ELEKTRONICKÝ PODPIS PODLE NAŘÍZENÍ eIDAS[*]

VLADIMÍR SMEJKAL[**], JINDŘICH KODL[***], MIROSLAV UŘIČAŘ[****]

ABSTRAKT

Právní vymezení elektronického podpisu v ČR bylo doposud dáno Směrnicí Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy, na jeho základě vytvořeným zákonem č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů (dále také jen „EPZ“) a novým občanským zákoníkem, zákonem č. 89/2012 Sb. (dále také jen „NOZ“).

Dne 23. července 2014 bylo vydáno Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále také jen „Nařízení“), které je – s určitými výjimkami – účinné od 1. července 2016. Protože jde o přímo působící předpis, bude jeho důsledkem s největší pravděpodobností zrušení, nebo značná redukce zákona o elektronickém podpisu, jakož i další změny v české legislativě.

Článek se zabývá jak právními, tak věcnými důsledky tohoto nového Nařízení v oblasti elektronického podpisu a hodnotí nové definice v Nařízení použité v kontextu s dosavadní právní úpravou.

[*] Příspěvek je výstupem projektu specifického výzkumu „Efektivní využití ICT a kvantitativních metod pro optimalizaci podnikových procesů“ Interní grantové agentury Vysokého učení technického v Brně s registračním číslem FP-S-15-2787.

[**] Prof. Ing. Vladimír Smejkal, CSc. LL.M. působí na Fakultě podnikatelské Vysokého učení technického v Brně a na Unicorn College v Praze. Zabývá se mj. problematikou informatické kriminality a právních aspektů informačních systémů a jejich bezpečností. V letech 2004 - 2014 byl členem Legislativní rady vlády ČR. Je soudním znalcem v oborech kybernetika, kriminalistika, ekonomika a autorská díla.

Kontaktní e-mail: smejkal@znalci.cz.

[***] Ing. Jindřich Kodl, CSc. je konzultantem a soudním znalcem v oblasti bezpečnosti informačních systémů a kryptologie. Je členem ISACA.

[****] Mgr. Miroslav Uřičař je ředitelem úseku práva, regulace, vnějších vztahů a bezpečnosti společnosti T-Mobile Czech Republic a.s. a předsedou legislativní komise České asociace pro soutěžní právo. Je dále členem představenstva Asociace provozovatelů mobilních sítí, členem výkonné rady UNICEF ČR a působí jako rozhodce Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky.

KLÍČOVÁ SLOVA

elektronická identifikace; elektronický podpis; elektronická značka; elektronická pečeť; elektronické časové razítko; dynamický biometrický podpis; elektronické právní jednání; služby vytvářející důvěru

ABSTRACT

The legal definition of electronic signature in the Czech Republic, has so far been given by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, was established on its basis by Act no. 227/2000 Coll., on electronic signatures, as amended and the new Law no. 89/2012 Coll., Civil Code.

The Regulation No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC that was issued on July 23, 2014 is – with certain exceptions – effective from 1 July 2016. Since this is a direct-acting prescription, it will be most likely the cause of the abolition or substantial reduction of the Act on Electronic Signatures as well as other changes in the Czech legislation.

The article deals with both legal and factual consequences of this new regulation in the field of electronic signature and evaluates new definitions of the Regulation used in the context of existing legislation.

KEYWORDS

electronic identification; electronic signature; electronic mark; electronic seal; electronic time stamp; dynamic biometric signature; electronic legal transactions; trust services

SEZNAM POUŽITÝCH ZKRATEK

ArchZ	zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů
ČR	časové razítko
DBP	dynamický biometrický podpis
DS	datová schránka podle zákona č. 300/2008 Sb., o elektronic-

	kých úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
ElÚkZ	zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
EP	elektronický podpis
EPZ	zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů
EZ	elektronická značka
ISDS	informační systém datových schránek podle § 14 zákona č. 300/2008 Sb. ve znění pozdějších předpisů
KvCt	kvalifikovaný certifikát
KvEP	kvalifikovaný elektronický podpis
NOZ	nový občanský zákoník, zákon č. 89/2012 Sb.
ObčZ	zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.
ZEP	zaručený elektronický podpis

1. ÚVOD – CÍLE A OBLAST PŮSOBNOSTI NAŘÍZENÍ

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 ve znění opravy ze dne 28. srpna 2014[1], známějšímu pod zkratkou „Nařízení eIDAS“ (což znamená *electronic identification and services*), se zaměřuje na více aspektů budování důvěryhodnosti v on-line prostředí. Hlavním mottem nařízení je zajištění interoperability na bázi kvalifikovaných služeb vytvářejících důvěru vykazujících srovnatelnou úroveň bezpečnosti a odpovědnosti v rámci EU.[2]

Podle čl. 1 je cílem nařízení zajistit řádné fungování vnitřního trhu a současně usilovat o odpovídající úroveň bezpečnosti prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru. Toto nařízení:

[1] Official Journal of the European Union, L 257, 28. 8. 2014, s. 73 – 114 a L 327, 12. 11. 2014, s. 9

[2] Viz body 4., 6., 7., 19., 20., 54., 77. Preambule Nařízení eIDAS

a) stanoví podmínky, za nichž členské státy uznávají prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému elektronické identifikace jiného členského státu;
b) stanoví pravidla pro služby vytvářející důvěru, zejména u elektronických transakcí; a
c) stanoví právní rámec pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek.

Cílem v oblasti elektronické identifikace je interoperabilita. V oblasti služeb vytvářejících důvěru je cílem harmonizace. V preambuli se uvádí obvyklé EU proklamace o hospodářském a sociálním rozvoji, k čemuž údajně přispěje jednotný digitální trh usnadněním přeshraničního využívání on-line služeb. To je poněkud vzdálenější cíl, nicméně bezprostředním smyslem Nařízení je sjednocení elektronické identifikace a její vzájemné uznávání v ostatních členských státech. Jeho cílem je zajistit, aby u přístupu k přeshraničním on-line službám poskytovaným členskými státy byla možná bezpečná elektronická identifikace a autentizace. Zásada vzájemného uznávání pro účely on-line služeb by se měla použít, jestliže systém elektronické identifikace oznamujícího členského státu splňuje podmínky pro oznámení a toto oznámení bylo zveřejněno v Úředním věstníku Evropské unie. Přitom úrovně záruky by měly vyjadřovat míru spolehlivosti prostředků pro elektronickou identifikaci při určování totožnosti osob, a tím poskytovat záruku, že osoba deklarující konkrétní totožnost je skutečně osobou, s níž je tato totožnost spojena. Podstatné je, že „*Stanovené požadavky by měly být z technologického hlediska neutrální. Měla by tedy existovat možnost splnit nezbytné bezpečnostní požadavky různými technologiemi.*[3]“

Jde o dokument, který odstraňuje řadu nepřesností vyplývajících v oblasti elektronického podpisu ze Směrnice 1999/93/ES a jejích národních implementací, které nebyly vždy konzistentní, a to ani vůči Směrnici, ani mezi sebou.[4] Nařízení se snaží integrovat vše, co nějakým způsobem souvisí s elektronickou identifikací a autentizací. Za tímto

[3] Bod 16 Preambule Nařízení eIDAS

účelem vystavělo poměrně složitou strukturu nástrojů o různých úrovních co do požadavků na ně kladených. Ne vždy zcela nutných, ne vždy zcela šťastných a – přinejmenším v jednom případě – vysloveně nevhodných, nebo přinejmenším zavádějících (viz čl. 25 odst. 2, k tomu pak dále).

Najdeme zde poněkud nešťastné rozlišování na „kvalifikované a nekvalifikované poskytovatele služeb vytvářejících důvěru"; nelze se přitom domnívat, že by uživatelé byli ochotni přehnaně využívat poskytovatele, jež budou označováni jako „nekvalifikovaní" a je otázkou, zda jde pouze o nešťastně zvolené označení, nebo o úmysl odradit jejich potenciální zákazníky. Přesto se jejich existence připouští s vymezením, že „*Nekvalifikovaní poskytovatelé služeb vytvářejících důvěru by měli podléhat nezatěžujícím a pružným činnostem následného dohledu, odůvodněným povahou jejich služeb a činností. Orgán dohledu by proto neměl mít obecnou povinnost vykonávat nad nekvalifikovanými poskytovateli služeb dohled.*[5]"

Nařízení ponechává námi trvale kritizované možnosti používání pseudonymů v certifikátech,[6] když poněkud licoměrně říká, že „*ustanovení o používání pseudonymů v certifikátech by neměla členským státům bránit v tom, aby vyžadovaly identifikaci osob podle práva Unie nebo podle vnitrostátního práva.* [7]" Autorům není příliš jasné, jak používání pseudonymů může pomoci žádoucímu vylepšení nástrojů pro elektronickou identifikaci a autentizaci. A contrario: proč si pořizovat pseudonymní, tedy v podstatě anonymní certifikát pro komunikaci, kde se chci nějakým způsobem podepsat. Autoři jsou si samozřejmě vědomi dikce ust. § 79 NOZ o pseudonymu a zde tedy také hledají odůvodnění smyslu tohoto institutu v EPZ a nyní i v Nařízení.

Nařízení zavádí režim odpovědnosti, podle kterého by všichni poskytovatelé služeb vytvářejících důvěru měli odpovídat za škodu, kterou fyzické nebo právnické osobě způsobí v důsledku nesplnění povinností podle tohoto nařízení.

---

[4] DUMORTIER, Jos a kol. *Study on legal and market aspects of the application of Directive 1999/93/EC laying down a Community framework for electronic signatures and on the practical applications of the electronic signature.* Catholic Univestity of Leuven, Belgie, zpracováno pro European Commission, Directorate General Information Society, Brusel 2003.

[5] Bod 36 Preambule Nařízení eIDAS

[6] Např. MATES, Pavel; SMEJKAL, Vladimír. *E-government v České republice. Právní a technologické aspekty.* 2. vydání. Praha: Leges, 2012.

[7] Bod 33 Preambule Nařízení eIDAS

Jak budou realizovány některé návrhy, těžko říci. To se týká např. bodu 42., podle kterého v případě, že poskytovatel poskytuje své služby na území jiného členského státu a nepodléhá v něm dohledu, nebo pokud se počítače poskytovatele nacházejí na území jiného členského státu, než ve kterém je usazen, by měl být zřízen systém vzájemné pomoci mezi orgány dohledu v členských státech.

Abychom uklidnili společnosti, které dnes zahájily poměrně razantní přechod na dynamický biometrický podpis (dále také jen „DBP“)[8], je třeba hned v úvodu zdůraznit, že podle čl. 2 se Nařízení nevztahuje na poskytování služeb vytvářejících důvěru, které jsou používány výhradně v rámci uzavřených systémů vyplývajících z vnitrostátního práva nebo z dohod mezi určeným okruhem účastníků. Nařízení se vztahuje na systémy elektronické identifikace oznámené členskými státy a na poskytovatele služeb vytvářejících důvěru – viz níže – usazené v Unii. Nařízení nemá vliv na vnitrostátní právo ani právo Unie týkající se uzavírání a platnosti smluv či jiných právních nebo procesních povinností týkajících se formy.

