Nařízení eIDAS (nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu)

Autoři: Bc. Filip Bílek, Ing. Ondřej Felix CSc., a kolektiv odboru veřejné správy a eGovernmentu Ministerstvo vnitra České republiky

Článek byl poprvé publikován ve Sborníku konference ISSS, duben 2014

Upozornění: terminologie českého překladu Nařízení eIDAS se pravděpodobně bude ještě měnit. Zde uvedené překladové termíny pojmů do českého jazyka proto není možné považovat za finální.

- - -

Zanedlouho vejde v celé Evropské unii v platnost dlouho očekávaný právní předpis umožňující přeshraniční uznávání a interoperabilitu bezpečných systémů elektronické identifikace a autentizace, který změní fungování elektronické veřejné správy (eGovernmentu) i v České republice. Jde o další krok k vytvoření jednotného digitálního trhu, který zahrnuje volný pohyb osob, zboží, kapitálu a nyní i služeb. Nebude již trvat dlouho a bude možné využívat online služby přeshraničně, což bude znamenat například, že student se bude moci přihlásit na zahraniční univerzitu online, občané budou moci vyplnit daňové přiznání v jiném členském státu online, bude možné online vyřídit nezbytné formality týkající se práce, bydlení a pobírání důchodu kdekoliv na území EU. Podnikatelům bude umožněno zřídit a provozovat podnik kdekoliv v Evropě, nezávisle na původním umístění, nebo se přihlásit elektronicky do výběrového řízení na zakázky v celé EU. Jak je vidět na výše zmíněných příkladech, nařízení umožní lepší využití elektronických prostředků v běžném životě.

První návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu (nařízení) vydala Evropská komise dne 4. června 2012. Tento návrh patří, jakožto jedno z klíčových opatření Aktu o jednotném trhu mezi nejvýznamnější iniciativy v oblasti budování jednotného digitálního trhu a má za cíl zvýšit důvěryhodnost elektronických transakcí v rámci vnitřního trhu EU. Komise zde navazuje na úkoly vytyčené v Digitální agendě pro Evropu. Obsah prvního návrhu vzešel z konzultací, jež probíhaly na více úrovních, studií a názorů a potřeb zúčastněných stran. Návrh byl v průběhu tří let opakovaně projednáván v rámci pracovní skupiny Rady pro telekomunikace a informační společnost, kdy se předmětem diskuzí staly všechny části návrhu a vznikl tak postupným jednáním kompromisní text návrhu.

Nařízení se dotkne zejména následujících oblastí:
1) důvěryhodná elektronická identita fyzické osoby;
2) důvěryhodný podpis zaručující integritu a vazbu na identitu fyzické osoby;
3) důvěryhodná značka zajišťující integritu a vazbu na právnickou osobu;
4) důvěryhodné časové razítko zajišťující integritu a vazbu na čas;
5) důvěryhodná služba registrovaného elektronického doručování zajišťující integritu a vazbu na odesílatele, adresáta a čas odeslání a doručení;
6) důvěryhodný dokument se zaručenou integritou;
7) důvěryhodnost webových stránek s vazbou na provozovatele.

Dne 28. února 2014 velvyslanci při EU schválili dosaženou politickou dohodu mezi reprezentanty EP, EK a Rady, která se týká posledních úprav tohoto důležitého návrhu pro lepší fungování vnitřního trhu. Dle aktuálního plánu bude návrh předložen na plenárním zasedání Evropského parlamentu (EP) v dubnu a Radě ministrů v červnu. Jelikož na základě proběhlých čtyř trialogů byly do návrhu zapracovány i některé připomínky EP, dá se očekávat, že návrh bude odsouhlasen bez připomínek a nařízení vstoupí v platnost 1. července 2014 (nařízení bude zveřejněno v Úředním věstníku EU). Data účinnosti jednotlivých částí jsou s ohledem na nutnost předložení souvisejících prováděcích aktů a na potřebu přizpůsobení členských států odložena tak, že ustanovení nařízení budou nabývat účinnosti postupně podle přijetí prováděcích aktů v období 2015 - 2018 a povinnost vzájemně uznávat oznámené prostředky pro elektronickou identifikaci nabyde účinnosti v polovině roku 2018. Dobrovolné uznávání oznámených systémů elektronické identifikace může v členském státě začít ihned po přijetí potřebných prováděcích aktů týkajících se úrovní zabezpečení a interoperability. Vzhledem ke zvolené právní formě, bude nařízení přímo aplikovatelné ve všech členských státech EU a bude tím zrušena stávající směrnice o elektronickém podpisu 1999/93/EC. Důležité je zmínit, že stávající legislativa EU se zaobírá zejména oblastí elektronického podpisu, kdežto nařízení bere v potaz celé spektrum důvěryhodných služeb a reaguje tak na neustálý vývoj a stanovuje jejich podmínky a vlastnosti tak, aby byla posílena důvěryhodnost těchto služeb s cílem motivovat potencionální uživatele k jejich využívání, což odpovídá výsledkům a dopadům očekávaným ze strany EK :

