va a s politickými stanovisky Unie, která má být společenstvím práva s vyšším standardem právní ochrany jednotlivce ve srovnání s obecným mezinárodním právem.

Jeden z možných směrů budoucího vývoje odpovědnosti Evropské unie naznačuje závazek v primárním právu – v čl. 6, odst. 2 SEU. Až se Evropská unie stane smluvní stranou Evropské úmluvy o ochraně lidských práv a základních svobod, bude možno ji přímo žalovat před Evropským soudem pro lidská práva jako subjekt odpovědný za porušení práv zaručovaných Úmluvou stejně jako smluvní státy. Vymahatelnost odpovědnostních povinností EU tak dostane zcela nový rozměr a přinese značné posílení práv jednotlivce.

Evropské nařízení eIDAS: Impuls pro sjednocení elektronického podpisu a identifikace v EU*

Vojtěch Kment
doktorand katedry teorie práva a právních učení Právnické fakulty Univerzity Karlovy v Praze

The EU regulation eIDAS: The Impuls to Unify the Electronic Signature and the Electronic Identification in the EU

Summary: *The paper shortly introduces the recently published Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (abbreviated „eIDAS„). Several areas of the electronic signature adjustment are considered questionable. The Regulation does not include the principle WIPIWIS (What Is Presented Is What Is Signed) as well as it does not determine suitable duties for the signatory and/or relying party. The lack of such provisions may cause the easy repudiation of the signature by the alleged signatory. While the Regulation boldly states the equivalance of the qualified electronic signature to the handwritten signature the analysis discovers that the legal evidence effect may hardly be considered the same. The Regulation also looses some conditions likely in order to allow the usage of the cloud saved private key. Such technique may improve the deployment of the electronic signature technology essentially but lower its security too. It is considered unfortunate that the Regulation abandoned the possibility to limit the use of the qualified certificate by the signatory because it would allow him to control its risks and expenditures. The paper summarizes the impact of eIDAS to the Czech legal system and the necessary related updates of the Czech law. The paper also describes some activities of the European Commission during the pending period of the preparation of the implementing acts.*

Key words: *eIDAS, electronic signature, electronic identification, european law*

Dne 28. srpna 2014 vyšlo v Úředním věstníku Evropské unie nové Nařízení Evropského parlamentu a Rady o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „eIDAS“[1] nebo „nařízení“).[2] Jako přímo aplikovatelný právní předpis by mělo významně ovlivnit pomocí počítačů prováděné právní jednání aj. elektronické transakce ve všech členských státech Evropské unie včetně České republiky. V tomto článku nařízení velmi stručně představuji, včetně informací o důvodech jeho přijímání, o procesu přijímání a hlavních očekávatelných právních důsledcích.

Nařízení má stanoveno několik přechodových období, předpokládá vydání dalších pro-

* Tento článek byl zpracován v rámci projektu specifického vysokoškolského výzkumu Univerzity Karlovy v Praze, který je registrován pod č. SVV č. 260 005.

1 Zkratka eIAS vyjadřuje obsah nařízení jako akronym ze slov „Identification-Authentification-Signature.“ Častěji užívaná eIDAS znamená buď totéž, nebo je považována za zkrácené vyjádření „electronic IDentification And Services.“

2 Viz http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

váděcích aktů s odkazy na technické specifikace, je však záhodno se s ním začít seznamovat. Kupř. schémata elektronické identifikace by mělo být možné dobrovolně uznávat již od roku 2015.

Oblast působnosti nařízení a podstata základních pojmů

V oblasti působnosti nařízení dosud v rámci práva EU platila nařízením rušená směrnice 1999/93/ES (dále „DirES"). Ta se zabývala rámcem elektronických podpisů ve Společenství a měla za cíl harmonizovat jejich právní úpravu. Na jejím základě byla do národních právních řádů transponována úprava elektronických podpisů, v ČR zákonem č. 227/2000 Sb., o elektronickém podpisu (dále jen „ZoEP"). Na elektronické podpisy aj. pojmy dle tohoto zákona se poté v ČR odvolává řada zejména procesních předpisů, jak správního práva včetně správního řádu, tak i všech soudních řádů (civilní, správní, trestní). Odvolávku obsahoval ale i dřívější občanský zákoník v § 40 a obsahuje ji ve svém § 561 i nový občanský zákoník, nyní touto formulací: „Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat." Lze tedy říci, že elektronický podpis byl směrnicí DirES i v českém právním řádu konstruován jako oborově průřezový právní institut, který potenciálně zasahuje všechna právní odvětví!

Po 14 letech zkušenosti lze ale konstatovat, že vysoká očekávání, která elektronický podpis vzbuzoval na přelomu milénia, prakticky nikde v Evropské unii dodnes nesplnil a to zejména co do svého rozšíření. Například dle údajů kvalifikovaných poskytovatelů certifikačních služeb sídlících v ČR[3] bylo za rok 2013 vydáno zhruba 280 tisíc kvalifikovaných certifikátů, což znamená, že vytvořit tzv. zaručený elektronický podpis je v ČR schopno méně než 4 % z počtu obyvatel v ekonomicky aktivním věku. Hlavní motivace Evropské unie ke změně bohužel nevycházela z tohoto fiaska, neboť by se pak soustředila na zjišťování příčin takového stavu. Evropská komise si dlouho neuspokojivé situace vůbec nebyla vědoma, nebo toto vědomí potlačovala. Komise sice vydala v březnu 2006 stručnou desetistránkovou přezkumnou zprávu ohledně naplňování DirES,[4] určenou Evropskému parlamentu a Radě, ve kterém nízkou rozšířenost přiznává, nicméně závěr vrcholí konstatováním:[5] „cíle Směrnice byly vesměs dosaženy a v této fázi nevyvstaly žádné jasné potřeby pro její revizi." Za zmínku stojí, že Komise vydala tuto zprávu téměř o tři roky později vůči termínu 19. 6. 2003, který byl stanoven směrnicí v čl. 12. Přitom Komise, nejpozději od tzv. Durmotierovy studie[6] z roku 2003, tyto informace o pouze izolovaných a vzájemně nekompatibilních ostrůvcích nasazování elektronického podpisu měla k dispozici. Nejméně do roku 2010 se pak na evropské úrovni nedělo prakticky nic až na příležitostně vypracovávané studie, z nichž nejvýznamnější zřejmě je tzv. CROBIES.[7] Jedním z hybatelů pokroku se pak kupodivu stalo přijetí směrnice 2006/123/ES, o službách na vnitřním trhu, která vyžaduje vytvoření tzv. jednotných kontaktních míst, se kterými by osoby mohly komunikovat i přeshraničně, vzdáleně a to i elektronicky. Právě při jejich zřizování se v praxi ukázalo, že řešení elektronického podpisu z různých členských států jsou nekompatibilní nejen technicky, ale i právně. Motivací Komise pro návrh nového nařízení proto především bylo zajištění přeshraniční interoperability elektronického podpisu. Tento důvod je uváděn Komisí i v důvodové části návrhu nařízení.[8] Forma nařízení pak zřejmě byla zvolena proto, aby co nejvíce odpadly potíže s možnými právními nesrovnalostmi mezi členskými státy navzájem.[9,10]

V průběhu let se k elektronickému podpisu přidávala i problematika elektronické identifikace. Asi prvně je v unijních dokumentech zmiňována v Akčním plánu pro elektronické podpisy a elektronickou identifikaci, zaměřeném na usnadnění poskytování přeshraničních veřejných služeb v rámci jednotného trhu.[11]

---

3 Jedná se o společnost První certifikační autorita, a.s., službu PostSignum České pošty s.p. a společnost eIdentity a.s.