Nařízení (regulation) je součástí tzv. sekundárního práva EU a svou povahou je obdobné zákonu, protože je bezprostředně závazné ve všech členských státech, nevyžaduje žádné implementace v národní legislativě a členské státy jsou povinny podle něj postupovat, jako by se jednalo o jejich vlastní právní předpis. Je závazné v celém rozsahu a přímo použitelné ve všech členských státech. Vyplývají z něj práva a povinnosti pro stát i jednotlivé osoby. Není tedy třeba provést transpozici do národního práva, jako tomu bylo v případě směrnice 1999/93/ES, která se stala zdrojem práva pro zákon o elektronickém podpisu č. 227/2000 Sb. Pokud nařízení stanoví něco jiného než národní právní předpis, musí mu dát členský stát přednost.

Obecné právní instituty týkající se právního jednání, uzavírání smluv na dálku apod. (u nás nyní soustředěné do nového občanského zákoníku) nebo postupy popsané v procesních předpisech (občanský soudní řád, trestní řád, daňový řád, zákon o elektronických právních úkonech a konverzi dokumentů) by tímto neměly být dotčeny; pokud se to nedá vyloučit, uvádíme to níže.

[8] Viz např. BERNÁŠEK, Aleš. Vlastnoruční digitální podpis a jeho implementace v O2 – část I. a II. *Data Security Management*, 2014, č. 3, s. 39 -39 a č. 4, s. 22 – 27.

Z výše uvedeného mj. vyplývá, že pokud budeme chtít realizovat něco jinak, nežli je popsáno v Nařízení, musíme si tedy vybudovat uzavřený systém, který u nadnárodních subjektů může být rovněž přeshraniční. A opačně – pro systémy otevřené, které předem neomezují nikoho v přístupu ke službám prostřednictvím sítí elektronických komunikací, platí Nařízení přímo a v plném rozsahu.

2. CÍLE NAŘÍZENÍ

Cíle Nařízení v sobě koncentrují zásady obsažené v citované Směrnici, ale i v dalších právních aktech EU[9]. Jsou to především:

- zvýšení důvěryhodnosti elektronických transakcí na vnitřním trhu [rozuměj EU] (bod 2. Preambule),
- odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci (bod 12. Preambule),
- zavedení a oznámení prostředků pro účely elektronické identifikace pro přístup k on-line službám včetně povinnosti je uznávat v členských státech (body 13. a 15. Preambule),
- stanovení obecného právního rámce pro využívání služeb vytvářejících důvěru včetně možnosti je použít jako důkaz v soudním a správním řízení (body 21. a 22. Preambule),
- stanovení odpovědnosti pro všechny poskytovatele služeb vytvářejících důvěru (bod 37. Preambule),
- zajištění soudržného rámce, který by v souvislosti se službami vytvářejícími důvěru zabezpečil vysokou úroveň bezpečnosti a právní jistotu (bod 44. Preambule),
- stanovení požadavků na kvalifikované prostředky pro vytváření elektronických podpisů, které mají zajistit funkčnost zaručených elektronických podpisů (bod 56. Preambule),
- zajištění dlouhodobého uchovávání informací, aby zajistilo dlouhodobou platnost elektronických podpisů a elektronických pečetí a zaručilo, že mohou být ověřeny bez ohledu na budoucí technologické změny (bod 61. Preambule),

[9] Např. Rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle Směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu. OJ L 274, 20. 10. 2009, s. 36 – 37.

- stanovení právního rámce, který usnadní přeshraniční uznávání služeb elektronického doporučeného doručování mezi stávajícími vnitrostátními právními systémy (bod 66. Preambule),
- stanovení povinnosti v oblasti bezpečnosti a odpovědnosti pro služby autentizace internetových stránek (bod 67. Preambule),
- zrušení směrnice 1999/93/ES, a to z důvodu právní jistoty a jasnosti (bod 73. Preambule).

Co se týká elektronických podpisů, uvádí se zde, že „*nařízení by mělo zavést zásadu, že elektronickému podpisu by neměly být upírány právní účinky na základě skutečnosti, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikovaný elektronický podpis. Ačkoliv k zajištění vzájemného uznávání elektronických podpisů je zapotřebí vysoká úroveň bezpečnosti, měly by být ve zvláštních případech, například v kontextu rozhodnutí Komise 2009/767/ES 10, přijímány rovněž elektronické podpisy s nižší zárukou bezpečnosti. Právní účinky elektronických podpisů v členských státech by však měly být vymezeny vnitrostátním právem, s výjimkou požadavků stanovených v tomto nařízení, podle něhož by měl mít kvalifikovaný elektronický podpis rovnocenný právní účinek jako podpis vlastnoruční*“.[10]

Nařízení se zabývá i formáty elektronických podpisů a razítek – nově označovaných jako „pečetě“. Podle bodu 50. Preambule „*Jelikož v současnosti používají příslušné orgány v členských státech při podepisování svých dokumentů elektronickými prostředky různé formáty zaručených elektronických podpisů, je cílem Nařízení zajistit, aby členské státy mohly při přijímání dokumentů, které byly podepsány elektronickými prostředky, technicky podporovat alespoň určitý počet formátů zaručených elektronických podpisů. Pokud příslušné orgány v členských státech používají zaručené elektronické pečetě, bude obdobně nutné zajistit, aby podporovaly přinejmenším určitý počet formátů zaručených elektronických pečetí*“. K tomu se vztahuje také svěření pravomoci Komisi upravit formáty zaručených elektronických podpisů a pečetí podle bodu 64. Preambule – viz dále.

Objevuje se zde nový institut „dočasného pozastavení platnosti kvalifikovaných certifikátů“. Podle názoru autorů toto spíše vnese větší zmatek do ověřování platnosti právních jednání či jiných transakcí, protože na rozdíl od současného binárního stavu „platný – neplatný, resp.

[10] Body 48 a 49 Preambule Nařízení eIDAS

zneplatněný“ certifikát, bude nutno zkoumat, zda byl úkon učiněn v době, kdy byl či nebyl certifikát pozastaven. Smysl této novinky je poněkud nejasný a přínos sporný, přičemž bude mít velký dopad na procesy spojené s revokací certifikátů.

Předpokládá se certifikace bezpečnosti IT systémů založená na mezinárodních normách, přičemž výslovně je uvedena ISO 15408. Jedná se o poměrně známá „Common Criteria“, která vznikla na základě již dříve používaných norem, především amerických TCSEC, evropských ITSEC a kanadských CTCPEC. Mezinárodní norma ISO/IEC 15408:1999 má status české technické normy. Česká verze nese označení ČSN ISO/IEC 15408. Jednotlivé díly jsou ve shodě s originálem normy označeny jako 15408-1, 15408-2 a 15408-3.[11] Pravděpodobně by to mohly být i normy řady ISO/IEC 27000, resp. ČSN ISO/IEC 27000.

Nařízení – na rozdíl od Směrnice z roku 1999 – kodifikuje také to, co známe z českého zákona o elektronickém podpisu: elektronické značky a časová razítka. Zavádí elektronickou pečeť a elektronické časové razítko.

Kromě toho článek 46 Nařízení proklamuje něco, co je např. u nás tvrzeno různým způsobem již přes 15 let, tj. že „*Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu.*“ Autoři si nemyslí, že je toto dnes třeba uvádět, protože za posledních dvacet let diskuse, zpočátku značně bouřlivá, o uznávání tzv. elektronických důkazů v podstatě utichla a všeobecně se nepochybuje o možnosti použít k dokazování i elektronické stopy.[12] V našich podmínkách pak lze poukázat na dikci § 3026 odst. 1 NOZ „*Nevylučuje-li to povaha písemnosti, platí ustanovení tohoto zákona o listině obdobně i pro jinou písemnost bez zřetele na její podobu.*“, přičemž jak podle autorů, tak podle důvodové zprávy k NOZ se touto jinou písemností myslí písemnost elektronická. Na druhou stranu proklamace článku 46 Nařízení ničemu nezaškodí; její smysl může spočívat ve snaze unifikovat právní úpravy napříč členskými státy, protože ty nedosahují stejného standardu.

[11] SMEJKAL, Vladimír; RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, str. 303 an.

[12] Ke stopám viz např. SMEJKAL, Vladimír. Metodika vyšetřování kybernetické kriminality. In: PORADA, Viktor; STRAUS, Jiří et al. *Kriminalistika (výzkum, pokroky, perspektivy)*. Plzeň: Ales Čeněk, 2013 nebo PORADA, Viktor; STRAUS, Jiří. *Kriminalistické stopy - Teorie, metodologie, praxe.* Aleš Čeněk, s.r.o., Plzeň, 2012.

Autoři Nařízení si patrně uvědomili neustálý vývoj technologií, ale i kybernetické kriminality[13]. Reakcí na tento vývoj jsou ustanovení, podle kterých by měla být Komisi svěřena pravomoc *„přijímat akty v souladu s článkem 290 Smlouvy o fungování EU, pokud jde o kritéria, která musí splňovat subjekty odpovědné za certifikaci kvalifikovaných prostředků pro vytváření elektronických podpisů*[14]“. Účelem svěření této pravomoci totiž má být pružné a rychlé doplnění určitých podrobných technických aspektů tohoto nařízení. Komisi by měly být svěřeny prováděcí pravomoci, zejména k určení referenčních čísel norem, jejichž použití zakládá předpoklad shody s určitými požadavky stanovenými v tomto nařízení, přičemž se předpokládá spolupráce zejména s Evropským výborem pro normalizaci (CEN), Evropským ústavem pro telekomunikační normy (ETSI), Mezinárodní organizací pro normalizaci (ISO) a Mezinárodní telekomunikační unií (ITU).

Poslední téma Nařízení, které je nicméně již mimo záběr tohoto článku, jsou služby autentizace internetových stránek, proto se jím detailně nezabýváme.

A konečně, jak již vyplývá z názvu Nařízení, ruší se jím směrnice 1999/93/ES. Tento krok je nezbytný, neboť cíle Nařízení jsou podstatně širší a řada definic, které do právního řádu EU citovaná směrnice zavedla, je zde přeformulována. Jedná se tedy o standardní legislativní postup.

