

Co přináší eIDAS v oblasti elektronické identifikace?

Elektronická identifikace představuje zcela novou oblast regulace. Díky ní již eID není výhradní doménou národních vlád a ministerstev, ale otevírá dveře i soukromým subjektům. Ty navíc mohou působit hned v několika zemích EU zároveň.

Jednou z významných novinek, které přináší evropské Nařízení eIDAS, je oblast elektronické identifikace včetně vzájemného uznávání např. elektronických občanských průkazů vydaných v jednotlivých členských státech. Tato myšlenka není v Evropě zdaleka nová. V minulosti byla ověřována v rámci několika pilotních projektů. Nyní se jí však dostalo nezbytné legislativní opory, od které si mnozí slibují celou řadu změn v oblasti eID. Uvidíme, zda tyto změny budou opravdu revoluční, nebo spíše jen evoluční.

Mezi klíčové principy, ze kterých Evropská unie vychází, se řadí tzv. jednotný vnitřní trh založený na volném pohybu osob, zboží, kapitálu a služeb. V průběhu posledního čtvrtstoletí se mnohé překážky, které bránily naplnění některé z těchto čtyř hlavních svobod, podařilo úspěšně odstranit.

Díky tomu dnes pro 21 miliónů malých a středních firem představují mezinárodní aktivity se společnostmi z jiných států EU podstatnou součást jejich podnikání.

Svoji roli při budování jednotného trhu sehrály rovněž informační technologie. Jejich dynamický rozvoj zapříčinil, že některé překážky sice byly odstraněny, další však díky nim vznikly. Příkladem je právě oblast elektronické identifikace a občanských průkazů. Zatímco dnes je možné cestovat od Algarve v Portugalsku po Varšavu či z Athén do švédské Växjö a svůj občanský průkaz bez problémů využívat při identifikaci na letištích, v hotelech i autopůjčovnách, u elektronických průkazů situace tak jednoduchá není. Pokud by chtěl např. Estonec, který je jednatelem firmy v České republice, odeslat elektronicky daňové přiznání nebo se přihlásit do své datové schránky, jako je tomu zvyklý ze své země, stane se to pro něj zatím nepřekonatelnou překážkou.

Změnu by mělo přinést právě Nařízení eIDAS[1], které je součástí širších snah Evropské komise o vybudování tzv. jednotného digitálního trhu, který lze označit za přirozené pokračování či další fázi jednotného vnitřního trhu.

Myšlenka vzájemného uznávání eID není nová

Snahy Evropské komise o umožnění vzájemného uznávání prostředků elektronické identifikace jako jedné ze součástí jednotného trhu jsou dlouhodobé a objevovaly se mnohem dříve než 23. července 2014, kdy bylo Nařízení eIDAS publikováno v Úředním věstníku.

V politické rovině se jedná především o strategii Digitální agenda pro Evropu¹ a z ní vycházející Evropský akční plán „eGovernment“ na období 2011 až 2015². Cílem těchto

