article is not concerning explanation of electronic signature itself.