3. DEFINICE V OBLASTI ELEKTRONICKÉHO PODPISU DŘÍVE A NYNÍ

V rámci nově formulovaných definic v Nařízení dochází k celé řadě změn, mnohé z nich mají pouze formální či upřesňující charakter, je však i nemálo těch, které jsou zásadní. Pro snadnější orientaci čtenáře jsme vytvořili tabulku zásadních pojmů, v níž jsme zahrnuli porovnání těchto pojmů dle právního řádu ČR, zejména podle zákona o elektronickém podpisu, a dle Nařízení, přičemž ty změny, které jsou dle našeho názoru zásadní, jsme označili **tučně.** Podtržením jsou pak označena místa, která nejsou podle názoru autorů ani v novém Nařízení dostatečně definována či snadno vyložitelná a která diskutujeme dále.

[13] Podrobně viz SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015.
[14] Bod 70 Preambule Nařízení eIDAS

TABULKA 1. POROVNÁNÍ ZÁKLADNÍCH POJMŮ

Pojem	**Podle zákona o elektronickém podpisu nebo jiného právního předpisu v české legislativě**	**Podle Nařízení**
podepisující osoba	fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby	fyzická osoba, která vytváří elektronický podpis
elektronický podpis	údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a **které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě**	data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a **která podepisující osoba používá k podepsání**
zaručený elektronický podpis	elektronický podpis, který splňuje následující požadavky 1. je jednoznačně spojen s podepisující osobou, 2. umožňuje identifikaci podepisující osoby **ve vztahu k datové zprávě,** 3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou, 4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat	elektronický podpis, který splňuje požadavky stanovené v článku 26: 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 změ-

		nu dat
kvalifikovaný elektronický podpis	**není výslovně definován**, nicméně je opisován frází „*použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu*“ – viz § 3 EPZ	zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy
data pro vytváření elektronických podpisů	jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu	jedinečná data, která podepisující osoba používá k vytváření elektronických podpisů
certifikát pro elektronický podpis	datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a **umožňuje ověřit její identitu**, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,	elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a **potvrzuje alespoň jméno nebo pseudonym této osoby**
kvalifikovaný certifikát pro elektronický podpis	certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb Podle § 12: (1) Kvalifikovaný certifikát musí obsahovat a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona, b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je	certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze I: Kvalifikované certifikáty pro elektronické podpisy obsahují a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako

	kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen, c) jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym, d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu, e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby, f) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává, g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb, h) počátek a konec platnosti kvalifikovaného certifikátu, i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,	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 kvalifi-

	j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít. (2) Omezení pro použití kvalifikovaného certifikátu podle odstavce 1 písm. i) a j) musí být zjevná třetím stranám. (3) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.	kovaného 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.**
služba vytvářející důvěru	- - -	elektronická služba, která je zpravidla poskytována za úplatu a spočívá: a) ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo

		b) ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo c) v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami
kvalifikovaná služba vytvářející důvěru	- - -	služba vytvářející důvěru, která splňuje použitelné požadavky stanovené v tomto nařízení
poskytovatel služeb vytvářejících důvěru	poskytovatelem certifikačních služeb se rozumí fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy	fyzická nebo právnická osoba, která poskytuje jednu či více služeb vytvářejících důvěru buď jako kvalifikovaný, nebo jako nekvalifikovaný poskytovatel služeb vytvářejících důvěru
kvalifikovaný poskytovatel služeb vytvářejících důvěru	kvalifikovaným poskytovatelem certifikačních služeb se rozumí poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů a **splnil ohlašovací povinnost podle § 6**	poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému **orgán dohledu udělil status kvalifikovaného poskytovatele**
produkt	nástrojem elektronického podpisu se rozumí technické zařízení nebo programové vybavení, nebo jejich součásti, používané poskytovatelem certifikačních slu-	technické zařízení nebo programové vybavení či jejich příslušné součásti, které jsou určeny k používání pro poskytování služeb vytvářejících důvěru

	žeb pro vytváření nebo ověřování elektronických podpisů nebo pro zajištění certifikačních služeb,	
prostředek pro vytváření elektronických podpisů	technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů	konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů
kvalifikovaný prostředek pro vytváření elektronických podpisů	- - -	prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II: 1. Kvalifikované prostředky pro vytváření elektronických podpisů vhodnými technickými prostředky a postupy přinejmenším zajistí, aby: a) byla přiměřeně zajištěna důvěrnost dat pro vytváření elektronických podpisů, která byla použita při vytváření elektronického podpisu; b) data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu se mohla prakticky vyskytnout pouze jednou; c) bylo přiměřeně zajištěno, že data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu nelze odvodit a že elektronický podpis je v současnosti dostupnými

		technickými prostředky spolehlivě chráněn proti padělání; d) oprávněná podepisující osoba měla možnost data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu spolehlivě chránit před jejich zneužitím třetí osobou. 2. Kvalifikované prostředky pro vytváření elektronických podpisů nesmějí měnit podepisovaná data ani bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním. 3. Data pro vytváření elektronických podpisů může jménem podepisující osoby vytvářet nebo spravovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru. 4. Aniž je dotčen bod 1 písm. d), smějí kvalifikovaní poskytovatelé služeb vytvářejících důvěru, kteří spravují data pro vytváření elektronických podpisů jménem podepisující osoby, kopírovat data pro vytváření elektronických podpisů pouze pro účely zálohování a jsou-li splněny tyto požadavky:

		a) bezpečnost zkopírovaných souborů dat je na stejné úrovni jako u původních souborů dat; b) počet zkopírovaných souborů dat nepřesáhne minimum potřebné pro zajištění kontinuity služby.
pečetící osoba	označující osobou se rozumí **fyzická osoba, právnická osoba nebo organizační složka státu,** která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou	**právnická osoba**, která vytváří elektronickou pečeť
elektronická pečeť	elektronickou značkou se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky 1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, 2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, 3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat	data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu

zaručená elektronická pečeť	- - -	elektronická pečeť, která splňuje požadavky stanovené v článku 36: a) je jednoznačně spojena s pečetící osobou; b) umožňuje identifikaci pečetící osoby; c) je vytvořena pomocí dat pro vytváření elektronických pečetí, která může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou; a d) je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat
kvalifikovaná elektronická pečeť	- - -	zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť
data pro vytváření elektronických pečetí	daty pro vytváření elektronických značek se rozumí jedinečná data, která označující osoba používá k vytváření elektronických značek	jedinečná data, která pečetící osoba používá k vytváření elektronických pečetí
certifikát pro elektronickou pečeť	datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování	elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických pečetí

	elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,	s určitou právnickou osobou a potvrzuje název této osoby
kvalifikovaný certifikát pro elektronickou pečeť	kvalifikovaným systémovým certifikátem se rozumí certifikát, který má náležitosti podle § 12a a byl vydán kvalifikovaným poskytovatelem certifikačních služeb Podle § 12a: Kvalifikovaný systémový certifikát musí obsahovat a) označení, že je vydán jako kvalifikovaný systémový certifikát podle tohoto zákona, b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen, c) jednoznačnou identifikaci označující osoby, případně prostředku pro vytváření elektronických značek, d) data pro ověřování elektronických značek, která	certifikát pro elektronickou pečeť, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v příloze III: Kvalifikované certifikáty pro elektronické pečetě obsahují: a) označení, alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronickou pečeť; 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;

	odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby, e) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný systémový certifikát vydává, f) číslo kvalifikovaného systémového certifikátu unikátní u daného kvalifikovaného poskytovatele certifikačních služeb, g) počátek a konec platnosti kvalifikovaného systémového certifikátu, h) omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám.	c) alespoň jméno pečetící osoby a případné registrační číslo uvedené v úředních záznamech; d) data pro ověřování platnosti elektronických pečetí, která odpovídají datům pro vytváření elektronických pečetí; 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 pečetí spojená s daty pro

		ověřování platnosti elektronických pečetí obsažena v kvalifikovaném prostředku pro vytváření elektronických pečetí, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.
prostředek pro vytváření elektronických pečetí	prostředkem pro vytváření elektronických značek se rozumí zařízení, které používá označující osoba pro vytváření elektronických značek a které splňuje další náležitosti stanovené tímto zákonem,	konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických pečetí
kvalifikovaný prostředek pro vytváření elektronických pečetí	- - -	prostředek pro vytváření elektronických pečetí, který přiměřeně splňuje požadavky stanovené v příloze II
elektronické časové razítko	- - -	data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a **prokazují, že tato jiná data existovala v daném okamžiku**
kvalifikované elektronické časové razítko	kvalifikovaným časovým razítkem se rozumí datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a **zaručuje, že uvedená data v elektronické**	elektronické časové razítko, které splňuje požadavky stanovené v článku 42: a) spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat; b) je založeno na zdroji přesného času, který je

	podobě existovala před daným časovým okamžikem	spojen s koordinovaným světovým časem; a c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou
elektronický dokument	- datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na technických nosičích dat, používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložená na technických nosičích ve formě datového souboru (podle EPZ) - dokumentem každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena (ArchZ)	jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka
služba elektronického doporučeného doručování	upraveno zákonem o elektronických úkonech a autorizované konverzi dokumentů[15]	služba, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání

[15] Podrobný rozbor viz SMEJKAL, Vladimír. *Datové schránky v právním řádu ČR. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, s komentářem*. 1. vydání. Praha: ABF, a.s., 2009 nebo MATES, Pavel; SMEJKAL, Vladimír. *E-government v České republice. Právní a technologické aspekty*. 2. podstatně přepracované a rozšířené vydání. Praha: Leges 2012, s. 162 an.

		s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn
kvalifikovaná služba elektronického doporučeného doručování	upraveno zákonem o elektronických úkonech a autorizované konverzi dokumentů	služba elektronického doporučeného doručování, která splňuje požadavky stanovené v článku 44: a) jsou poskytovány jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru; b) s vysokou úrovní spolehlivosti zajišťují identifikaci odesílatele; c) zajišťují identifikaci příjemce před doručením dat; d) odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat; e) odesílatel a příjemce dat jsou jednoznačně vyrozuměni o případných změnách dat potřebných za účelem odeslání nebo přijetí dat; f) datum a čas odeslání, přijetí a případná změna dat jsou označeny prostřednictvím kvalifikovaného e-

		lektronického časového razítka.
data pro ověřování platnosti	daty pro ověřování elektronických podpisů se rozumí jedinečná data, která se používají pro ověření elektronického podpisu, daty pro ověřování elektronických značek se rozumí jedinečná data, která se používají pro ověření elektronických značek,	data, která se používají k ověření platnosti elektronického podpisu nebo elektronické pečeti
ověřování platnosti	- - -	postup ověřující shodu a potvrzující platnost elektronického podpisu nebo elektronické pečeti

4. ELEKTRONICKÁ ČASOVÁ RAZÍTKA

Elektronická časová razítka (dále jen „ČR“) máme v české legislativě od roku 2004, byť pouze jako kvalifikovaná, což autoři dlouhodobě nepovažují za metodicky správné a ostatně ani za logicky odůvodněné (začínat definici hned „vyšším stupněm“ bez definování základního, jak tomu je u elektronického podpisu, je přinejmenším zvláštní). Nařízení obsahuje obě definiční úrovně (bod 33. a 34. čl. 3) a podle čl. 41 Nařízení podobně jako u elektronického podpisu a pečeti zdůrazňuje, že ani „*elektronickému časovému razítku nesmějí být upírány právní účinky a nesmí být odmítáno jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické časové razítko*“.