¹ KOM(2010)245

² KOM(2010)743

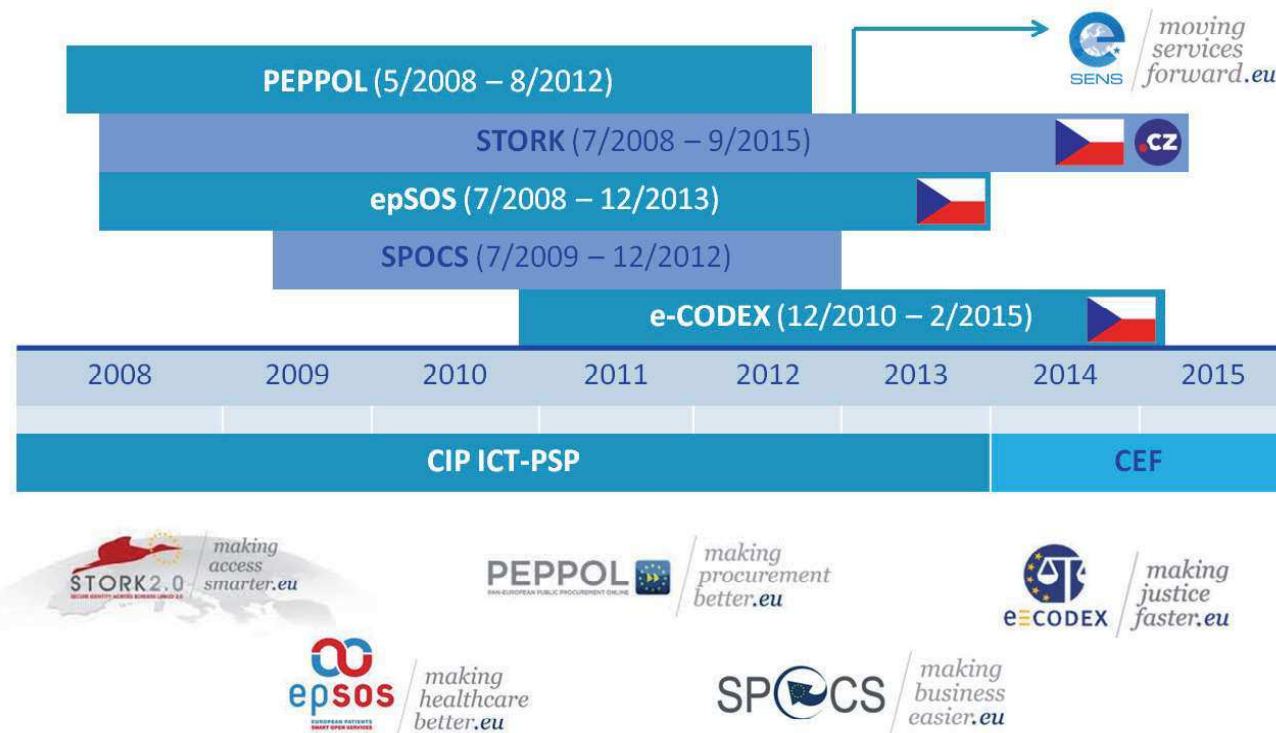
dokumentů bylo vytvoření elektronických služeb, které podnikatelům umožní zřídit a provozovat podnik kdekoli v Evropě, nezávisle na původním umístění. Občanům dovolí studovat, pracovat, bydlet a pobírat důchod kdekoli na území Evropské unie.

Nedílnou součástí snah o vytvoření jednotného digitálního trhu jsou již od roku 2008 (viz obr. 1) tzv. rozsáhlé pilotní projekty (LSP), ve kterých se členské státy připravovaly a testovaly interoperabilitu svých systémů pro poskytování přeshraničních služeb (více viz [4]). Tyto projekty podporované Evropskou komisí položily základ nejednoho legislativního dokumentu.

V oblasti elektronické identifikace sehrály významnou roli projekty STORK a STORK 2.0³, které položily základy infrastruktury pro vzájemné uznávání eID v podobě tzv. PEPS (Pan European Proxy Services) a definovaly požadavky na tzv. úroveň důvěry označované jako Quality Authentication Assurance (QAA). eIDAS je převzal v podobě tzv. úrovně záruky.[5] Na druhou stranu je pravda, že pilotní scénáře nebyly pro uživatele příliš atraktivní, a tak počet přeshraničních transakcí nedosáhl významných čísel.

Mezi další LSP patří projekt epSOS, který se věnoval oblasti e-Health a sdílení základních dat o pacientech (např. krevní skupiny), aby tyto údaje byly k dispozici lékařům ošetřujícím např. zraněného českého lyžaře v Rakousku.

Projekt PEPPOL se zase zaměřoval na problematiku přeshraničního zadávání veřejných zakázek a usnadnění komunikace jak mezi dodavatelem a odběratelem ve všech fázích výběru veřejné zakázky, tak v případě vlastního nákupu a platby.



Obr. 1: Časová osa realizace rozsáhlých pilotních projektů jednotného digitálního trhu

Cílem projektu SPOCS bylo naopak usnadnit zahájení podnikání v jiném členském státě a propojit tzv. jednotná kontaktní místa v návaznosti na požadavky kladené Směrnicí o službách.

e-CODEX, historicky nejmladší LSP zaměřený na konkrétní oblast e-Governmentu, se zabýval problematikou e-Justice a usnadněním přeshraniční spolupráce např. při realizaci Evropského platebního rozkazu (EPO), Evropského zatýkacího rozkazu (EAW) či vzájemného uznávání peněžitých trestů a pokut.