4 Commission of the European Communities, *Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures*, COM (2006) 120 final, Brussels: 2006. Viz http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:01 20:FIN:EN:PDF

5 Commission of the European Communities, *op. cit.*, s. 10.

6 DURMOTIER, J. / KELM, S., NILSSON, H. / SKOUMA, G. / VAN EECKE, P.: *The legal and market aspects of electronic singnatures – final report, Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EEA, the Candidate and the Accession countries,* Interdisciplinary centre for Law & Information Technology (ICRI) – Katholieke Universiteit Leuven, Leuven: October 2003. http://www.epractice.eu/files/media/media_581.pdf – navštíveno 11/2013.

7 SEALED, TIME.LEX. SIEMENS: *CROBIES: Study on Cross-Border Interoperability of eSignatures – Head Document*, 2010.

8 Proposal for a Regulation of the European Parliament and of the Council on the electronic identification and trust services for electronic transactions in the internal market, drafted by European Commission in Brussels, 4.6.2012 COM(2012) 238 final, 2012/0146 (COD), s. 4.

9 Viz *op. cit.*, s. 3.

10 Podobně neuspokojivá situace koncepčního zvládání technologií elektronického podpisu úřady ale panuje i na národní úrovni v ČR. Po mnoha organizačních změnách došlo cca v roce 2011 k úplnému zrušení oddělení elektronického podpisu na Ministerstvu vnitra a tím potažmo ke ztrátě institucionální paměti o této problematice na úrovni orgánů ústřední státní správy.

11 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on an Action Plan on esignatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM(2008)798, Brussels: November 2008.

Pro praktické přiblížení pojmů, elektronickou identifikací lze rozumět jednorázovou autentizaci osoby spojenou s prokázáním totožnosti osoby (uživatele) na počátku počítačového sezení nebo před provedením důležité operace. Autentizací a potažmo identifikací (byť nepříliš silnou) je například zadání přihlašovacího jména a hesla k poštovnímu účtu na službě *gmail.com*, nebo do datové schránky v ČR. Identifikace je důležitá až nutná služba, pokud chcete některé informace poskytovat pouze některým osobám. Například funkce vzdáleného přístupu do spisu v jakémkoli veřejnoprávním řízení bude vyžadovat, aby nahlížející osoba byla bezprostředně předtím identifikována. Autentizace a identifikace jsou však málo dostatečné, má-li být prokázán obsah právního jednání osoby. Lze je přirovnat k situaci, kdy je na vrátnici či recepci podniku ověřována totožnost fyzické osoby např. vůči občanskému průkazu. Z průběhu takového postupu a záznamu o něm např. v návštěvní knize lze soudit, že se daná fyzická osoba na recepci podniku vyskytla a do podniku poté vstoupila, bez dalšího však již nikoli to, o čem a jak v podniku jednala nebo se chovala. Stejná potíž panuje i v případě počítačového systému. Důkaz o následném jednání sice je v principu možný, ale velmi složitý a situace pro vedení takového důkazu musí být připravena již předem, než k nasazení počítačového systému vůbec dojde. Jiným příkladem autentizace a identifikace z běžného světa by mohlo být vzájemné představení se dvou osob, spojené například s výměnou vizitek, ale někdy i za pomoci společně známého prostředníka, který strany stručně uvede. Strany komunikace se tak na jejím počátku v jisté míře spolehlivosti ujistí o tom, kým protějšek je. Obsah jednání si však musí především každá strana zvlášť pamatovat.[12]

Pro důkaz o obsahu jednání slouží právě elektronický podpis, jehož hlavní funkcí je prokázání původce podepsaných dat, přičemž se předpokládá, že podepsaná data mohou obsahovat a vyjadřovat právní jednání. I u elektronického podpisu se někdy hovoří o autentizaci a identifikaci, ty však neprobíhají mezi dvěma v budoucnu jednajícími entitami, ale vedou se ve vztahu k podepsaným datům, jimiž rozumím i případy podepsaného dokumentu nebo podepsané datové zprávy. Ověřit tento vztah by měla být v principu schopna jakákoli jiná osoba, tedy nejen například adresát projevu, ale i někdo jiný, z čehož pro právo nejdůležitější třetí osobou je potenciální soudce, který má někdy později rozhodnout případný spor mezi původcem a adresátem. Tím se tento mechanismus značně liší od výše zmíněné elektronické identifikace, v níž ujištění o identitě probíhá pouze mezi komunikujícími stranami samými. Je bohužel pravda, že zejména v případě slabších metod může být uvedený metodický rozdíl setřen. Kupř. zadání PIN[13] je jistě autentizací a proto spíše elektronickou identifikací, ale někdy bývá považováno i za tzv. prostý elektronický podpis. V terminologii eIDAS jsou stanoveny jako dva hlavní a vzájemně exkluzivní pojmy elektronická identifikace a elektronický podpis. Pojem autentizace pak je v eIDAS zaveden jako související nebo nadřazený oběma uvedeným, tj. částečně odlišně od způsobu, jak je v počítačové praxi běžně používán a spíše blíže k významu slova *pravost* či obratu *zajištění pravosti*.

Studie vypracovávané pro Komisi (např. zmíněná CROBIES) dále upozorňovaly, že není jasné, proč služby poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty, jsou v rámci EU regulovány poměrně přísně, zatímco jiné služby obdobné důležitosti nikoli (např. ani vydávání časových razítek). Mělo se jednat i o služby zaručeného doručování (tj. obdoby tuzemských datových schránek), nebo o služby dlouhodobé úschovy a archivace elektronických dokumentů.