U kvalifikovaného elektronického časového razítka platí domněnka správnosti data a času, které udává, a integrity dat, s nimiž jsou toto datum a tento čas spojeny. Definiční čl. 3 Nařízení to říká výslovně (a správněji nežli stávající EPZ): „*elektronickým časovým razítkem jsou data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku*“. Došlo tedy k odstranění nevhodné definice časového razítka podle stávajícího zákona,

na kterou bylo v minulosti opakovaně upozorňováno. Pokud se totiž v definici KvČR dle ust. § 2 písm. r) EPZ praví, že „*kvalifikovaným časovým razítkem datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem*“, pak existuje jistá past doslovného výkladu této definice, která vychází ze zahraničního dokumentu, tvořeného technology.[16] Lze totiž diskutovat o tom, jak dlouho data existovala před daným časovým okamžikem – hodinu, týden, rok, desetiletí? Podle názoru autorů cit. práce, by bylo přesnější použít definici jinou, právnicky přesnější, tj. typu „data existovala v okamžiku doručení vzorku (hash) dokumentu k poskytovateli“.[17] Definice v Nařízení tento problém odstraňuje při zachování vysoké míry obecnosti a technologické nezávislosti.

Kvalifikované elektronické časové razítko vydané v jednom členském státě se uznává jako kvalifikované elektronické časové razítko ve všech členských státech. Především, ale nejen pro tento účel jsou v čl. 42 definovány požadavky na kvalifikovaná elektronická časová razítka:

a) spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat;

b) je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem[18]; a c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru (viz Kapitola III Nařízení) nebo označeno jinou rovnocennou metodou.

5. ELEKTRONICKÉ PEČETI

Směrnice 1999/93/ES neznala elektronické značky, na rozdíl od českého EPZ, kam byly zavedeny novelou EPZ zákonem č. 440/2004 Sb. společně s časovými razítky. V Nařízení se značky objevily, neboť všeobecná

[16] Viz Např. RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), Part. 1. Introduction: A time-stamping service supports assertions of proof that a datum existed before a particular time. Similarly ETSI TS 102 023 V1.2.1 (2003-01), part 3.1.

[17] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 152.

[18] Koordinovaný světový čas (Coordinated Universal Time), pro který je používána zkratka UTC, je celosvětový časový standard vycházející z tzv. mezinárodního atomového času, jehož časová pásma jsou definována svými odchylkami od UTC.

užitečnost takového nástroje je známa, a to jako „elektronické pečeti". Anglický termín „seal" mohl být ovšem přeložen také jako „razítko", neboť o to v Nařízení právě jde. V definici v čl. 3 bod 24. najdeme, že „*pečetící osobou je právnická osoba, která vytváří elektronickou pečeť*", a dále v bodu 29., že „*certifikátem pro elektronickou pečeť je elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických pečetí s určitou právnickou osobou a potvrzuje název této osoby*" – pro laiky lze připodobnit ke klasickému razítku.

Čl. 35 až 39 říkají pro pečeti totéž, co čl. 25 až 29 pro elektronické podpisy. Je otázkou legislativní techniky, zda nešlo konstatovat – vzhledem k totální shodě textů – pouze to, že ustanovení o podpisech se pro pečetě použijí obdobně. Je zajímavé, že v čl. 39 a 40 toto bylo možno použít s odkazem na čl. 29 až 34.

Podle bodu 29. jsou tedy vyloučeny osoby fyzické. Nevíme proč, lze se domnívat, že zřejmě proto, že ty mohou používat svůj elektronický podpis, což je ovšem něco zcela odlišného. V případě podpisu podle Nařízení jde o data, která podepisující osoba používá k podepsání (viz čl. 3 bod 10), neboli jedná se nepochybně o projev vůle (podle NOZ právní jednání). U pečeti jde o data, „*která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu*" (čl. 3 bod 25). Elektronická pečeť je tedy jakýmsi průkazem kvality, příp. původu dat a autorům není jasné, proč jsou o tuto možnost fyzické osoby (typicky pak fyzické osoby podnikající) ochuzeny. To, že místo elektronické značky, kterou podle českého zákona může označovat fyzická i právnická osoba, budeme mít elektronickou pečeť a tu pouze pro právnické osoby, považujeme za nepřijatelné omezení fyzických osob, zejména fyzických osob podnikajících, či dokonce těch, kdo na základě nějakého pověření vykonávají činnost orgánů veřejné správy.[19]

Lze připomínkovat i další definice Nařízení:

1. kvalifikovaný certifikát pro elektronický podpis – velmi obtížně lze dovodit, co v příloze I se rozumí pod písmenem j), kde se praví „*pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena*

[19] Že takové osoby mohou existovat, je poměrně známým faktem a připouští to i EPZ v § 11 odst. 1 písm. e) nebo zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů v § 2 písm. c). Týká se to např. notářů a exekutorů.

v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování“; autoři tuší, že formulace je převzata z norem ETSI a má říci, že kvalifikovaný certifikát obsahuje pár klíčů, kdy privátní klíč je uložen bezpečně (např. v zařízení HSM) a je zaručena jeho nepopiratelnost (nonrepudiation), přičemž daný certifikát nemusí být vydán certifikační autoritou. V některých systémech mohou být totiž vyvářeny lokální certifikáty, k nimž jsou připojeny poznámky, resp. provozní data, která blíže specifikují prostředek, ve kterém byl certifikát vytvořen; poznámka pak dává informace, že i takto vytvořený certifikát je pro daný účel důvěryhodný;

2. prostředek pro vytváření elektronických podpisů a stejně prostředek pro vytváření elektronických pečetí – proč je třeba zdůrazňovat, že se jedná o „konfigurované“ programové vybavení nebo technické zařízení, resp. každé smysluplně použitelné zařízení by mělo být nějako konfigurováno,
3. certifikát pro elektronickou pečeť – proč certifikát potvrzuje název této osoby: proč jen název; nevíme, jak tomu je v jiných státech, ale lze se domnívat, že zaměnitelných názvů právnických osob i zde bude značné množství.

6. ELEKTRONICKÉ PODPISY

6.1 PODPISY PODLE SOUČASNÉ A NOVÉ PRÁVNÍ ÚPRAVY

Definice elektronického podpisu patří podle názoru autorů mezi ty, které si zasluhují hlubší zamyšlení. Podle rušené Směrnice[20] byl elektronický podpis definován jako „*údaj v elektronické podobě, který je připojen či logicky spojen s jinými elektronickými daty a který slouží jako metoda ověření pravosti*[21]“. Pravdou je, že tvrzení „údaj slouží jako metoda“ je poněkud neortodoxní, nicméně je zřejmé, že Směrnici šlo o *ověření pravosti podpisu*. Původní znění

[20] Směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy

[21] Čl. 2 bod 1 Směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy

českého EPZ v roce 2000[22] jej definovalo jako „*údaje… které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě*[23]“, podle stávajícího EPZ je elektronický podpis definován jako „*údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*[24]“. Vidíme, že českému zákonodárci nevadí nesmyslné ztotožnění údaje = metoda, ale zato důsledně nahradil ověření pravosti podpisu *ověřením identity podepsané osoby*. Pravděpodobně vzhledem k dikci § 40 odst. 4 předchozího občanského zákoníku (ObčZ), podle kterého „*Písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.*“. Tento požadavek ale nesouvisí s podpisem samotným, ale písemnou formou právního úkonu (podle ObčZ). Přes všechny nepřesnosti jsme nicméně stále věděli, že jde o atributy, které nám umožní ověřit pravost podpisu a to tak, že jsme schopni identifikovat osobu, která jej učinila.

Nařízení ale činí zásadní posun, když tvrdí, že elektronický podpis jsou „*data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání.*[25]“

Jinými slovy, nejde nám již o následnou možnost ověření pravosti podpisu či identity osoby pomocí dat nazvaných „elektronický podpis“, ale o to, že je položeno rovnítko mezi elektronický podpis a data, „*která podepisující osoba používá k podepsání.*[26]“ Z našeho pohledu to je rozhodně pozitivní. Tím totiž dochází k chápání podpisu podle jeho primární funkce, tj. jako k doložení skutečnosti, že určitá osoba projevila svoji vůli, případně že se v určitou dobu nacházela na určitém místě, popř. že stvrzuje platnost určitého dokumentu.[27] Jak říká americké právo, „*podpis spočívá v umístění jména na konec listiny, s cílem potvrdit její platnost. Může být vlastnoruční, vytištěný, vyražený na razítku, napsaný psacím strojem, vyrytý, ofotografovaný,*

[22] Zákon č. 227/2000 Sb. o elektronickém podpisu
[23] Ustanovení § 2 odst. a) zákona č. 227/2000 Sb. o elektronickém podpisu
[24] Ustanovení § 2 odst. a) zákona č. 227/2000 Sb. o elektronickém podpisu v platném znění
[25] Čl. 3 bod 10 Nařízení eIDAS
[26] Čl. 3 bod 10 Nařízení eIDAS
[27] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 271 an.

vyříznutý z jedné listiny a připojený ke druhé. Rovněž litografovaný podpis na listině postačuje k potvrzení její platnosti, přičemž je nepodstatné, jakým nástrojem se podpis udělá.“[28] Osoba si může za svůj podpis zvolit jakýkoli znak, symbol nebo kresbu. Současná právní úprava daná směrnicí 1999/93/ES a EPZ posouvala podpis někam jinam a přiřazovala mu funkci metody k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě (viz § 2 písm. a/ EPZ).

V rámci současných technologických možností přichází v úvahu řada variant skutečného provedení elektronického podpisu. V následujícím textu se proto budeme věnovat rozboru všech možností, přičemž budeme předpokládat, že čtenářům jsou známy principy podpisů na bázi asymetrické kryptografie,[29] které donedávna představovaly hlavní variantu realizace zaručeného elektronického podpisu podle směrnice a EPZ.

Pokud podepisující osoba používá k podepsání elektronickým podpisem data dle bodu 13 čl. 3 Nařízení, podle kterého „*daty pro vytváření elektronických podpisů jsou jedinečná data, která podepisující osoba používá k vytváření elektronických podpisů*“, pak při použití metody asymetrické kryptografie je těmito daty tajný (soukromý) klíč.