Na výše uvedených pět rozsáhlých projektů pak od dubna 2013 navázal projekt e-SENS (Electronic Simple European Networked Services)⁴, jehož ukončení je plánováno ke konci března příštího roku. Cílem tohoto projektu je integrovat řešení vzniklá z dosavadních LSP a postupně vytvářet tzv. základní kameny (building blocks) pro budování přeshraničních služeb e-Governmentu. Např. oblast elektronického doručování (e-Delivery) by tak měla být řešena univerzálně pro všechny služby e-Governmentu, ať se jedná o již zmíněnou e-Justici, zasílání elektronických faktur v rámci veřejných zakázek nebo doručování úředních rozhodnutí podobně, jako je tomu od roku 2009 v České republice v případě datových schránek.

³ Secure idenTity acrOss boRders linKed 2.0. Více informací o projektu na <https://www.eid-stork2.eu/>

⁴ Více informací o projektu na <http://www.esens.cz/>

Právní ukotvení a definici těchto základních stavebních kamenů (graficky znázorněných na obr. 2) nalezneme v rámci Nařízení Evropského parlamentu a Rady č. 283/2014 o hlavních směrech transevropských sítí v oblasti telekomunikační infrastruktury, tj. dokumentu, který byl publikován ještě před Nařízením eIDAS a kterému stále není věnována patřičná pozornost. Přitom právě toto nařízení představuje základ finančního Nástroje pro propojení Evropy (Connecting Europe Facility) a definici klíčových služeb evropského e-Governmentu umožňujících vzájemné propojení a spolupráci mezi členskými státy.

Mnohé členské státy včetně České republiky se díky řešení rozsáhlých pilotních projektů mohly připravit na požadavky, které na ně bude později klást legislativa s tím, že především softwarové výstupy projektu STORK, resp. STORK 2.0 a projektu e-SENS lze díky distribuci v podobě otevřeného softwaru využít při přípravách na Nařízení eIDAS a integraci do národních projektů e-Governmentu.

Základem je důvěra

Jeden z klíčových principů, na kterých je Nařízení eIDAS založeno, představuje vzájemná důvěra mezi členskými státy. Tento princip je již dlouhodobě uplatňován při vzájemném uznávání kvalifikovaných certifikátů pro elektronické podpisy. Nyní se tato myšlenka rozšiřuje (byť za jiných podmínek) na oblast eID, kde význam se promítl i do samotné zkratky eIDAS (Electronic Identification and Services).



Obr. 2: Základní stavební bloky pro přeshraniční digitální služby

Další z principů eIDAS představuje technologická neutralita, kdy jako tzv. prostředky pro elektronickou identifikaci lze využít jak elektronické občanské průkazy s čipem, tak moderní a uživatelsky přívětivější mobilní eID založené na autentizačních SMS zprávách známých např. z oblasti elektronického bankovníctví nebo na zcela nových způsobech mobilní identifikace (jako příklad lze uvést britskou službu YOTI⁵).

eIDAS zároveň podporuje, aby tyto autentizační prostředky vydávaly nejen členské státy, ale rovněž soukromoprávní subjekty, a uživatelé se tak mohli ke službám e-Govern-

mentu v různých zemích EU přihlašovat stejně, jako se přihlašují do své banky či prostřednictvím služby mojeID⁶ do elektronických obchodů, diskuzí na zpravodajských serverech či knihoven.

Zkušenosti ze skandinávských zemí, ale rovněž např. z Lucemburska či Velké Británie, totiž ukázaly, že úspěšný eID prostředek by měl umožňovat přihlašování nejen pro potřeby komunikace s veřejnou správou, ale rovněž k dalším komerčním i nekomerčním službám tak, aby občané mohli tento nástroj využívat pravidelně, nikoli jen jednou za čas (často jedenkrát ročně), kdy potřebují odeslat na úřad např. daňové přiznání.