V průběhu vývoje nasazování elektronických podpisů se dále zjistilo, na úrovni unijní i v ČR, že služby spojené pouze s vydáváním kvalifikovaných certifikátů nejsou dostatečné, že je nutné tyto služby doplnit o služby tzv. časových razítek.[14] V ČR byl kupř. jednou z novel ZoEP zaveden institut kvalifikovaného časového razítka. Zhruba od roku 2003 se pro souhrn různých poskytovatelů (vydávajících certifikáty, vydávajících časová razítka, popř. v zahraničí vydávajících i zařízení pro bezpečné vytváření elektronického podpisu – zpravidla ve formě čipových karet) začal v evropské literatuře používat společný pojem Trust Service Provider (TSP), čehož přesným překladem by bylo poskytovatel důvěrových služeb, nicméně často se dosud používal i překlad poskytovatel důvěryhodných služeb (po eIDAS se bude používat poskytovatel služeb vytvářejících důvěru), nebo poskytovatel důvěry. Jejich služby jsou označovány jako Trust service, což bylo až dosud překládáno jako důvěryhodné služby, nicméně v době po nařízení eIDAS lze očekávat, že se ujme překladateli nařízení zvolený obrat služby vytvářející důvěru, který se dostal i do samotného názvu nařízení. Jeden TSP může poskyto-

[12] Pokud k zachycení obsahu právního jednání nepoužijí jiné prostředky, které však již nejsou samotnou identifikací.
[13] PIN – Personal Identification Number (osobní identifikační číslo).
[14] Např. v německém právu měl o této potřebě zákonodárce jasno od samého počátku.

vat jeden nebo více druhů takových služeb. Zvolený překlad v eIDAS je docela vhodný, jelikož služba TSP sice musí být důvěryhodná, ale jejím pravým smyslem je především poskytovat důvěru v něco dalšího. Oním dalším může být totožnost osoby (informace o ní) v případě kvalifikovaného certifikátu, čas (informace o čase) v kvalifikovaném časovém razítku, informace o použití bezpečného prostředku pro vytváření podpisu apod. Zhruba od roku 2006 se ve vyspělých zemích EU ve spojitosti s elektronickým podpisem uvažuje i o archivačních či úschovních službách, které by umožnily dlouhodobě uchovávat platnost elektronických podpisů, a zhruba od roku 2008 dále se začínají považovat za důležité i služby zaručeného doručení.[15] Zájemce o historický výklad lze upozornit, že ideová východiska a mentální stav autorů návrhu nařízení jsou zřejmě nejúplněji a nejaktuálněji shrnuty ve studii označované jako *IAS*.[16]

Stručně lze obsah eIDAS shrnout tak, že se nařízení snaží spojit v jednom právním předpisu (1) úplně novou základní úpravu pro elektronickou identifikaci a (2) významnou novelizaci úpravy elektronického podpisu, přičemž v druhé oblasti se nově předpokládá mnohem větší význam pro využití služeb vytvářejících důvěru, které nově zahrnují i služby elektronického doporučeného doručování. K těmto tématikám byly navíc poněkud neústrojně přidány i služby vytváření, ověřování shody a platnosti certifikátů pro autentizaci internetových stránek.[17]

Novinky: Elektronická identifikace

V oblasti elektronické identifikace se v eIDAS projevily dva faktory. Prvním je, že pozdní harmonizace evropským právem zde způsobila, že mnohé členské státy již přijaly zvláštní právní úpravy a technicky implementovaly svá vlastní a navzájem zatím neslučitelná řešení, přičemž do nich již investovaly značné prostředky. Druhý zjištěný faktor je, že členské státy nemají příliš zájem na tom podřizovat své systémy identifikace státům jiným, ani Evropské unii. Výsledkem v eIDAS proto je metodika oznamování (notifikací) tzv. systémů elektronické identifikace. Každý stát tedy může dále vytvářet vlastní identifikační systémy, pro něž buď vydává tzv. prostředky pro elektronickou identifikaci, nebo tyto prostředky uznává. Pro účel jejich využití osobami nebo úřady z jiných členských států je ale povinen zajistit možnost on-line ověření identifikačních údajů na dálku. Členský stát přitom odpovídá za škodu, kterou způsobí, pokud by tuto autentizační službu řádně neprovozoval, nebo pokud by obsažené identifikační údaje nebyly řádně spojeny s identifikovanou osobou.

Nařízení eIDAS přitom zavádí tři kategorie úrovně záruk systémů elektronické identifikace: nízká, značná a vysoká. Metodika vzájemného uznávání elektronické identifikace mezi členskými státy je na tyto úrovně navázána.

K potřebné technické harmonizaci elektronické identifikace má dále dojít splňováním technických specifikací, k jejichž zveřejnění je Komise zmocněna formou prováděcích aktů. Zda se technická harmonizace zdaří, bude proto značně záležet především na kvalitě budoucích technických specifikací a na ochotě a schopnosti úřadů členských států je splňovat. Představíme-li si, že každý členský stát EU bude používat byť i jen několik „svých" systémů elektronické identifikace, každý v celé škále úrovní záruk, může počet notifikovaných systémů elektronické identifikace brzy snadno vyšplhat na několik set. Podpora tak mnoha systémů současně se může stát noční můrou poskytovatelů elektronických služeb. Jakákoli možnost pan-EU úspěchu bude proto podmíněna výše zmíněnými technickými specifikacemi či technickými normami, aby byly navrženy tak, že umožní vzájemnou technickou interoperabilitu dosud neinteroperabilních identifikačních systémů. Nezdaří-li se tento úkol, bude identifikační budoucnost EU pochmurná. Komise sice podporuje některé projekty IT s elektronickou identifikací, zejména projekt STORK[18] resp. STORK 2.0,[19] bez podpory a zahrnutí identifikačních systémů členských států však nebudou mít spíše pouze unijní projekty šanci na úspěch. Nadpoloviční část členských států se sice pilot-

[15] Zatímco v ČR se v této oblasti nasadily datové schránky České pošty s. p., v Německu se jedná o otevřenější systém DeMail, a na úrovni Evropské unie se zpracovával projekt REM – Registered Email, rovněž koncipovaný jako otevřený.

[16] DLA Piper, Sealed, Time.lex, PriceWaterhouseCoopers, SGA: *Feasibility study on an electronic identification, authentication and signature policy (IAS), Final Report*, A study prepared for the European Commission DG Communications Networks, Content & Technology, Ref. Ares(2013)2869715 – 13/08/2013, Brusel: 2013.

[17] Zde se naopak jedná o překlad ne zcela vhodný (v eIDAS anglicky *website certificate*). V technické praxi se běžně nazývá *serverový certifikát*. Bývá od TSP poskytován jako vedlejší služba a typicky slouží pro autentizaci a identifikaci webového serveru jako samočinně běžící technické entity, spravované určitou osobou, jejíž totožnost je v certifikátu uvedena, na počátku webového sezení nějakého uživatele (typicky fyzické osoby). Nevhodnost překladu *certifikát pro autentizaci internetových stránek* plyne z toho, že takový certifikát se vydává na jeden webový server, na jeden website, tj. pouze jeden. Certifikát pak autentizuje webový server a nikoli jednotlivé internetové stránky. Je zcela na zařízení serveru, jaké internetové (webové) stránky bude uživatelům představovat.

[18] Secure idenTity acrOss boRders linKed. Jedná se o pilotní projekt velkého rozsahu, na němž se podílelo 14 až 17 (na závěr) členských států EU a EHS a byl kofinancován Evropskou komisí. Probíhal v letech 2008–2011. https://www.eid-stork.eu.