Ale pojďme v úvahách dále. Pokud tedy má mít osoba nějaká data (elektronická), jež může použít k podepsání, znamená to, že elektronickým podpisem jsou jakákoliv data v elektronické podobě, která jsou schopna být „*připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena*“[30]. Čili vlastně cokoliv, co můžeme zdigitalizovat. Elektronickým podpisem (prostým) podle Nařízení je tedy PIN, heslo, fráze, obrázek atd., tedy jakýkoliv digitální záznam, který má podobu nul a jedniček a který připojíme k podepisovanému dokumentu. To je také správně, protože v minulosti jsme složitě konstruovali výklad, jak podle Směrnice, resp. EPZ prohlásit použití PIN u platební karty za podepsání elektronické transakce. Naskýtá se také zajímavá možnost používat pro „prostý“ elektronický podpis hlas: hlas nepochybně digitalizovat lze, dokonce je sám o sobě jedinečným natolik, že jej prý lze jen velmi stěží napodobit, aniž by to při

[28] Maricopa County v. Osborn, 60 Ariz. 290, 136 P.2d 270, 274. Cit. dle BLACK, Henry Campbell; NOLAN, Joseph R.; NOLAN-HALEY, Jacqueline M. *Blackův právnický slovník.* 6. vyd., v ČR 1. Praha: Victoria Publishing, 1993, s. 1268.

[29] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 281 an.

[30] Čl. 3 bod 13 Nařízení eIDAS

následné analýze zůstalo skryto. Tím bychom vlastně vytvořili požadovanou vícefaktorovou autentizaci[31] u základního typu elektronického podpisu.

Klasický, tedy vlastnoruční podpis (který není definován právním řádem a ten s ním pracuje jako s notorietou) není vytvářen žádnými daty. *„Vlastnoruční podpis je výsledkem uplatnění návyku psaní, získaného v podobě individuálního a relativně stálého písemného projevu člověka. Vznik individuálnosti písma je důsledkem vytvoření dynamického stereotypu psaní, tedy vypracování složitého systému podmíněných reflexů, které jsou závislé na stupni procvičování. Při vytvoření konkrétního písemného projevu – tedy např. podpisu – se uplatňují ale i aktuální vnější a vnitřní podmínky, za kterých psaní probíhá a v jejichž důsledku může být získaný dynamický stereotyp narušen. Zkoumání pravosti písma (podpisu), které je zaměřeno na grafickou stránku směřující k identifikaci pisatele, je prováděno pomocí různých metod. Jak u podepisování, tak u zkoumání pravosti (ověřování) podpisu jde tedy o procesy převážně subjektivního charakteru, v nichž se promítají obecné a individuální vlastnosti zúčastněných osob. Tyto vlastnosti se dnes využijí i při ověřování pravosti tzv. dynamického biometrického podpisu, který kombinuje vlastnosti jak grafického, tak elektronického podpisu.*[32]*“*

Jde o tzv. biomechanický proces vzniku lidského podpisu, který není nikterak jednoduchý. Primární vzruch vzniká v centrálním nervovém systému – v lidském mozku s předem definovanou intenzitou a trváním. Nervový systém pak aktivuje příslušné svaly v definovaném pořadí. Pohyb pera po papíře, což je výsledek stahování a uvolňování svalů, zanechává stopu hrotu psacího nástroje.

Pokud se osoba vlastnoručně podepisuje, pak existují v zásadě dvě možnosti:

a) podepisuje se na nějakém fyzickém nosiči nástrojem (tužka, pero), který zanechává grafickou stopu – obraz podpisu (statický obraz), typicky na papíru, ale v podstatě jakémkoliv hmotném nosiči;

---

[31] Viz např. SMEJKAL, Vladimír; KODL, Jindřich. Development trends of electronic authentication. In: *Proceedings of the 42nd Annual Konference 2008 IEEE International Carnahan Conference on Security Technology*, Diplomat Hotel Prague, Czech Republic, October 13 - 16, 2008, s. 1 – 6.

[32] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s., s. 271.

b) podepisuje se na zařízení, které kromě obrázku snímá i neviditelné dynamické vlastnosti tohoto podpisu, spojené s typickým chováním podepisující se osoby – časy, rychlosti, zrychlení apod. Tím vzniká dynamický biometrický podpis (DBP).[33]

Podle autorů nová definice elektronického podpisu posiluje postavení DBP v právním řádu EU a ČR a vytváří možnosti pro přijetí i dalších, v budoucnu se objevivších metod pro elektronické podepisování, zejména, ale nikoliv pouze na bázi biometrie. Proto mu věnujeme níže více pozornosti.

Dynamický biometrický podpis je podobný případ, jako ve fyzice elektromagnetické záření, na které lze nahlížet jako na částici – kvantum energie v podobě fotonů, ale stejně dobře i jako na vlnění, a to v závislosti na uspořádání experimentu a způsobu pozorování.[34] Hovoříme o tzv. dualitě. Stejně tak DBP můžeme chápat dvěma paralelními způsoby, a to současně jako:

1. vizuální, viditelný, vlastnoruční podpis,
2. neviditelný, digitální, elektronický podpis.

Při vytvoření DBP vzniknou současně obě formy podpisu, kdy data použitá k podepsání jsou snímána 3D snímačem a mohou být jak uložena, tak zobrazena. DBP má tedy rovněž duální charakter, nicméně – na rozdíl od světla jakožto nejznámější formy elektromagnetického záření – můžeme u DBP jednotlivé složky oddělit a nakládat s nimi samostatně. Přitom stále se bude jednat o určitou formu podpisu, v 1. případě okem viditelného, ve 2. případě neviditelného, nicméně zobrazitelného prostřednictvím technického zařízení stejně, jako tomu je u podpisu kryptografického. Rozdílem mezi kryptografickým podpisem a DBP je mj. i to, že i z biometrických parametrů můžeme získat obrázek podpisu, zatímco u podpisu kryptografického je to pouze řada čísel.

---

[33] Viz SMEJKAL, Vladimír; KODL, Jindřich. Strong authentication using dynamic biometric signature. Proceedings of 45th Annual 2011 IEEE International Carnahan Conference on Security Technology (ICCST), 18-21 October 2011, Tecnocampus Mataró Maresme, Barcelona, Španělsko, s. 340 – 344 a SMEJKAL, Vladimír; KODL, Jindřich; KODL, Jindřich Jr. Implementing Trustworthy Dynamic Biometric Signature according to the Electronic Signature Regulations. In: *Proceedings of 47th Annual 2013 IEEE International Carnahan Conference on Security Technology (ICCST)*, 9-11 October 2013, Medellín, Colombia, ISBN: 978-958-8790-65-7, s. 165 – 170.

[34] Tzv. myšlenku duality částic a vlnění formuloval v roce 1905 Albert Einstein pro objasnění fotoelektrického jevu.

Data vytvořená vlastnoručním podpisem nejsou absolutně konstantní a neměnná, jako tomu je v případě soukromého klíče při asymetrické kryptografii, ale jsou dostatečně přesná a podrobná pro to, abychom je strojově, případně s pomocí písmoznalce ověřili.[35] Výhodou oproti kryptografickému elektronickému podpisu je existence oné „vlastnoručnosti", která je u soukromého klíče zajišťována pouze právním prohlášením podle § 5 odst. 1 písm. a) EPZ, podle kterého je podepisující osoba povinna zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití.[36]

V obou případech jsou tato data těmi daty, *která podepisující osoba používá k podepsání*[37], a s různou mírou věrohodnosti a námahy jsou daty, které nám umožní ověřit pravost podpisu prostřednictvím identifikace osoby, která jej učinila.

Nařízení se týká – jak název naznačuje – elektronické identifikace, ale především služeb s ní spojených, jež jsou nazývány „služby vytvářející důvěru". Co se týká oblasti, kterou bychom mohli nazvat „elektronický podpis – elektronická značka – časové razítko", pak zde nedochází k žádné dramatické změně oproti stávajícímu stavu. Na druhou stranu ale také byly promeškány některé příležitosti. V bodu (27) odůvodnění Nařízení se uvádí: „*Toto nařízení by mělo být z technologického hlediska neutrální. Právních účinků, které přiznává, by mělo být možné dosáhnout jakýmikoli technickými prostředky, jsou-li splněny požadavky tohoto nařízení.*" Podle názoru autorů to není zcela tak; EU se v roce 1999 vydalo – z tehdejšího pohledu pochopitelně a oprávněně – v oblasti elektronického právního jednání cestou jedinou: prostřednictvím elektronického podpisu na bázi asymetrické kryptografie, byť ve Směrnici 1999/93 v čl. 2 definice ad (4) zní „*daty pro vytváření podpisu se rozumí jedinečná data, jako jsou kódy nebo soukromé kryptografické klíče…*", takže již tato směrnice vytvořila prostor

[35] Viz SMEJKAL, Vladimír; KODL, Jindřich. Assessment of the authenticity of Dynamic Biometric Signature. The results of experiments. In: *Proceedings of 48th Annual 2014 IEEE International Carnahan Conference on Security Technology (ICCST)*, 13-16 October 2014, Roma, Italia, ISBN: 978-1-4799-3530-7, s. 45 – 49.

[36] SMEJKAL, Vladimír; KODL, Jindřich. Vícefaktorová autentizace a dynamický biometrický podpis. In: *Sborník 16. ročníku mezinárodní konference Information Security Summit (IS2)*, 27. – 28. května 2015, Praha: TATE International, s.r.o., s. 107 – 119.

[37] Čl. 3 bod 10 Nařízení eIDAS

pro jiné než kryptografické EP. Nicméně v posledních 5-10 letech se stále více diskutuje o vícefaktorové autentizaci[38] a o využití biometrických nástrojů pro identifikaci a autentizaci včetně podepisování.[39] Pouhý podpis jako obrázek představuje stejně jako heslo pouze jeden autentizační faktor a současným trendem je vícefaktorová autentizace[40], tj. k obrázku potřebujeme přidat něco dalšího, například biometrický záznam.

Podpis coby součást písemných právních úkonů byl v našem právním řádu upraven dříve v ust. § 40 odst. 3 a 4 ObčZ, nyní v ust. § 561 – 562 NOZ. Tomu odpovídala i úprava v EPZ, jež vycházel ze směrnice 1999/93/ES. Nařízení v tomto nepřináší žádnou změnu, neboť jak kryptografický elektronický podpis, tak dynamický biometrický podpis je vlastnoručním podpisem ve smyslu ust. § 561 odst. 1 věta první NOZ a vyhovuje požadavkům na písemnost podle § 562 odst. 1 NOZ. Oba jsou elektronickým podpisem podle platného EPZ a rovněž elektronickým podpisem podle Nařízení. Vyplývá to jak z výše citovaných definic, tak z principů, které se nacházejí v bodech 48 až 65 Nařízení a které se týkají přijímání elektronických podpisů s nižší zárukou bezpečnosti, jež nesplňují požadavky na kvalifikovaný elektronický podpis.[41] Tento princip je v čl. 25 odst. 1 Nařízení formulován následovně: *„1. Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.“*

Ve speciálních případech by zřejmě pak jako „obyčejný“ elektronický podpis ve smyslu Nařízení obstál i jiný druh digitálního záznamu, jak je uvedeno výše. Dikce věty druhé odst. 1 § 561 NOZ *„Jiný právní předpis*

---

[38] Viz SMEJKAL, Vladimír; KODL, Jindřich. Strong authentication using dynamic biometric signature. In: *Proceedings of 45th Annual 2011 IEEE International Carnahan Conference on Security Technology (ICCST)*, 18-21 October 2011, Tecnocampus Mataró Maresme, Barcelona, Španělsko, s. 340 – 344.