Při nastavení důvěry mezi členskými státy vycházejí nařízení z již zmíněných zkušeností projektu STORK. Na rozdíl od něj

⁵ Tato aplikace pro mobilní telefony je založena na ověření informací o dané osobě na základě údajů z (naskenovaného či vyfoceného) občanského průkazu a fotografie pořízené samotným uživatelem. Ten se pak sám může rozhodnout, s kým bude údaje sdílet, a v případě, že bude daná aplikace uznávána, ji použít rovněž např. k prokázání věku při vstupu na diskotéku. Personálu se přitom nemusí zobrazovat datum narození, ale pouze informace „starší 18 let“. Více informací o této službě na www.yoti.com.

⁶ Více informací o této službě, jejímž provozovatelem je sdružení CZ.NIC, správce národní domény .cz, je možné nalézt na www.mojeid.cz.

ale formou minimálních standardů definuje (viz čl. 8 nařízení) pro prostředky elektronické identifikace pouze následující tři úrovně důvěry:

- nízká úroveň označuje prostředek, který nabízí omezenou míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby a je charakterizován pomocí souvisejících technických specifikací, norem a postupů včetně technických kontrol, jejichž účelem je snížit riziko zneužití nebo změny totožnosti,
- značná úroveň označuje prostředek, který nabízí značnou míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby a je charakterizován pomocí souvisejících technických specifikací, norem a postupů včetně technických kontrol, jejichž účelem je značně snížit riziko zneužití nebo změny totožnosti,
- vysoká úroveň označuje prostředek, který nabízí vyšší míru spolehlivosti u deklarované nebo uváděné totožnosti určité osoby než prostředek pro elektronickou identifikaci se značnou úrovní záruky a je charakterizován pomocí souvisejících technických specifikací, norem a postupů včetně technických kontrol, jejichž účelem je předejít zneužití nebo změně totožnosti.

Konkrétní požadavky na nízkou, značnou nebo vysokou úroveň záruky definuje zmíněné prováděcí nařízení č. 2015/1502 [3], které stanoví celkem 16 kritérií zohledňujících důvěryhodnost poskytnutých atributů a autentizačního prostředku. Výslednou úroveň daného prostředku pak určuje jeho nejslabší článek.

Klíčové kritérium pro stanovení dané úrovně představuje „vlastnost prostředku elektronické identifikace“, kdy větší-

nou uživateli nejvyužívanější způsob přihlašování prostřednictvím uživatelského jména a hesla (tzv. jednofaktorová autentizace) odpovídá nízké úrovni důvěry. Pro dosažení značné úrovně je třeba využít dvoufaktorovou autentizaci, ať již v podobě jednorázových SMS či one-time-password (OTP) generovaného prostřednictvím speciální aplikace v mobilním telefonu. U vysoké úrovně záruky je pak vyžadováno využití takových prostředků, které chrání proti vyhotovení duplikátů a neoprávněné manipulaci, tj. např. eID karet či tokenů.

Zároveň ani vysoká úroveň důvěry nemusí být dostatečná pro některé specifické služby, jako je např. založení účtu v bance vyžadující fyzickou přítomnost dané osoby. Zde je podle mě škoda, že eIDAS není zohledněn v dalších právních předpisech a že s využitím eIDAS identifikace např. zatím příliš nepočítá ani nová evropská Směrnice o platebních službách (PSD2) nebo nedávno schválený český zákon č. 186/2014 Sb., o hazardních hrách.

V souvislosti s možným využitím jednotlivých prostředků je dále třeba počítat s tím, že ani to nejsilnější ověření nemusí být dostatečné pro všechny služby. Je na každém členském státě, aby si stanovil, jakou úroveň důvěry pro konkrétní službu vyžaduje. eIDAS zároveň nezavádí povinnost elektronizace jednotlivých agend, a tak např. v Estonsku, které je často dáváno v oblasti elektronizace za příklad, existují agentury jako svatba či prodej nemovitostí, které kompletně přes Internet nevyřídíte.

Jak propojit jednotlivé země?

Při propojování jednotlivých zemí vychází nařízení eIDAS především z výsledků projektu STORK a STORK 2.0, kdy se však již v roce 2008 ukázala značná odlišnost jednotlivých národních systémů a jejich legislativy.