[19] Navazující projekt. Účastní se jej více členských států, nově včetně ČR, nikoli však již Německo. Spoluúčastníky projektu jsou i soukromoprávní subjekty. Probíhá od roku 2012. https://www.eid-stork2.eu.

ních projektů STORK zúčastnila nebo účastní, míra jejich angažmá je však zatím nejasná.

Novinky: Elektronický podpis

Oproti elektronické identifikaci mohla oblast úpravy elektronického podpisu v eIDAS těžit ze zkušeností, které členské státy i EU nasbíraly s elektronickým podpisem v rámci harmonizace podle směrnice 1999/93/ES. I když jsou implementace v členských státech navzájem technicky i právně zatím nekompatibilní, směrnici se přeci jen podařilo založit jednu společnou architekturu či přístup k elektronickým podpisům ve všech členských státech, která spočívá na tzv. infrastruktuře veřejného klíče (Public Key Infrastructure, PKI), na činnosti poskytovatelů certifikačních služeb a jimi vydávaných kvalifikovaných certifikátů. V právních řádech členských států existuje i podobná terminologie. Tyto faktory zásadně usnadnily budování společného řešení elektronického podpisu. Praktický rozdíl se projevuje v tom, že v oblasti elektronického podpisu základem technického řešení budou technické specifikace a technické normy vyhlášené prováděcími akty Komise, k jejichž vydání je Komise v eIDAS rovněž zmocněna. Na přípravě těchto technických specifikací se již několik let pracuje v rámci tzv. Mandátu 460.[20] Tyto mandáty jsou způsobem, kterým Komise zmocňuje a potažmo i financuje vytváření technických specifikací či norem v rámci evropských normalizačních institucí, jako jsou např. CEN[21] nebo CENELEC,[22] a v rámci elektronického podpisu zejména aktivní ETSI.[23] Oproti elektronické identifikaci lze v oblasti elektronického podpisu proto zcela realisticky doufat, že vzniknou společné technické normy na úrovni celé EU, podle nichž budou navrhovány všechny produkty a služby, takže technická kompatibilita a interoperabilita by měla být dosažitelná. Význam tohoto technického sjednocení nelze nedocenit. Zatímco na základě směrnice 1999/93/ES vyhlásila Komise pouhé tři technické specifikace, nyní již považované za zastaralé, podle Mandátu 460 se připravuje více než 50 technických specifikací, které víceméně jsou skutečně potřebné a mnoho z nich zcela nutných. Právě tato disproporce počtu potřebných technických specifikací velmi názorně představuje, proč nebylo dosud dosaženo interoperability elektronického podpisu na úrovni EU.

Na druhé straně je možné hodnotit eIDAS z pohledu právní kvality navržené úpravy, čemuž budou věnovány následující řádky.

Soukromý klíč uložený v cloudu

Autoři návrhu nařízení se rozhodli, že chtějí podporovat možnost uložení tzv. dat pro vytváření elektronického podpisu (v praxi PKI se označují jako soukromý klíč) v cloudově provozovaných kryptografických zařízeních, ev. i včetně možnosti delegace vlastního vytvoření elektronického podpisu na poskytovatele takových služeb pro vytváření důvěry. Toto řešení má své výhody z hlediska správy, nasazování, udržování, zajišťování provozu a v některých ohledech i z hlediska bezpečnosti. Má ovšem dvě nevýhody. První je závislost na konektivitě. Bez funkční konektivity k poskytovateli se podepisující osoba nepodepíše. Druhá nevýhoda je zásadní – uživatel ztrácí fyzickou kontrolu nad svým soukromým klíčem. Fyzické držení je přitom jedním ze zásadních faktorů tzv. fyzické bezpečnosti, která je vždy důležitou součástí počítačové bezpečnosti jako takové. Kromě zmínění této možnosti v bodech odůvodnění této změně koncepce nasvědčuje i nová podmínka tzv. „výhradní kontroly." Zatímco dle směrnice 1999/93/ES se pro tzv. zaručený elektronický podpis požadovalo vytvoření podpisu pomocí „využití prostředků, které podepisující osoba může mít plně pod svou kontrolou", v čl. 26 eIDAS nově zní: „je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou." Znění eIDAS, kromě toho, že je nejasné (srov. informaci z červnového workshopu v Bruselu níže), představuje podmínku znatelně užší. Podmínka DirES se vztahovala na všechny technické prostředky, které se na vytváření podpisu zúčastnily. V technické praxi proto nikoli pouze na soukromý klíč, ale i na jeho technický kontejner, typicky čipovou kartu, a dále i na všechen jiný hardware a software, který se na vytváření podpisu podílel, tj. zejména i na aplikaci vytvářející elektronický podpis a potažmo i některé periferie, jako např. bezpečná čtečka čipových karet. Vztahovat by se rovněž měla na operační systém, nebo aspoň na jeho funkce, kterými zajišťuje tzv. bezpečné cesty a bezpečné kanály mezi periferiemi lidského rozhraní, aplikací vytvářející podpis a čipovou kartou. Podmínka

[20] GENERAL: *M/460 EN Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies applied to Electronic Signature*, Brussels, 22–nd December 2009. http://www.etsi.org/images/files/ECMandates/m460.pdf.

[21] Comité Européen de Normalisation (Evropský výbor pro normalizaci).

[22] Comité Européen de Normalisation Electrotechnique (Evropská komise pro standardizaci v elektrotechnice).

[23] European Telecommunications Standards Institute.

v eIDAS se vztahuje pouze na výhradní kontrolu nad použitím soukromého klíče, navíc změkčenou z plné kontroly na kontrolu s vysokou úrovní důvěry.[24]

Vynechání WIPIWIS

Akronym WIPIWIS má význam *What Is Presented Is What Is Signed*, nebo-li podepsáno je to, co je předloženo (zobrazeno). Z hlediska podpisu se jedná o poměrně stěžejní zásadu, neboť vznáší požadavek na celkové technické uspořádání tak, aby si podepisující osoba mohla být jista, že podepisuje to, co skutečně vidí (popř. jinak vnímá svými smysly, elektronicky podepsat lze třeba i zvukový záznam). V případě klasického vlastnoručního podpisu na běžný papír je tato podmínka tak samozřejmá, že ji vlastně jednak ani nikdo nevznáší, ani si ji běžně neuvědomuje. V technické praxi však je důležitá, neboť funkce zobrazení i vytvoření podpisu jsou technicky oddělené a prováděné různými zařízeními nebo jejich částmi. Autoři návrhu nařízení si zásady buď nebyli vůbec vědomi, nebo ji z nepochopitelných důvodů vynechali. Platí přitom, že zásada ani v ideovém východisku, kterým bezpochyby byla směrnice 1999/93/ES (DirES), nebyla dosud explicitně vyjádřena. Lze ji ale dovodit jako realizovatelnou např. z požadavku na výhradní kontrolu zařízení, která v DirES byla, v eIDAS již ale není. Pro zajímavost, obdobně WIPIWIS není explicitně vyjádřena ani v současném českém ZoEP, ovšem i zde dosud byla podmínka výhradní kontroly veškerého zařízení. Podmínka je ovšem explicitnější součástí např. německého právního řádu, který stanoví určité podmínky i na aplikace vytvářející elektronický podpis.