[39] Viz např. SMEJKAL, Vladimír; KODL, Jindřich, op. cit; SMEJKAL, Vladimír; KODL, Jindřich. Dynamický biometrický podpis – místo mýtů fakta. *Data Security Management*, XVI., 2012, č. 2, str. 20 – 23; DOSTÁLEK, Libor. Formáty pro zaručené elektronické podpisy. *Data Security Management*, XVI., 2012, č. 3, str. 42 – 45; Bernášek, Aleš, op. cit.

[40] SMEJKAL, Vladimír, KODL, Jindřich. Development trends of electronic authentication. In: *Proceedings of the 42nd Annual Konference 2008 IEEE International Carnahan Conference on Security Technology*, Diplomat Hotel Prague, Czech Republic, October 13 - 16, 2008, s. 1–6.

[41] Viz Rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím "jednotných kontaktních míst" podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu (Úř. věst. L 274, 20. 10. 2009, s. 36).

stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat“ bude zřejmě použitelná i po nabytí účinnosti Nařízení, které nepochybně může být oním „jiným právním předpisem“.

6.2 VLASTNORUČNÍ PODPIS DLE NAŘÍZENÍ

V čl. 25 odst. 2 Nařízení nalezneme konstatování, že „*Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.“* Je to vhodné, správné a přiměřené? Nutno předeslat, že příznivci elektronické komunikace již mnoho let poukazují na to, že „vyšší“ druhy elektronického podpisu podle EPZ (kvalifikovaný a zaručený elektronický podpis) by mohly být považovány za podpis vlastnoruční, neboť vykazují stejnou, spíše pak vyšší míru bezpečnosti, než klasický vlastnoruční podpis.

Ve skutečnosti tomu tak není. Jedním z rozdílů mezi kryptografickým a vlastnoručním podpisem (ať již s nebo bez biometriky) je skutečnost, že soukromý klíč není chráněn proti porušování právních a bezpečnostních opatření jeho vlastníkem. Typickou situací, s níž se autoři běžně setkávají, je použití soukromého klíče určité osoby (manažera, advokáta) jinou osobou (sekretářkou, asistentem), a to s jeho vědomím a na jeho výslovný pokyn. Statická biometrie není sice také zcela chráněna před použitím jinou osobou, ale s „propůjčením identity“ pomocí např. otisku prstu vytvořeného z vhodné umělé hmoty se v běžné praxi nesetkáváme. Ovšem zločinný útok na identitu je u statické biometrie daleko snazší, nežli u biometrie dynamické.

Je vhodné uvést, že formulaci „vlastnoruční podpis“ v českém právním řádu nenajdeme, naproti tomu je zde používán termín „podpis“, čímž se myslí právě podpis vlastnoruční (jak nasvědčuje dikce mnoha předpisů, např. § 33a odst. 4 zákona o účetnictví[42], přičemž se připouští, že tento „může být nahrazen mechanickými prostředky tam, kde je to obvyklé“[43]), případně pak podpis elektronický (obvykle s odkazem na EPZ).

V souvislosti se závěťmi používáme v právní terminologii označení „alografní závěť“ pro závěť, kterou zůstavitel nenapsal vlastní rukou, a „holografní závěť“ pro závěť sepsanou vlastní rukou (nyní viz ust. § 1533

[42] Zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
[43] § 561 odst. 1 věta druhá NOZ

– 1534 NOZ).[44] Bude zajímavé pak v návaznosti na zmíněný čl. 25 odst. 2 diskutovat, zda Nařízení může změnit stávající jednoznačný výklad ust. § 1534 předpokládající, že závěť, jež může být napsána na stroji či počítači, musí zůstavitel podepsat vlastní rukou, tj. učinit vlastnoruční podpis, nebo zda to může být kvalifikovaný elektronický podpis.

Vlastnoruční podpis je výsledkem uplatnění návyku psaní, získaného v podobě individuálního a relativně stálého písemného projevu člověka. Vznik individuálnosti písma je důsledkem vytvoření dynamického stereotypu psaní, tedy vypracování složitého systému podmíněných reflexů, které jsou závislé na stupni procvičování. Při vytvoření konkrétního písemného projevu – tedy např. podpisu – se uplatňují ale i aktuální vnější a vnitřní podmínky, za kterých psaní probíhá a v jejichž důsledku může být získaný dynamický stereotyp narušen.[45]

Kvalifikovaný elektronický podpis (dále také jen „KvEP“) je definován v čl. 3 odst. 12 Nařízení jako „*zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy*“. Kvalifikovaným prostředkem pro vytváření elektronických podpisů se rozumí podle odst. 23) prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II Nařízení. Tato příloha je formulována technologicky neutrálně a „nežene“ nás rovnou do hájemství asymetrické kryptografie. Ovšem druhý požadavek, podle kterého „*zaručený elektronický podpis… je založen na kvalifikovaném certifikátu pro elektronické podpisy*“ již vede přes certifikát k asymetrické kryptografii. Znamená tedy dikce čl. 25 odst. 2, že jiný než KvEP nemůže být považován za rovnocenný vlastnoručnímu podpisu?

Podle názoru autorů nelze toto tvrdit. Nařízení pouze činí jednoduchou cestu k uznání kryptografického podpisu na úrovni KvEP jako podpisu vlastnoručního a zavádí pravidlo, že kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech. (čl. 25 odst. 3). Nařízení ale neříká, že za vlastnoruční

[44] Tato terminologie vychází z použití předpon „alo“ pro odlišný či jiný a „holo“ pro celý, úplný, nedotčený.

[45] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 271.

podpis nemůže být v souladu s národním právním řádem považován i jiný druh podpisu, neboť „obyčejný“ elektronický podpis podle čl. 3 odst. 10 nebo zaručený elektronický podpis („ZEP“) podle odst. 11 čl. 3 již může být realizován jinou technologií, pokud splní zde formulované pojmové znaky (a v případě ZEP ještě požadavky stanovené v článku 26 – viz tabulka výše. V takovém případě budeme vycházet z dikce ust. § 561 a § 562 NOZ:

„§ 561 – (1) K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé. Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat. § 562 – (1) Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby.“

Jiným právním předpisem podle § 561 odst. 1 věty třetí je současný zákon o elektronickém podpisu. Pokud by byl nějakým způsobem změněn (v důsledku Nařízení), pak s přihlédnutím k dikci Nařízení v bodu (49) odůvodnění by se za podpis měly považovat všechny formy elektronického podpisu podle Nařízení. A kromě toho čl. 27 odst. 1 Nařízení, podle kterého se výslovně připouští pro využití určité on-line služby, která je poskytována subjektem veřejného sektoru nebo jeho jménem, zaručené elektronické podpisy, zaručené elektronické podpisy založené na kvalifikovaném certifikátu pro elektronické podpisy a kvalifikované elektronické podpisy.

Autoři se obávají, že čl. 25 odst. 2 může být státními orgány, resp. jimi vytvořenou legislativou interpretován úzce a v rozporu s principy tohoto Nařízení tak, že pouze KvEP je tím jediným, který může být považován za podpis vlastnoruční. Konec konců s restriktivním přístupem jsme se setkali již v rámci zákona č. 167/2012 Sb., kterým se změnil zákon č. 499/2004 Sb., o archivnictví a spisové službě, zákon č. 227/2000 Sb., o elektronickém podpisu a další zákony, přičemž provedené změny nebyly vždy zcela vhodné. Novela mj. v EPZ vypustila bez náhrady definici elektronické veřejné listiny a ve všech dosavadních předpisech původně požadovaný „zaručený elektronický podpis založený na kvalifikovaném certifikátu“ byl nahrazen podpisem vyššího stupně, tj. „uznávaným elektronickým podpisem“, ačkoliv k tomu nejsou žádné právní, ani technické důvody.

Takovýto závěr by autoři považovali za zcela nesprávný a navíc nemající oporu v odst. 2, když toto ustanovení výslovně klade rovnítko mezi KvEP a vlastnoruční podpis, žádné jiné formy podpisu nezmiňuje a pokus o uplatnění argumentu a contrario zde autoři nepovažují za možný – ani z jiných ustanovení Nařízení, ani z Nařízení jako celku nelze dovodit, že by jeho cílem bylo jakkoli se vymezit vůči jiným formám elektronického podpisu, v Nařízení výslovně neupraveným, což je nejvýrazněji, ale nikoliv jako jediný právě příklad dynamického biometrického podpisu, a to navzdory poněkud nešťastnému ustanovení čl. 25 odst. 2 Nařízení. Pokud by se v odst. 2 místo o vlastnoručním podpisu hovořilo o úředně ověřeném podpisu, bylo by takové ustanovení plně na místě. Současný zákon o elektronickém podpisu zatím neobsáhl takovou právní úpravu, aby nahradil úředně ověřený podpis, pouze vytvořil alternativu k podpisu vlastnoručnímu, jakkoliv by to drobnou úpravou § 11 EPZ a využitím sítě Czech POINT bylo zřejmě řešitelné.[46]

Je ale především zvláštní, jak po celou dobu oněch 15 let od vydání Směrnice jsou na elektronické podpisy stále znovu a znovu kladeny nepoměrně vyšší požadavky, nežli na podpisy na papíru, ačkoliv podpis na papíru je snadněji padělatelný nežli podpis elektronický. Obecně stále platí již od dob římského práva, že zákonodárce by se měl vyhýbat kazuistickým úpravám a usilovat naopak o co nejobecnější definice. Autoři jsou si vědomi toho, že v praxi je však bohužel situace často opačná – právě kazuistické předpisy čím dál více znejasňují právní řád ČR i EU. Zejména v oblasti vyvíjející se natolik dynamicky, jako je tomu v oblasti informačních technologií (např., ale nikoliv pouze u elektronického podpisu), se k tomu navíc přidává požadavek technické neutrality – je zřejmé, že vývoj se nezastaví u dnes používaných forem elektronického podpisu a lze očekávat, že dříve, či později (dle názoru autorů spíše dříve) budeme řešit výkladové problémy způsobené tím, že reálný vývoj opět předběhl text Nařízení.