Fyzické osoby	Právníkové osoby
Povinné atributy	
Příjmení (současné)	Název (současný)
Jméno (současné)	Jedinečný (ideálně neměnný) identifikátor
Datum narození	
Jedinečný (ideálně neměnný) identifikátor	
Volitelné atributy	
Rodné příjmení/jméno	Adresa (současná)
Místo narození	IČ
Adresa (současná)	DIČ
Pohlaví	Další identifikátory (např. EORI)

Tabulka 1: Přehled atributů předávaných v rámci přeshraniční identifikace

Místo jednotného „evropského“ občanského průkazu, který by byl obdobou např. karty zdravotní pojišťovny, se členské státy vydaly cestou založenou na architektuře národních bran ve STORKu označovaných Pan European Proxy Services (PEPS), v rámci eIDAS definovaných jako tzv. eIDAS uzly (eIDAS nodes). Český eIDAS uzel je v rámci projektu CZ.PEPS budován na základě smlouvy s Evropskou komisí sdružením CZ.NIC.

Tyto brány jsou prostřednictvím protokolu SAML 2.0 vzájemně propojeny systémem „každý s každým“. Úkolem jednotlivých provozovatelů PEPS je zajistit napojení těchto bran na národní eID prostředky, přičemž eIDAS podporuje využití více prostředků (např. elektronického občanského průkazu, mobilního eID či USB tokenu, a to i od různých poskytovatelů), aby měl uživatel možnost volby.

Z pohledu předávaných údajů si zatím eIDAS, resp. jeho prováděcí nařízení č. 2015/1501 [2], neklade příliš vysoké cíle – z tabulky 1 je patrné, že tento rozsah je srovnatelný s minimálním rozsahem údajů obsažených v základních registrech.

Podobně jako u českých základních registrů není mezi povinnými údaji (atributy) zahrnuto telefonní číslo či e-mail, pomocí něhož by mohly např. e-shopy či další komerční služby zajistit snadné ztotožnění uživatelů.

Ve vztahu k základním registrům a aktuálnosti údajů zároveň ani vysoká úroveň záruky nepožaduje ověření údajů při každém přihlášení. eIDAS tak v oblasti elektronické identifikace vychází z podobného principu jako u elektronických podpisů, kdy skutečné údaje (např. bydliště) lze ověřit až zpětně u daného poskytovatele, např. na základě dotazu policie či soudu.

Jak eIDAS ovlivní eID v České republice?

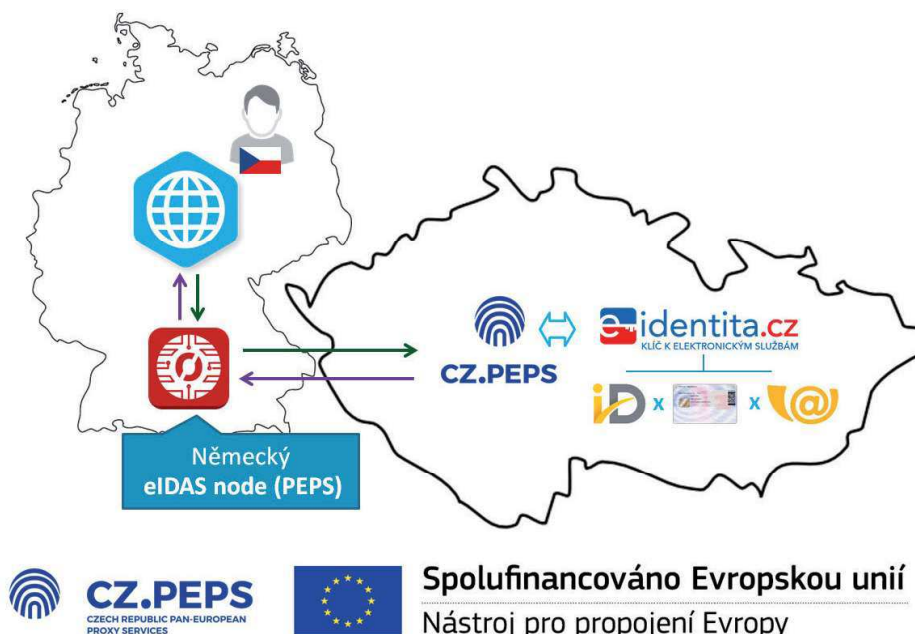
V České republice je implementace eIDAS rozdělena do dvou klíčových právních předpisů, které se snaží respektovat strukturu nařízení. Zatímco tzv. služby vytvářející důvěru (tj. oblast elektronického podpisu a pečeti, časových razítek či elektronického doručování) jsou upraveny zákonem o službách vytvářejících důvěru, který v tuto chvíli čeká na vydání ve Sbírce zákonů (byl již podepsán prezidentem), pro oblast elektronické identifikace je připravován zvláštní zákon, jehož paragrafové znění plánuje Ministerstvo vnitra ČR představit do konce tohoto roku.