Zrušení omezení použití certifikátu

Dosavadní DirES umožňovala, aby součástí obsahu kvalifikovaného certifikátu bylo omezení jeho použití. Takové omezení v principu umožňovalo ochranu podepisující osoby – pokud by byl kvalifikovaný certifikát použit pro právní jednání, které odporovalo omezení vyjádřenému v certifikátu, bylo možné jej považovat za jednání neplatné. V ČR sice žádný ze tří akreditovaných poskytovatelů certifikačních služeb tuto možnost neumožňuje a potažmo se v ČR nepoužívá,[25] v Německu však byla poskytovateli umožněná a je i využívaná. Kupř. němečtí advokáti používají kvalifikované certifikáty s uvedením omezení na transakce do 100 EUR, přičemž německé soudy judikovaly, že takovéto certifikáty jsou plně použitelné pro procesní úkony u soudů, které advokáti provádějí jménem svých klientů, protože se nejedná o přímé finanční transakce.[26] Autory německé doktríny pak možnost uvést omezení byla považována za důležitý právní nástroj, jak řídit riziko použití elektronického podpisu u podepisující osoby,[27] která může své technické a organizační prostředí podepisování přizpůsobit hodnotě a rizikům sebou prováděných transakcí. Zjednodušeně řečeno, je-li hodnota transakcí nízká, lze použít prostředky a postupy s malou nebo nízkou bezpečností a spoléhat se na právní omezení v kvalifikovaném certifikátu, který je vždy vysoce bezpečný, je-li vysoká, bude tomu odpovídat i volba prostředků a náklady na ně. Takové uspořádání je poměrně racionální, neboť je to právě podepisující osoba, která jednak zná hodnotu svých transakcí nebo výši rizik, jednak současně nese i náklady na pořízení prostředků a provádění postupů. Snahy stanovit jednotnou úroveň bezpečnosti zařízení pro elektronický podpis buď vedou na nízké náklady, kdy se ale mnohé podepisující osoby budou zdráhat je používat vůbec, nebo na vysokou bezpečnost, která ale bude pro mnohé podepisující osoby nepřiměřeně drahá, takže je opět nebudou používat. Dobrým řešením není ani jednotná střední cesta úrovně bezpečnosti. Citovaným německým právníkům proto omezení v certifikátu přichází jako ideální způsob úpravy na míru potřeb jednotlivým osobám, jakkoli se současně připouštělo, že právně takové sebeomezení nemá zatím zcela jasnou povahu. Jinou námitkou proti přípustnosti omezení v certifikátu je, že velmi často vyžaduje v zásadě manuální kontrolu významu omezení vůči podepsanému textu. Proto je toto omezení poměrně neoblíbené i u techniků a programátorů, kterým neumožňuje plně automatizovat proces ověření platnosti elektronického podpisu, ale může vyžadovat lidskou intervenci obsluhy. Buď jak buď, možnost uvádět omezení v kvalifikovaném certifikátu pro elektronický podpis byla v eIDAS vypuštěna.

Chybějící povinnosti podepisující i spoléhající osoby

Celé eIDAS je zformulováno způsobem, jako by se autoři textu obávali stanovit jakékoli povin-

[24] Český překlad eIDAS zde není šťastný, anglické slovo *confidence* zde mělo být přeloženo spíše jako přesvědčení a nikoli jako důvěra.

[25] O vyjádření takového omezení se osobně snažívám náhradně stanovením zvláštních organizačních útvarů organizace.

[26] BFH, 18. 10. 2006 – XI R 22/06, http://lexetius.com/2006,3265, R. 35.

[27] FISCHER-DIESKAU, S. / HORNUNG, G.: *Die Beschränkung des qualifizierten Zertifikats § 7 Abs. 1 Nr. 7 SigG als wichtiges Mittel der Risikokalkulation*, Multimedia und Recht (MMR), 6. Jg. (2007), Heft 6, C.H.Beck: 2003, s. 384–389.

nosti pro subjekty podepisující osoby a spoléhající osoby, snad z důvodů, aby je neodradili od používání elektronického podpisu. Bohužel tyto povinnosti nelze jednoznačně odvodit ani z případných práv těchto subjektů jako komplementární. V eIDAS tak kupř. chybí i jakákoli povinnost podepisující osoby chránit svá data (soukromý klíč) a prostředky pro vytváření podpisu, jak je vyjádřena třeba v § 5 ZoEP. Chybí-li vyjádření takové povinnosti, nemůže ale spoléhající osoba s právní jistotou spoléhat, že podepisující osoba skutečně svá data a prostředky pro vytváření podpisu dostatečně chrání, což následně značně oslabuje důvěryhodnost přijatého elektronického podpisu, neboť není dostatečně právně zajištěno, že elektronický podpis skutečně vytvořila osoba, která je uvedena v souvisejícím kvalifikovaném certifikátu. Protože lehkomyslným jednání neporuší žádnou právní povinnost, není možné plnění vyžadovat ani náhradně formou náhrady škody.

Stanovení rovnocennosti elektronického podpisu s vlastnoručním

V eIDAS se v článku 25 odst. 2 stanoví: „Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu."[28] Na jednu stranu se zdá, že rovnocennost či ekvivalence je žádoucí grál, který kvalifikovaný elektronický podpis (jedna z náročnějších variant elektronických podpisů, v nařízení upravená) jako právní institut potřebuje v právní rovině dosáhnout, na straně druhé toto ustanovení bude zřejmě i přes svou zdánlivou jednoznačnost vytvářet interpretační potíže. Z textu se zdá, že se nejedná o právní domněnku, ať již vyvratitelnou či spíše nevyvratitelnou. Nepovažuji ho ani za právní fikci, dle níž by např. elektronický podpis nahrazoval vlastnoruční, i když zejména anglické znění by tuto možnost částečně připouštělo. Spíše jej považuji za právní pravidlo stanovící rovnocenné právní účinky, přičemž normálem těchto právních účinků je vlastnoruční podpis. Je tedy nutné si klást otázku, jaký právní účinek vlastnoručního podpisu vlastně je. První potíží bude, že v různých členských státech bude právní účinek nepochybně různý. Proto bude vždy nejprve třeba zkoumat otázku rozhodného práva. Dalším problémem je, že sám o sobě stojící vlastnoruční podpis nemá běžně právní účinek žádný, ale získává ho až ve spojení s kontextem, ve kterém se vyskytuje, v prostředí právního řádu ČR typicky ve spojení s písemností, která slovně nebo znaky vyjadřuje obsah právního jednání. Lze úspěšně pochybovat, že by uvedené ustanovení eIDAS například umožňovalo vydávání směnek v elektronické podobě. Snadné kopírování elektronických dat znemožňuje inkorporaci a vznik cenného papíru v nezaknihované podobě, jakým je směnka. Máme zde tedy nejméně jeden případ, kdy použití kvalifikovaného elektronického podpisu (Qualified Electronic Signature, QES) ve vztahu k jinak shodné písemnosti naprosto nemůže založit stejný právní účinek, jako by měl podpis vlastnoruční. Obdobně tomu bude ve všech případech, kdy některé právo stanoví pro nějaké právní jednání určitou formu provedení.