Řešením splňujícím požadavek bodu (49) a realizujícím princip technologické neutrality bude rozšíření českého EPZ, resp. pravděpodobného torza, které vzhledem k Nařízení z něj zůstane, o ustanovení, které bude deklarovat, že za vlastnoruční podpis budeme

[46] MATES, Pavel; SMEJKAL, Vladimír, op. cit., s. 254.

považovat i zaručený elektronický podpis, tedy nikoliv jako doposud absolutizovaný uznávaný EP[47]. Jenže vzhledem k silné lobby poskytovatelů certifikačních služeb na příslušných orgánech, se lze obávat spíše pravého opaku, a to přes existenci rozsudku Nejvyššího správního soudu ze dne 16. 3. 2007, podle kterého „*Zaručený elektronický podpis jako jeden z druhů elektronického podpisu představuje ekvivalent "ověřeného podpisu" na papíru a využívá takových technologických postupů, které umožňují jednoznačnou identifikaci a autentizaci osoby, která podpis vytvořila. Zaručený elektronický podpis zaručuje, že datovou zprávu podepsala oprávněná osoba. Zaručené elektronické podpisy podložené osvědčením vydaným ověřovatelem informací (poskytovatelem certifikačních služeb) budou potom uznány jako vlastnoruční podpis v případech, kdy takový vlastnoruční podpis požadují právní předpisy nebo dohoda stran.*[48]“

Článek 27, který upravuje elektronické podpisy ve veřejných službách, v odst. 3 uvádí, že „*Členské státy nesmějí v případě přeshraničního využívání on-line služby poskytované subjektem veřejného sektoru vyžadovat elektronický podpis s vyšší zárukou bezpečnosti než kvalifikovaný elektronický podpis.*“ Vzhledem k tomu, že komunikace s orgány veřejné moci musí být i přeshraniční, mohlo by tímto dojít k potlačení hypertrofického nasazení uznávaného elektronického podpisu podle § 11 EPZ, ke kterému došlo v rámci velmi svérázné novely EPZ zákonem č. 167/2012 Sb. Ta nahradila ust. § 11 novým zněním a především do dalších předpisů týkajících se soukromoprávních subjektů „natvrdo“ místo zaručeného elektronického podpisu na bázi kvalifikovaného certifikátu navedlo požadavek na používání uznávaných podpisů. Potom vzhledem k rovnému přístupu k osobám v rámci EU by v souladu s odst. 3 nemělo být ani pro tuzemské osoby požadováno použití uznávaných podpisů.

Ostatně, výše zmiňovaný příklad dynamického biometrického podpisu není jistě jediným příkladem podpisu, který vybočuje z poněkud svazujících definic Nařízení. Autoři se ve své praxi setkali s otázkou, jak je tomu například u smluv uzavíraných dnes poměrně běžně u řady finančních institucí, či operátorů elektronických komunikací v rámci telefonického hovoru. Telefonický hovor v současnosti v sítích elektronických komunikací

[47] Viz např. rozhodnutí II. ÚS 218/06-1, II. ÚS 299/06-1, 7 Afs 83/2006-97.
[48] Rozsudek Nejvyššího správního soudu ze dne 16. 3. 2007, spis. zn. 5 Afs 110/2006-113.

(viz ust. § 2 písm. h) a i) zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů v platném znění) bezesporu probíhá „elektronicky“. O tom, že lze tímto způsobem platně uzavřít smlouvu, také nelze mít pochybnosti. Lze však takto uzavřenou smlouvu také elektronicky podepsat?

První otázkou je, zda lze právní jednání učiněné hlasem, bez jeho písemného zachycení, spolehlivě přiřadit konkrétní fyzické osobě. Na tuto otázku odpovídá odvětví tzv. audioexpertizy (fonoskopie, tedy odvětví zabývající se zkoumáním lidského hlasu s cílem ztotožnit neznámého mluvčího s mluvčím, u kterého je jeho identita známa, tedy takového mluvčího verifikovat) a odpovídá na ni kladně – navzdory tomu, že hlas fyzické osoby není s plynutím času a vlivem dalších okolností (vnějších i vnitřních – např. zdravotních) zcela neměnný, lze po provedení analýzy učinit jednoznačný závěr o totožnosti mluvčího.

Pakliže je možno hlasem, a tedy nepísemně, přesto však elektronicky, uzavřít smlouvu, co je u takto uzavřené smlouvy oním podpisem? Přikláníme se k závěru, že takovýmto „podpisem“ je u hlasem uzavírané smlouvy samotný hlasový projev kontrahenta/mluvčího – osvědčuje jeho souhlas s textem uzavírané smlouvy a přitom – podobně jako vlastnoruční podpis, resp. mnohdy patrně i jednoznačněji – splňuje kritérium jednoznačnosti. V režimu podle NOZ se jedná o právní jednání ve smyslu ust. § 545 an. NOZ, a to jako jednání realizované konáním ve smyslu § 546 jako jednání spíše výslovné (hlasem), nežli konkludentní (chováním).

Lze zde však hovořit o podpisu elektronickém jen proto, že je hlasový projev učiněn s využitím elektronických prostředků (a případně jeho nahrávka zaznamenána na elektronické médium)? Samotná skutečnost, že smlouva byla hlasově uzavřena za použití sítě elektronických komunikací, je pro učinění závěru ohledně jejího elektronického podpisu irelevantní. Rozhodující je, zda by „hlasový podpis“ bylo možno zahrnout do definice elektronického podpisu, ať již při použití definice v ZEP, či při použití definice dle Nařízení. Hlas je sice logicky spojen s datovou zprávou – hlasovou nahrávkou, která je oním hlasem činěna, navíc – ve světle výše uvedeného ohledně jednoznačnosti závěru analýzy hlasu - slouží jako metoda k ověření identity podepsané osoby, tím spíše svůj hlas podepisující osoba používá k podepsání (a dokonce lze říci, že hlas/hlasový podpis: 1. je

jednoznačně spojen s podepisující osobou, 2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě a 3. nepochybně byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou), lze však učinit paralelu mezi hlasem coby „údajem v elektronické podobě"? Tuto úvahu ponechávají autoři k diskusi.

7. OVĚŘOVÁNÍ PLATNOSTI KVALIFIKOVANÝCH ELEKTRONICKÝCH PODPISŮ A DALŠÍ SLUŽBY

Podle čl. 32 Nařízení se 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, který obsahuje požadavky na zaručené elektronické podpisy.

Zajímavá je dikce písm. b), podle níž je možné ověřovat KvEP i po vypršení platnosti certifikátů; podstatné je, že certifikát byl platný v okamžiku podpisu. Naproti tomu český zákon o archivnictví výslovně požaduje přidání časového razítka, aby mohl být podepsaný dokument považován za pravý – viz § 69a odst. 5 zákona č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů (dále také jen

ArchZ) a podobně tomu je i při provádění konverze podle § 24 odst. 1 písm. b) zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (dále také jen ElÚkZ). I v tomto směru tedy autoři hodnotí Nařízení pozitivně; otázkou ovšem je, jak budeme moci určit bez časového razítka, kdy byl podpis učiněn. Podle názoru autorů časové období, v němž byl podpis vytvořen, by bylo možné vysledovat z metod a procesů, kterými byl podpis vytvořen, tedy podle metody RSA (konkrétně podle použité délky klíčů), podle typu hash funkce (dříve SHA-1, nyní SHA-256) apod. Jedná se však o údaje, u nichž je nutno počítat s tolerancí cca 5 let; přesný časový okamžik, kdy byl podpis ve skutečnosti vytvořen, bez vazby na důvěryhodný časový údaj nezjistíme.

Následující články Nařízení kodifikují „přídavné“ služby týkající se elektronických podpisů. Čl. 33 zavádí „kvalifikovanou službu ověřování platnosti kvalifikovaných elektronických podpisů“, kterou může poskytovat kvalifikovaný poskytovatel služeb vytvářejících důvěru. Čl. 34 pak definuje „kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů“. V tomto případě, stejně jako u podpisů, certifikátů, pečetí, časových razítek atd. může Komise prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikovanou službu uchovávání kvalifikovaných elektronických podpisů. Nechme se tedy překvapit, jaké metody budou doporučeny.

8. ODPOVĚDNOST ZA ŠKODU

Jedním z cílů Nařízení je podle bodu 18. Preambule „*stanovit odpovědnost oznamujícího členského státu, strany vydávající prostředky pro elektronickou identifikaci a strany provozující postup autentizace za nedodržení příslušných povinností z tohoto nařízení vyplývajících*“. Tato odpovědnost za škodu je definována v čl. 11 Nařízení a týká se přeshraničních transakcí.

Dalším cílem je podle bodu 35 definování odpovědnosti poskytovatelů služeb vytvářejících důvěru. Nařízení v čl. 13 zavádí režim odpovědnosti, podle kterého by všichni poskytovatelé služeb vytvářejících důvěru měli odpovídat za škodu, kterou fyzické nebo právnické osobě způsobí v důsledku nesplnění povinností podle tohoto nařízení. Posoudit finanční riziko, které poskytovatelé služeb vytvářejících důvěru mohou být nuceni nést nebo které by mělo být kryto jejich pojistnou smlouvou, není snadné.

Za účelem snížení tohoto rizika (příp. jeho snadnějšího posouzení) Nařízení poskytovatelům služeb vytvářejících důvěru umožňuje stanovit za určitých podmínek omezení týkající se využívání jimi poskytovaných služeb a zprostit se tak odpovědnosti za škody vyplývající z využívání služeb nad rámec těchto omezení. Zákazníci by měli být o těchto omezeních předem řádně informováni a tato omezení by měla být rozpoznatelná pro třetí osoby, například tím, že informace o těchto omezeních budou zahrnuty v podmínkách poskytované služby, nebo jinými rozpoznatelnými prostředky. Za účelem účinného uplatňování těchto zásad by se toto nařízení mělo použít v souladu s vnitrostátními pravidly odpovědnosti. Tato vnitrostátní pravidla týkající se například vymezení škody, úmyslu nebo nedbalosti nebo související platná procesní pravidla proto tímto nařízením nejsou dotčena.