Přestože eIDAS členským státům neukládá povinnost vydávání elektronických občanských průkazů či jiných eID prostředků, Česká republika se podobně jako další země snaží této legislativy využít ke zkvalitnění svého e-Governmentu. Fungující elektronická identifikace přitom představuje zá-

kladní předpoklad ovlivňující vyspělost jednotlivých elektronických služeb a možnost občanů či podnikatelů vyřídit danou agendu čistě prostřednictvím Internetu.

Pro občany bude mezi nejviditelnější změny patřit především vydávání nových občanských průkazů. Jejich součástí bude rovněž čip umožňující elektronickou identifikaci či uložení kvalifikovaného certifikátu pro elektronický podpis. Pozitivní změnou jistě je, že na rozdíl od dnešního stavu již nebude nutné za čip připlácet 500 Kč. Méně pozitivní je skutečnost, že Ministerstvo vnitra ČR vydávání těchto průkazů opakovaně posunulo. Podle aktuálních informací budou nové občanské průkazy vydávány až od roku 2018.

Do té doby budou pravděpodobně v České republice dostupné i jiné nástroje včetně tzv. Národní identitní autority (NIA), resp. systému *identita.cz* provozovaného Správou základních registrů. Tento systém by se měl v budoucnu stát rozhraním umožňujícím jak přihlašování k vybraným službám v České republice, tak v souladu s eIDAS i v zahraničí a podporovat různé elektronické nástroje. Vedle elektronických občanských průkazů se hovoří např. o možnosti identifikace přes datové schránky, což dnes využívá např. Česká správa sociálního zabezpečení, nebo o službě *mojeID*. Možné schéma fungování přeshraniční identifikace znázorňuje obr. 3.

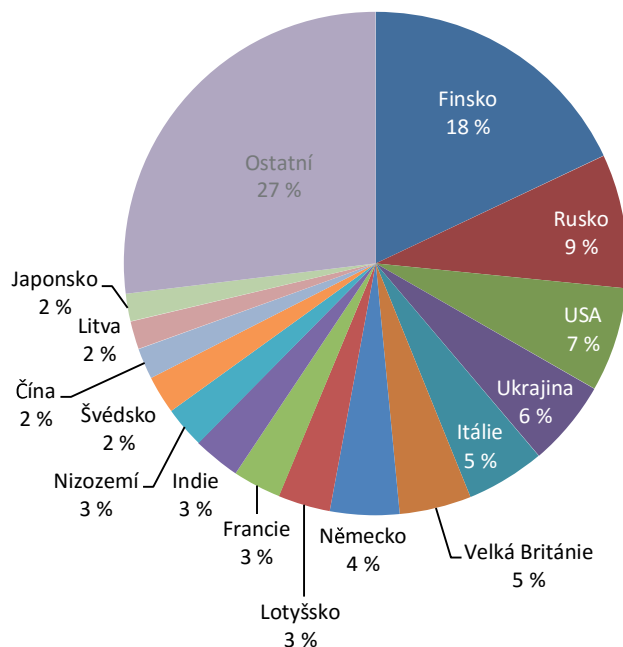


Obr. 3: Schéma fungování přeshraniční elektronické identifikace

Úspěch jednotlivých prostředků elektronické identifikace bude značně záležet na počtu a atraktivitě služeb, ke kterým bude možné se daným prostředkem přihlásit. Současné občanské průkazy s čipem bohužel nabídl jen možnost uložení kvalifikovaného certifikátu pro elektronický podpis. Díky nesplnění požadavků na tzv. důvěryhodné prostředky (QESCD) dle eIDAS současné průkazy nemohou být použity pro vytváření kvalifikovaného elektronického podpisu dle eIDAS.