„Stanovení jednoznačného právního prostředí pro elektronickou identifikaci, autentizaci, podpis a související důvěryhodné služby, jež zvýší pohodlí a důvěru uživatelů v digitální svět.“

Důvěra v online světě je klíčová z hlediska ekonomického a společenského rozvoje. Z tohoto důvodu je nutné posílit právní jistoty a vyslat k potencionálním uživatelům jasnou zprávu, že mohou bez obav využívat elektronické důvěryhodné služby, ať se jedná o občany, soukromé společnosti či subjekty veřejného sektoru. Tudíž jednou z nejdůležitějších definic v návrhu nařízení je zcela jistě definice důvěryhodné služby, respektive co lze považovat za důvěryhodnou službu. **Za důvěryhodnou službu se považuje mimo jiné vytváření, verifikace a validace elektronických podpisů, značek a časových razítek a certifikátů týkajících se těchto služeb.**

Návrh se také zaobírá problematikou používání elektronické identifikace (eID). V současné době existují překážky v používání prostředků pro elektronickou identifikaci (prostředků eID) v jiných zemích než v těch, ve kterých byly vydány, a které brání poskytovatelům služeb ve využívání všech výhod vnitřního trhu. Z tohoto důvodu nařízení ukládá uznávat systémy elektronické identifikace, které budou jednotlivými členskými státy notifikovány (oznámeny) za předpokladu splnění určitých podmínek. Notifikace těchto systémů není povinná, každý členský stát má možnost si zvolit, které z používaných systémů notifikuje a tím umožní uznání prostředků eID vydaných v rámci tohoto systému i v ostatních státech minimálně při přístupu ke službám poskytovaným veřejným sektorem. Této oblasti se věnoval mezinárodní projekt STORK, na který navazuje STORK 2.0.

Dostupnost autentizačního procesu zajišťuje oznamující stát a musí být zajištěna tak, aby každá spoléhající se strana mohla prostřednictvím tohoto procesu ověřit identifikační údaje, které obdržela elektronickou cestou. Je stanovena také odpovědnost zúčastněných stran v případě selhání přeshraniční autentizace. Členské státy mohou definovat podmínky používání takovéto autentizace pro spoléhající se strany pocházející ze soukromého sektoru. Rozlišují se úrovně zabezpečení

systémů elektronické identifikace v závislosti na způsobu zjištění identity konkrétní osoby. Jsou definovány tři úrovně zabezpečení (low, substantial a high), kde nejvyšší úroveň by měla poskytnout vysoký stupeň důvěry v identitu ověřované osoby. Pro tuto oblast EK vytvoří konkrétní prováděcí akty, které mají zabezpečit funkčnost úrovní zabezpečení.

Vůbec nařízení, jako celek, klade důraz na vzájemnou spolupráci členských států a organizací v celé řadě aspektů, kdy by si navzájem měly vyměňovat poznatky a zkušenosti, které by vedly ke zlepšení fungování jednotného vnitřního trhu.

Také došlo k rozšíření nařízení v oblasti nároku na náhradu škody, kterou by způsobil svojí nedbalostí poskytovatel důvěryhodných služeb v důsledku nedodržení bezpečnostních postupů. U orgánů dohledu došlo k rozšíření působnosti, co se týče poskytovatelů důvěryhodných služeb i kvalifikovaných poskytovatelů důvěryhodných služeb. Nařízení jim ukládá přijmout relevantní opatření, jak technická, tak i organizační tak, aby byla zajištěna bezpečnost poskytovaných služeb. Při narušení bezpečnosti je stanovena povinnost, aby poskytovatel důvěryhodných služeb vyrozuměl v co nejkratší době o této události orgán dohledu a, pokud bezpečnostní narušení může ovlivnit uživatele služby, informoval i je.

Současná podoba trusted listů dozná také změn, protože trusted listy by podle tohoto nařízení měly obsahovat informace o kvalifikovaných poskytovatelích důvěryhodných služeb – připomeňme si, že důvěryhodné služby zahrnují mnohem širší spektrum služeb než doposud.