Další podstatnou komplikací je, že zatímco vlastnoruční podpis prakticky nelze nevědomky připojit k písemnosti, kterou osoba o své vlastní vůli nevidí, u elektronického podpisu, včetně kvalifikovaného elektronického podpisu dle eIDAS, tomu tak být může, neboť zásada WIPIWIS byla opuštěna. Vynechání povinností podepisujícího v eIDAS pak způsobuje druhou, právně mnohem snazší, možnost popření vytvoření podpisu uvedenou podepisující osobou. V obou těchto ohledech QES vůbec není rovnocenný vlastnoručnímu podpisu a je těžké dovozovat, že by i přesto měl mít shodné právní účinky, jakkoli tak právní předpis na první pohled stanoví.

Z hlediska právních účinků lze u vlastnoručního podpisu vysledovat dva okruhy, které se pravidelně vyskytují. Prvním je splnění požadavků na písemnou formu právního jednání. Přítomnost podpisu bývá v právních řádech některých členských států, včetně ČR, nutnou náležitostí písemné formy. Druhý druh účinků bývá důkazní účinek. Pravost vlastnoručního podpisu, ověřitelná potenciálně znalecky, bývá často prostředkem ověření pravosti celé podepsané listiny. Soudím, že rovnocennost právních účinků podle eIDAS bude snad možné připustit pro splnění náležitostí formy, důkazní účinek však rovnocenný za současného znění eIDAS rozhodně není.

Německý profesor A. Roßnagel, který je hlavní autoritou německé nauky elektronického podpisu, na návrh eIDAS vytvořený Komisí v roce 2012, poté co se stal vstupním dokumentem legislativního procesu v EU, reagoval značnou kritikou,[29] která zřejmě právě k ustanovením jako je zde zmíněné obsahovala: „[Návrh] zavádí důkazní domněnky bez toho, aby domněnkám stanovil dostatečné základy."[30] Jakkoli došlo

[28] V anglickém znění, z něhož bylo překládáno do češtiny: *„A qualified electronic signature shall have the equivalent legal effect of a handwritten signature."*

[29] ROSSNAGEL, A.: *Rechtsetzung zu Sicherheitsdiensten: Europäisierung ja, Monopolisierung nein!*, Multimedia und Recht, 15. Jg. (2012), C. H. Beck: 2012, s. 781–782.

[30] Doslovně: *„Er führt Beweisvermutungen ein, ohne hierfür ausreichende Vermutungsgrundlagen festzulegen."*

v průběhu dvouletého legislativního procesu Evropské unie k neuvěřitelnému množství změn textace, nedošlo až na výjimky k podstatným změnám smyslu. Zhruba lze říci, že legislativní záměr Komise, který byl obsažen v textu původního návrhu, je obsažen i ve výsledném textu eIDAS až na to, že je kvalitněji formulován co do právního jazyka. Lepší výsledná forma zde bohužel nemůže zachránit chybějící nebo chybný věcný obsah.

Requiem za českou elektronickou značku

Nařízení zavádí dva exkluzivní pojmy: elektronický podpis, jehož znakem je, že je vytvářen fyzickou osobou, a nově elektronickou pečeť, jejímž znakem je, že přináleží přímo právnické osobě a její vytvoření je připsáno právnické osobě samé. Pojetí právnické osoby má být podle práva EU přitom značně široké, aby zahrnovalo co nejširší množství subjektů.

Tato systematika není bezesporná a zejména ne dostačující. V počítačové praxi se vyskytuje potřeba něčeho, co technicky má shodný výsledný formát jako elektronický podpis, ale vzniká bez přímé kontroly fyzické osoby, ať již v certifikátu je tato osoba uvedena, nebo je v něm uveden například subjekt jejího zaměstnavatele. Jednou z novel se do českého ZoEP pro tento účel zavedla elektronická značka. I když její právní vymezení není zcela příkladné, poskytovala samostatný název a především odlišení od případů elektronického podpisu. Tím se následně v jiných právních předpisech umožňovalo odlišit případy a požadavky, kdy dostačuje elektronická značka a kdy musí být přítomen elektronický podpis.

Nařízení pro účel „elektronických podpisů" vytvářených automaty, ať již iniciovanými pro jednání za fyzickou nebo právnickou osobu, žádný zvláštní právní institut nemá, jakkoli je zřejmé, že se jedná o kvalitativně přeci jen odlišný průběh vytvoření, který by měl být patrný i na výsledku a na právním vymezení následků, nebo předpokladů pro jejich výskyt. Pro vytváření doručenek došlých zpráv na elektronické podatelně pravděpodobně dostačuje elektronická značka z ČR, pro podpis správního rozhodnutí by měl být přítomen elektronický podpis.

Bruselský workshop a budoucí prováděcí akty

V červnu se v bruselském sídle Evropské Komise na Place Madou konal workshop[31] zainteresovaných stran (tzv. *stakeholders*) ohledně přijímání nařízení eIDAS. Legislativní proces přitom již tehdy byl ve svém samém závěru a obsah textu nařízení nebylo možné změnit. Smyslem workshopu proto byla vzájemná komunikace pro účel vytváření prováděcích aktů, k jejichž vydávání je Komise nařízením zmocněna.

Vystupujícími na workshopu byly osoby konsorcia kontrahovaného Komisí pro tvorbu studie IAS2,[32] která navazuje na výše zmíněnou studii IAS a slouží pro podporu implementace nařízení Komisí. Shromážděnými účastníky byly osoby ze všech členských států, které se problematikou zabývají a měly zájem se účastnit. Zahrnují například úředníky státní správy, regulačních subjektů, zaměstnance poskytovatelů certifikačních služeb, ale i osoby z univerzit, soukromých praxí nebo jiné profesionály.

Studie je rozdělena do několika expertních skupin, z nichž nejpočetnější je právní (6 členů), dále pak technicko-normativní, ekonomická a komunikační. Jedná se nyní o prakticky jedinou právní platformu, v jejímž rámci Komise částečně komunikuje s odbornou veřejností o eIDAS. Ohlášeným účelem workshopu dle pozvánky měl být sběr potřeb a diskuse o nich, jako zpětná vazba od zainteresovaných stran vůči Komisi pro účely tvorby prováděcích aktů. Směrování informací na workshopu bylo spíše opačné, neboť po úvodu Andrea Servidy, pracovníka Komise v roli vedoucího legislativní skupiny pro eIDAS,[33] následovala až do večera série prezentací členů konsorcia. Ty jsou nalezitelné na webových stránkách studie[34] a seznamovaly s postupem prací probíhajících na pozadí. Dotazy či podněty z pléna byly spíše příležitostné než systematické. Charakter diskuse měl závěrečný půlhodinový panel. Podněty zpracovatelům studie a potažmo i Komisi je pochopitelně možné zasílat i nyní, a to i když jste se workshopu nezúčastnili.