eID podle Estonců

Díky zavedení principu vzájemného uznávání na českém trhu budou moci působit nejen tuzemští, ale i zahraniční poskytovatelé identit (tzv. IDP). Nejhlasitěji se v této souvislosti o své slovo hlásí Estonsko. V prosinci 2014 představilo tzv. projekt e-Residency umožňující stát se za poplatek 100 EUR – virtuálním občanem této pobaltské země, který však vlastní reálný



Obr. 4: Státy s nejvyšším počtem žadatelů o e-Residency

přukaz totožnosti splňující požadavky kladené na vysokou úroveň záruky dle eIDAS. Zatím o toto virtuální občanství požádalo na 13 000 občanů z celkem 133 různých zemí včetně 75 Čechů. Nejvíce žadatelů přitom pochází ze sousedních zemí – Finska a Ruska (viz obr. 4).

Estonské virtuální občanství je díky možnosti on-line založení firmy výhodné především pro ty, kteří v této zemi chtějí začít podnikat. Držitel e-Residency zároveň mohou on-line podávat daňové přiznání. Díky ověření přes zabezpečený on-line chat by od podzimu letošního roku mělo být možné i on-line založení účtu v bance.

V budoucnu bude možné využít estonské eID rovněž v rámci přeshraniční identifikace dle nařízení eIDAS. Jen tak je mož-

né, že např. Češi se budou přihlašovat ke slovenské elektronické schránce nikoli pomocí českého, ale estonského občanského průkazu. Vivat jednotný digitální trh.

Závěr

Od eIDAS si nelze slibovat automatické zpřístupnění elektronické identifikace široké veřejnosti. Nařízení totiž v mnoha oblastech dává příležitost, ale nenařizuje. Bude záležet jen na členských státech, jak se k záležitosti eID postaví.

Zkušenosti z rozsáhlých pilotních projektů včetně STORK jen zdůraznily, že bez dostatečně atraktivních služeb se elektronické občanské průkazy stanou jen nevyužívaným „nosičem“, jako je tomu nyní bohužel v České republice. V tomto ohledu nelze vkládat do eIDAS naděje, neboť toto nařízení nejen, že nezavádí povinnost elektronizace služeb veřejné správy, ale ani neukládá členským státům povinnost nějaké elektronické prostředky vydávat.

Pro masové rozšíření elektronické identifikace a zlepšení e-Governmentu bude nutné, aby stát spolupracoval se soukromým sektorem a občané mohli využít jednoho nástroje

nejen k přihlašování k elektronickým službám veřejné správy, ale rovněž k co největšímu množství dalších služeb – elektronickým obchodům, komunitním portálům nebo pro objednání k lékaři.

Pro Českou republiku by bylo chybou se spoléhat jen na občanské průkazy. Zkušenosti např. z Rakouska totiž ukázaly, že většina obyvatel dává přednost mobilní identifikaci, kterou lze snadno využít i ve stále rozšiřnějších mobilních telefonech či tabletech.



Jiří Průša
jiri.prusa@nic.cz

Mgr. Jiří Průša



univerzity Praha. V současné době pracuje ve sdružení CZ.NIC, kde má na starosti realizaci projektů s Evropskou komisí včetně projektu STORK 2.0, e-SENS a CZ.PEPS. Zároveň je členem pracovních skupin Evropské komi-

POUŽITÉ ZDROJE

- [1] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. Dostupné na WWW <<http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910>>.
- [2] Prováděcí nařízení Komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. Dostupné na WWW <<http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32015R1501>>.
- [3] Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. Dostupné na WWW <<http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32015R1502>>.
- [4] European eGovernment and the Large Scale Pilots Projects implementing cross-border public services. Research*eu focus magazine. Lucemburk: CORDIS Unit; Publications Office of the European Union, 2012, 2012(2), 4–6. ISSN 1831-1903.
- [5] JIŘÍČEK, Zdeněk. STORK 2.0: cesta k jednotnému prostoru pro elektronickou identifikaci a autentizaci v Evropě. In: Internet ve státní správě a samosprávě (ISSS) 2014. Hradec Králové: TRIADA, spol. s r. o., 2014, 79–80.