Další regulovanou oblastí je elektronický podpis, kde již pro tuto oblast existuje příslušná směrnice **1999/93/EC**, ze které nové nařízení v této oblasti de facto vychází a dále ji rozšiřuje. Je nutné dodat, že přijetím nařízení bude směrnice **1999/93/EC** zrušena a to k 1. červenci 2016. Pojem „zaručený elektronický podpis“ (advanced electronic signature) zůstává zachován, ale nově se zavádí pojem „kvalifikovaný elektronický podpis“ (qualified electronic signature), který musí být založen na kvalifikovaném certifikátu a zároveň elektronický podpis musí být vytvořen pomocí kvalifikovaného zařízení pro vytváření elektronického podpisu (dnešní bezpečná zařízení pro tvorbu elektronického podpisu, tzv. SSCD zařízení, by měla být uznaná podle nového nařízení jako kvalifikovaná zařízení). Tento typ podpisu má mít stejné právní účinky jako vlastnoruční podpis ve všech členských státech, zatímco právní účinky u ostatních typů elektronických podpisů mají být definovány na úrovni národního práva. Existuje zde jistá podobnost s „naším“ uznávaným elektronickým podpisem, jak jej definuje zákon č. 227/2000 Sb. (zákon o elektronickém podpisu), dle kterého uznávaný elektronický podpis musí být založen na kvalifikovaném certifikátu vydaným akreditovanou certifikační autoritou, ale již se neklade taková povinnost na použití speciálních zařízení pro tvorbu elektronického podpisu. V nařízení jsou rovněž specifikovány požadavky, které musí splnit kvalifikované certifikáty pro elektronický podpis a požadavky na kvalifikovaná zařízení pro vytváření elektronického podpisu, které vesměs vycházejí a rozšiřují stávající směrnici. Je zachována koncepce certifikace zařízení pro tvorbu elektronického podpisu. Certifikaci zařízení by měl provést subjekt pověřený členským státem, aby potvrdil, že zařízení splňuje specifikované požadavky na kvalifikované zařízení pro tvorbu elektronického podpisu. Seznam certifikovaných zařízení zveřejňuje Komise. Novinkou v nařízení je stanovení podmínek pro kvalifikované uchovávání kvalifikovaných elektronických podpisů, kdy poskytovatel důvěryhodných služeb musí použít patřičné technologie umožňující dlouhodobé zajištění důvěryhodnosti dat.

Legalizuje se definice elektronické značky (anglický termín „electronic seal“) a časových razítek - náš zákon o elektronickém podpise zná termíny elektronická značka či časové razítko, nicméně ve stávající směrnici **1999/93/EC** zmíněny nebyly. Nové nařízení to teď mění a na evropské úrovni se

zavádějí pojmy elektronická značka a časové razítko a k tomu jejich kvalifikované typy, kdy opět u kvalifikovaných značek či razítek jsou přiznány jisté vlastnosti.

Konkrétně kvalifikovaná elektronická značka by měla zajistit právní domněnku, která zaručuje původ a integritu dat, s nimiž je spojena a kvalifikované časové razítko by mělo zajistit právní domněnku ohledně spolehlivosti časového okamžiku a integrity dat, se kterými je časové razítko spojeno. Podobně, jako jsou definovány požadavky v oblasti elektronického podpisu, jsou definovány rovněž i pro oblast elektronických značek. Stanovena je také povinnost uznávat kvalifikované elektronické značky a kvalifikovaná časová razítka vydaná v jednom členském státě ve všech členských státech. U kvalifikovaných elektronických značek existuje rozdíl mezi jejich vymezením v nařízení a ve stávajícím zákonu o elektronickém podpisu, podle kterého elektronickou značkou může data označit osoba fyzická i osoba právnická. Podle nového nařízení elektronickou značkou může data „označit“ pouze právnická osoba (dle definice „creator of a seal“).

V souhrnu tedy kvalifikovaný elektronický podpis, značka a časové razítko jsou nástroje pro zajištění důvěryhodnosti a integrity elektronického dokumentu. V praxi by tedy důvěryhodný dokument pocházející od právnické osoby mohl obsahovat tyto prvky:

- elektronický podpis, který zaručuje identitu fyzické osoby, která je oprávněna dokumenty podepisovat;
- elektronickou značku zaručující identitu právnické osoby;
- elektronické časové razítko zaručující integritu a vazbu na čas.

Nařízení se věnuje také problematice služby elektronického doručování, kde jsou opět definovány dvě verze – nekvalifikovaná a kvalifikovaná. Pro kvalifikovanou verzi služby jsou definovány podmínky, které služba musí splňovat, aby mohla být považována za kvalifikovanou.

Toto nařízení vstupuje v platnost dvacátým dnem po zveřejnění v Úředním věstníku Evropské unie. S výjimkou některých ustanovení se použitelnost (účinnost) tohoto nařízení předpokládá od 1. července 2016. Od tohoto data se zruší stávající směrnice 1999/93/ ES a odkazy na zrušenou směrnici budou považovány za odkazy na nařízení. Datum účinnosti jednotlivých opatření je rozděleno s ohledem na fakt, že například pro uznávání prostředků pro elektronickou identifikaci je třeba nejprve vytvořit relevantní prováděcí akty. Nařízení počítá s řadou přechodných opatření.

Z výše uvedeného vyplývá, že implementace tohoto nařízení bude náročná a přinese s sebou nutnost úprav některých stávajících informačních systémů veřejné správy tak, aby způsobem odpovídajícím ustanovením nového nařízení mohly podporovat národní prostředky eID všech členských států Evropské unie vydané v rámci jejich oznámených systémů elektronické identifikace. Předpokládanými nástroji pro implementaci nařízení budou základní registry spolu s elektronickými občanskými průkazy, úprava informačního systému datových schránek a novelizace některých zákonů, jako např. zákona o elektronickém podpisu nebo zákona o archivnictví.