Vysloveně právním informacím byla věnována polovina odpoledne. Zajímavým zjištěním jistě je, že v průběhu legislativního procesu byla z návrhu vypuštěna prakticky všechna zmocnění pro vydávání aktů v přenesené pravomoci (*delegated acts*) a zbyly pouze prováděcí akty (*implementing acts*). Přinejmenším v oblasti působnosti eIDAS členské státy neměly zájem ten-

[31] Stakeholders Workshop on electronic identification and trust services, 18–th June 2014, Brussels. Autor se workshopu účastnil v rámci řešení projektu SVV č. 260 005.
[32] Viz http://blogs.dlapiper.com/iasproject/.
[33] Head of Task Force „Legislation Team (eIDAS)"; podle dalších informací z LinkedIn je A. Servida jaderný inženýr s postgraduálním studiem v oboru umělé inteligence, který se zabývá otázkami síťové a počítačové bezpečnosti; prakticky byl zastřešující osobou za Komisi, která zabezpečovala průchod nařízení Evropským parlamentem i Radou.
[34] Viz http//www.iasproject.eu, konkrétní workshop je na adrese:http://blogs.dlapiper.com/iasproject/workshops/workshop-2-agenda-and-slides.

to nový polisabonský institut evropského práva využít.

R. Genghini[35] se dotkl dvou témat. Prvním byla otázka, zda služby vytvářející důvěru[36] (Trust Services) a kvalifikované služby vytvářející důvěru (Qualified Trust Services), uvedené v nařízení, představují taxativní, anebo jen demonstrativní seznam. Snesl důvody pro obě argumentace s tím, že za optimální kompromis a výklad považuje dobrovolný *opt-in* těch poskytovatelů, jejichž předmět činnosti neodpovídá činnostem uvedeným v eIDAS, ale mají zájem o zařazení do regulovaného režimu např. z důvodu možnosti uvádět pak pro svou činnost značku důvěry EU[37] a tím lépe konkurovat např. velkým společnostem. Tento náhled považuji za poměrně překvapivý, neboť dosud jsem měl za to, že výčet služeb vytvářejících důvěru v eIDAS je taxativní. Jak uváděl i Genghini, umožňuje to, aby na trhu ICT mohly volně vznikat zcela nové služby bez potřeby potenciálně se podřizovat regulaci obsažené v eIDAS. V druhém tématu elektronického doporučeného doručování je dle Genghiniho třeba prozkoumat nejen zřejmého kandidáta REM,[38] ale veškeré reálně existující nebo normalizačními organizacemi navrhované služby, jako jsou mnohé systémy OASIS,[39] ale i SWIFT,[40] UPU EPM[41] nebo e-Sens.[42] Obecně pak doporučuje, aby oblast zůstala otevřená technickým inovacím.

Značnou část zpětné vazby účastníků zastal D. Pinkas[43] z Francie, který vystupoval vůči mnoha částem nařízení velmi kriticky a na akci distribuoval i trojici svých krátkých opozičních článků. Dle něj například nařízení nezajišťuje při identifikaci ochranu soukromí již návrhem (*privacy by design*), ačkoli tak je v čl. 12 odst. 3 nařízení určeno, ale jedná se o sledování již návrhem (*spy by design*). Důvěryhodné seznamy dle Pinkase vůbec nemusí být aktuální a to klidně v rozmezí několika týdnů. Vadná je dle něj i úprava elektronických podpisů. Některé jeho námitky sdílím, byť mé hodnocení může být odlišné, některé považuji za právníkem snadno překlenutelné. D. Pinkas například prostým jazykovým výkladem dospívá k tomu, že certifikát nebude moci obsahovat ani omezení *keyUsage* jako technický parametr certifikátu dle X.509.[44] Dle mého názoru si zde lze právně vypomoci a parametr připustit, neboť se jím určuje, že se jedná o certifikát pro elektronický podpis. Použití parametru zde tedy plyne z označení certifikát pro elektronický podpis, určující i účel použití certifikátu.

V panelové diskusi jsem v rámci zjišťování informací pro případný historický výklad vznesl dotaz, zda někdo v auditoriu zná důvod změny definice zaručeného elektronického podpisu doplněním obratu „s vysokou úrovní důvěry" (anglicky *with a high level of confidence*) ohledně použití pod výhradní kontrolou podepisujícího. Panelisté odvětili, že obrat vznikl v Komisi a otázku může zodpovědět pouze ona. Několik minut po mně dotaz zopakoval anglický advokát S. Mason s tím, že i on je frází zcela zmaten, neboť není jasné o čí přesvědčení (*confidence*)[45] se má jednat, zda o přesvědčení podepisujícího nebo orgánu dohledu, zda přesvědčení má být subjektivní, nebo objektivní etc. G. Galler, další přítomný pracovník Komise, který se pravděpodobně na formování textu eIDAS podílel i osobně, poté odpověděl, že prostě chtěli odstranit rezolutnost znění dřívější směrnice, která podmínku výhradní kontroly stanovila dle jeho názoru příliš striktně. Rozuměl-li jsem jeho vyjádření správně, pak z jeho pohledu počítačového inženýra nelze u žádné implementace zaručit stoprocentní jistotu o funkci, neboť nelze předem vyloučit možnost budoucích projevů chyb nebo vyjevení slabin, např. i v rámci metod útoků, které v současnosti nejsou ani známé. Přesto takovou implementaci v zásadě již nelze dále zlepšovat a elektronické podpisy pomocí ní vytvořené je potřeba považovat za platné a vyhovující definici, pročež byla definice preventivně zmírněna. Jednalo by se tedy o přesvědčení odborné osoby, objektivizované srovnáním se stavem vědy a techniky. Toto pojetí „vysoké míry přesvědčení" by mi přišlo ještě přijatelné. Zda se tak výklad ustálí, ovšem nevím a dle mého názoru obrat neměl být vůbec přidáván.

V závěru panelu z pléna vystoupila čerstvá ex-poslankyně Evropského parlamentu A. Andersdotter,[46] která prohlásila, že je-li nařízení

[35] R. Genghini je italský právník, ředitel skupiny ETSI ESI v letech 1999-2009 v ETSI.

[36] Doslovný český překlad pro „*trust services*" by byl „důvěrové služby". Během legislativního procesu kolísal od „důvěryhodných služeb" (což není přesné) až po výsledné „služby vytvářející důvěru".

[37] Jedná se o novou grafickou značku (EU trustmark), určenou pro označení kvalifikovaných poskytovatelů služeb vytvářejících důvěru.

[38] ETSI TS102 640 Registered Electronic Mail v2.1.1.

[39] OASIS je standardizační konsorcium činné v oblasti ebXML.

[40] Society for Worldwide Interbank Financial Telecommunication – Společnost pro celosvětovou mezibankovní finanční telekomunikaci.