Povinnost nahradit škodu je dnes vymezena v ust. § 2909 až § 2913 NOZ, a to na základě: 1. porušení dobrých mravů (§ 2909), 2. porušení zákona (§ 2910) nebo 3. porušení smluvní povinnosti (§ 2913). Podle § 2910 *„Škůdce, který vlastním zaviněním poruší povinnost stanovenou zákonem a zasáhne tak do absolutního práva poškozeného, nahradí poškozenému, co tím způsobil. Povinnost k náhradě vznikne i škůdci, který zasáhne do jiného práva poškozeného zaviněným porušením zákonné povinnosti stanovené na ochranu takového práva.*“ První věta chrání osobnostní práva, věcná práva a práva k nehmotným statkům. V případě věty druhé se musí jednat o porušení speciální prevenční normy, kterou v daném případě je Nařízení, které je přímo použitelnou právní normou EU a kde se v čl. 13 odst. 1 konstatuje, že „*poskytovatelé služeb vytvářejících důvěru odpovídají za škodu, kterou úmyslně nebo z nedbalosti způsobí fyzické nebo právnické osobě nesplněním povinností podle tohoto nařízení*“. Pokud se zde konstatuje, že „V *případě kvalifikovaného poskytovatele služeb vytvářejících důvěru se úmysl nebo nedbalost předpokládá, pokud daný kvalifikovaný poskytovatel služeb vytvářejících důvěru neprokáže, že škoda podle prvního pododstavce nastala bez jeho úmyslu nebo nedbalosti.*“, pak podle názoru autorů je zřejmě v rozporu s českým právem, aby se prokazování či neprokazování zavinění vztahovalo pouze na určitou skupinu poskytovatelů služeb. Podle NOZ osoba způsobí škodu zaviněně, pokud ji spáchala úmyslně nebo z nedbalosti, přičemž podle § 2911 se předpokládá, že k porušení povinnosti ze zákona došlo

z nedbalosti. Škůdce je tedy za škodu odpovědný zpravidla pouze v případě, že ji skutečně zavinil, bez ohledu na to, jak je označen či jakému dohledu podléhá. Nicméně toto by měl řešit odst. 3 čl. 13, podle kterého platí, že „*odstavce 1 a 2 se použijí v souladu s vnitrostátními pravidly upravujícími odpovědnost za škodu*“. Je otázkou, zda bude ust. čl. 13 odst. 1 Nařízení vnímáno v ČR jako lex specialis k NOZ, či nikoliv.

Co se týká odst. 2 čl. 13, podle kterého „*Pokud poskytovatelé služeb vytvářejících důvěru své zákazníky předem řádně informují o omezeních týkajících se využívání jimi poskytovaných služeb a tato omezení jsou rozpoznatelná pro třetí osoby, neodpovídají poskytovatelé služeb vytvářejících důvěru za škody způsobené využíváním služeb nad rámec uvedených omezení.*“, pak v současnosti lze tato omezení definovat funkčně (postupy poskytovatelů nebo vlastnosti služeb či produktů); omezení ve formě limitace náhrady škody případně vzniklé využíváním služeb vytvářejících důvěru patrně čl. 13 odst. 2 neměl na mysli, když z jeho textu vyplývá, že má jít o „omezení týkající se využívání poskytovaných služeb“. Nehledě na toto ustanovení je však obecně v českém právním řádu možné i limitovat výši náhrady škody, a to dle NOZ, což by bylo možno uplatnit i na služby vytvářející důvěru – v daném případě by se ovšem s ohledem na dikci § 2898 NOZ takováto limitace vztahovala pouze na případy „běžné nedbalosti“, neboť dle téhož ustanovení NOZ „*Nepřihlíží se k ujednání, které předem vylučuje nebo omezuje povinnost k náhradě újmy způsobené člověku na jeho přirozených právech, anebo způsobené úmyslně nebo z hrubé nedbalosti; nepřihlíží se ani k ujednání, které předem vylučuje nebo omezuje právo slabší strany na náhradu jakékoli újmy. V těchto případech se práva na náhradu nelze ani platně vzdát.*“

9. SLUŽBA ELEKTRONICKÉHO DOPORUČENÉHO DORUČOVÁNÍ

Bod (66) odůvodnění Nařízení konstatuje, že „*Je nezbytné stanovit právní rámec, který usnadní přeshraniční uznávání služeb elektronického doporučeného doručování mezi stávajícími vnitrostátními právními systémy. Tento rámec by mohl rovněž přinést nové tržní příležitosti pro poskytovatele služeb vytvářejících důvěru z Unie, kteří budou moci nabízet nové panevropské služby elektronického doporučeného doručování.*“. Autorům není zcela zřejmý důvod, pro který byl použit termín „doporučené doručování“ místo např. vhodnějšího

„důvěryhodné doručování“. Podstatnější problém ale zjistíme později při čtení dalších ustanovení.

Koncepce tohoto doručování není příliš specifikována. Čl. 43 odst. 1 Nařízení vychází z již tradiční proklamace o tom, že „*Datům odeslaným a přijatým prostřednictvím služby elektronického doporučeného doručování nesmějí být upírány právní účinky a nesmějí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že mají elektronickou podobu nebo že nesplňují požadavky na kvalifikovanou službu elektronického doporučeného doručování.*“.

Teprve odst. 2 nám prozradí, oč by se asi mělo jednat. Podle něj „U *dat odeslaných a přijatých prostřednictvím kvalifikované služby elektronického doporučeného doručování platí domněnka integrity dat, odeslání těchto dat identifikovaným odesílatelem, jejich přijetí identifikovaným příjemcem a správnosti data a času odeslání a přijetí, jež jsou u kvalifikované služby elektronického doporučeného doručování uvedeny.*“. Všechny tyto požadavky splňují datové schránky podle ElÚkZ. Až bychom se mohli domnívat, že se tvůrci Nařízení inspirovali právě jimi.

Požadavky na kvalifikované služby elektronického doporučeného doručování dle čl. 44 jsou ale zbytečně kazuistickým popisem, který vyžaduje striktní řešení tam, kde lze postupovat i prostřednictvím jiných mechanismů. Zatímco požadavky odst. 1 písm. a), b), c)e a f) lze považovat za standardní, nejproblematičtější je dikce písm. d), podle kterého „*odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat“*.

Existuje řada jiných možností, jak zajistit, „*aby byla vyloučena možnost nezjistitelné změny dat“,* zejména s využitím kryptografických nástrojů, které nicméně nebudou ani zaručeným elektronickým podpisem, ani zaručenou elektronickou pečetí. Nebo opačně: pokud autoři Nařízení chtěli, aby byly zprávy elektronicky podepsány či orazítkovány, měli to napsat rovnou a jednoznačně.

Protože nevíme, jakými postupy jsou požadavky čl. 44 realizovány v informačním systému datových schránek (viz ust. § 14 ElÚkZ), bude na správci IS DS, kterým je Ministerstvo vnitra, aby tyto aspekty prozkoumal

a zaujal k nim stanovisko. V tomto případě se jeví jako obzvlášť důležité a současně náročné, zajistit interoperabilitu mezi různými systémy elektronického doporučeného doručování. Je otázkou, zda a jak to bude dosažitelné, resp. zda se kvůli požadované interoperabilitě nevrátíme od datových schránek zpět do minulosti. Pokud bychom brali v potaz splnění všech požadavků čl. 44 odst. 1, pak totiž asi nebudeme potřebovat IS DS, ale spíše jen nějaké prostředí pro užívání EP/EZ/ČR.

10. ZÁVĚR

V Nařízení se tvrdí, že „*Budování důvěryhodnosti on-line prostředí má pro hospodářský a sociální rozvoj klíčový význam. Nedostatečná důvěra, zejména v důsledku pocitu nedostatku právní jistoty, vede k tomu, že se spotřebitelé, podniky a orgány veřejné moci zdráhají provádět transakce elektronickými prostředky a přijímat nové služby.*“ Po seznámení s jeho obsahem, přinejmenším v oblasti elektronického podpisu, můžeme sice mít pocit, že by mohlo vést ke zvýšení právní jistoty, a to i přesto, že jeho text je těžkopádný a legislativně poněkud nešťastný. Je třeba ocenit, že byl po 15 letech vydán nový dokument, nicméně další rozvoj vědy a techniky v oblasti elektronické identifikace a autentizace se do něj promítl v tak malé míře, že je třeba si položit otázku, zda rozsah a především praktický přínos změn je skutečně adekvátní dlouhotrvajícímu legislativnímu procesu příprav na text zcela nového nařízení. Je zřejmé, že terminologie je v mnohém poplatná normám ETSI bez snahy o větší obecnost a univerzálnost. Hlavní problém vidíme v jejím rigidním lpění na asymetrické kryptografii a zejména certifikátech, jako údajně jediné možné variantě pro bezpečný elektronický podpis, resp. jakoukoliv autentizaci s vyšší úrovní zaručenosti.

To se týká jak elektronického podpisu, resp. povýšení KvEP na podpis vlastnoruční (čl. 25 odst. 2 Nařízení), jakož i některých požadavků na systémy elektronického doporučeného doručování (čl. 44 odst. 1 písm. d). Naštěstí vzhledem k výše zmíněné „dualitě“ dynamického biometrického podpisu lze očekávat přinejmenším diskusi v souvislosti s ním a vlastnoručním podpisem.

Z našeho pohledu není dynamický biometrický podpis náhradou kryptografického elektronického podpisu, ale významnou alternativou,

kterou lze použít v případech, kdy implementování certifikátů, bezpečné ukládání a „hlídání" privátních klíčů apod., by významným způsobem narušilo rutinní a ustálené procesy, případně působilo jako bariéra odrazující běžné uživatele (smluvní strany).[49] Zasloužil by si proto větší podporu zejména v tomto Nařízení.

Zásadní novou kvalitu Nařízení prakticky nepřináší, byť v detailech je lze považovat za lepší variantu oproti směrnici 1999/93/ES. Určitě pak ne v České republice, která některé velice pokročilé nástroje eGovernmentu, jako jsou např. elektronická značka, časové razítko a především systém důvěryhodného doručování pomocí datových schránek zakotvila ve své legislativě a prakticky jej realizovala již před několika lety. Mohlo by mít význam spíše z hlediska interoperability, ale to uvidíme až podle toho, jak budou nastaveny technické parametry a jak se s Nařízením vypořádají členské země. Jak si autoři pamatují z projednávání implementace Směrnice o elektronických podpisech v roce 2003[50], ani po pěti letech od jejího vydání se to členským zemím nepodařilo a v některých se tak nestalo doposud. Proto neočekáváme, že by došlo k zásadnímu zlomu brzy po nabytí účinnosti Nařízení.

Tento příspěvek se pokusil vyložit jednotlivá ustanovení Nařízení eIDAS týkající se elektronického podpisu a témat souvisejících alespoň tak, aby Nařízení neškodilo stávajícím dobrým a zavedeným institutům a bylo aplikovatelné nejen v České republice. Nejsme si bohužel jisti, že to vždy bude možné (viz výše k čl. 25 odst. 2 a k čl. 44). Jsme však přesvědčeni, že by si jej přečíst všichni, kdo přicházejí do kontaktu s elektronickými podpisy, aby nepodlehli různým účelovým, ba mnohdy dokonce přímo „katastrofickým výkladům" o dopadech vyvolaných Nařízením, jež se nyní objevují a s nimiž se autoři setkávají nezřídka i v odborných příspěvcích a diskusích na Internetu.

[49] SMEJKAL, Vladimír, KODL, Jindřich. Vícefaktorová autentizace a dynamický biometrický podpis. In: *Sborník 16. ročníku mezinárodní konference Information Security Summit (IS2)*, 27. – 28. května 2015, Praha: TATE International, s.r.o., s. 107 – 119.

[50] DUMORTIER, Jos a kol., op. cit.