[41] Projekt Universal Postal Union zvaný Electronic PostMark.

[42] E-Sens je projekt EU, viz. http://www.esens.eu.

[43] D. Pinkas byl členem skupiny *European Electronic Signature Standardization Initiative*, existující v letech 1999–2004, vzniklé na žádost Evropské komise v rámci normalizačních organizací CEN, CENELEC a ETSI.

[44] ITU-T Recommendation X.509: Information technology - Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

[45] *Důvěra* pro *confidence* je nevýstižný překlad, vhodnější by zde bylo právě *přesvědčení*, český překlad nařízení je a bude jen průměrně kvalitní, byť výrazně lepší než u směrnice 1999/93/ES. Osobám hledajícím více než jen orientaci v předpise je stále nutné doporučit číst znění anglické popř. jiné.

[46] Andersdotter byla v právě skončeném období Evropskou poslankyní za švédskou Pirátskou stranu, na průchodu eIDAS Evropským parlamentem se podílela jako jeden z pěti tzv. stínových zpravodajů, kteří se o postup schvalování konkrétního předpisu starají ve značně zvýšené míře.

nesrozumitelné, pak je to tím, že nesrozumitelný a hrubě nekvalitní byl již samotný text návrhu nařízení od Komise z roku 2012. Evropský parlament jako těleso je dle ní složeno z politických zástupců a nikoli z expertů. Poslanci se snažili návrh zlepšit, jak jen to bylo možné, ovšem například pět měsíců strávili jen dohady nad tím, jaký je rozdíl mezi autentizací a identifikací.

Závěr

V tomto článku jsem se mohl dotknout pouze některých záležitostí spojených s novým nařízením eIDAS, které považuji za důležité a byly mi dostatečně známé[47] již před publikací výsledného znění nařízení.

Na přijetí nařízení bude potřeba v českém právním řádu reagovat. Relativně nejsnazší částí reakce budou technické novely, které budou v existujících zákonech aj. právních předpisech nahrazovat odkazy na ZoEP odkazy na eIDAS a jeho pojmy. Ani tyto úpravy nemusí být zcela triviální, neboť pojmy ZoEP a eIDAS se zcela nekryjí.

Obtížnější částí bude komplementární úprava, čímž rozumím doplňkovou úpravu k eIDAS ve velmi těsné návaznosti na něj. Český zákonodárce se bude pohybovat na tenkém ledě, neboť na jedné straně evropské právo si pro formu nařízení ostře vyhrazuje svou aplikační přednost, na straně druhé četné nedokonalosti eIDAS budou vyžadovat zaplnit mezery a doplnění představuje jednu z možností, jak nedokonalosti přeci jen napravit. Není například zcela vyloučené, že by tímto způsobem třeba elektronickou značku bylo možné v českém právním řádu přeci jen zachránit. Bude zřejmě vhodné sledovat i legislativní aktivity doplňující přijetí eIDAS v jiných členských státech a nechat se jimi jak inspirovat, tak se pohybovat v rámci hlavního legislativního i technického proudu v zemích EU.

Významnou změnu nebo doplnění budou vyžadovat předpisy upravující nyní v ČR provoz datových schránek, neboť ty bude nutné minimálně navázat na služby elektronického doporučeného doručování podle eIDAS.

Kromě úřadů se na změny budou muset postupně připravit i současní poskytovatelé certifikačních služeb, kterým rozhodně vzroste konkurence ze zahraničí.

Asi nejobtížnější potřeby mají institucionální ráz. I když vyhlášeným účelem, vetknutým i do samotného názvu nařízení, jsou elektronické transakce na vnitřním trhu, u nařízení lze očekávat praktické použití zejména v oblasti e-governmentu, tj. správního jednání členských států, popř. i e-justice, tj. soudnictví. V ČR ale v současnosti neexistuje ústřední správní úřad, který by problematiku elektronických podpisů věcně a právně ovládal. Kompetenční zákon sice působnost v oblasti elektronického podpisu svěřuje Ministerstvu vnitra, to však po mnoha organizačních změnách v roce 2011 zrušilo oddělení elektronického podpisu, čímž zanikl útvar, který se elektronickému podpisu věnoval celou dekádu od přijetí ZoEP, byť postupně pod hlavičkou tří různých správních úřadů. Současně zanikla institucionální paměť a znalosti státu, kterou k problematice snad měl. Tento stav má nejméně dva silně negativní důsledky.

Prvním je, že v ČR nikdo úřady a veřejnou správu nevede metodicky ke správnému používání elektronických podpisů, a to ani, když díky zavedení datových schránek vznikají řádově desítky milionů elektronicky podepsaných elektronických dokumentů.

Druhým negativem je, že v průběhu přijímání nařízení eIDAS nebylo Ministerstvo vnitra mocno za ČR vůbec vyjádřit jasně svoji pozici, popř. naléhat na zlepšení obsahu eIDAS v komisích Rady, ve kterých mělo plnohodnotnou účast. Je otázka, jak si bude Ministerstvo vnitra (MV) počínat vůči EU v další periodě přijímání prováděcích aktů k eIDAS? Nejen elektronický podpis, ale i elektronická identifikace je v dosavadním provádění e-governmentu v ČR značně zanedbána.

Úplným závěrem trochu optimističtějšího tónu. Jakkoli je eIDAS z právního pohledu značně nedokonalým předpisem, z technického hlediska poskytne impuls pro tvorbu několika desítek potřebných technických specifikací a norem, které budou přinejmenším elektronický podpis, a doufejme, že i elektronickou identifikaci, sjednocovat pro území všech 27 členských států s více než 500 miliony obyvatel. To bude mít dobrý dopad nejenom na přeshraniční interoperabilitu, ale především na zájem dodavatelských společností, včetně těch větších, o podporu implementace „evropského podpisu" a „evropské identifikace" do mnoha nových softwarových aplikací, tedy potažmo i do mnoha nových obchodních nebo správních použití. Oproti tomu paralelní implementace 27 variant velmi podobných, ale technicky i právně přeci jen mírně odlišných, elektronických podpisů lukrativní nebyla a není. Dále – i když právní předpis není právně dokonalý, technická implementace, včetně organizačních aj. podmínek nasazení techniky, může být subjekty dobrovolně realizována i nad požadavky práva, neboť špatné nasazení není ekonomicky významně levnější

[47] Viz např. stanovisko autora k návrhu nařízení: http://www.vkc.cz/pdf/Opinion_V-Kment_edited_11th_Dec2012.pdf.

než nasazení dobré, které naopak perspektivně může zabránit jak mrhání prostředky, tak i případným škodám. Úřady by v takovém technickém úsilí měly jít příkladem a měl by existovat ústřední správní úřad nebo institut, který by takové nasazování metodicky prosazoval a měl i dostatečné pravomoci či možnosti skutečného prosazení.

Zde je na místě opět trochu pesimismu, neboť mi není známa metoda, jakou by taková osvícená činnost úřadů mohla vzniknout.