Změny v elektronické identifikaci

přinesou spolupráci státu a soukromého sektoru

Jiří Průša

Již čtyři roky si mohou Češi požádat o elektronický občanský průkaz s čipem. Zájem veřejnosti o tento typ dokladu je však téměř nulový – v současné době jej vlastní necelých 30 000 občanů. Důvodem je nejen pětisetkorunový poplatek, ale především značně omezená funkce čipu, na který je možné uložit pouze kvalifikovaný certifikát pro elektronický podpis. Pozitivní změny vedoucí k většímu využívání elektronických občanských průkazů bychom se měli dočkat od 1. ledna 2017, kdy Ministerstvo vnitra ČR plánuje začít vydávat občanský průkaz s čipem bezplatně a zároveň v podobě tzv. Národní identifikační autority (NIA) zprovoznit infrastrukturu pro funkční elektronickou identifikaci.

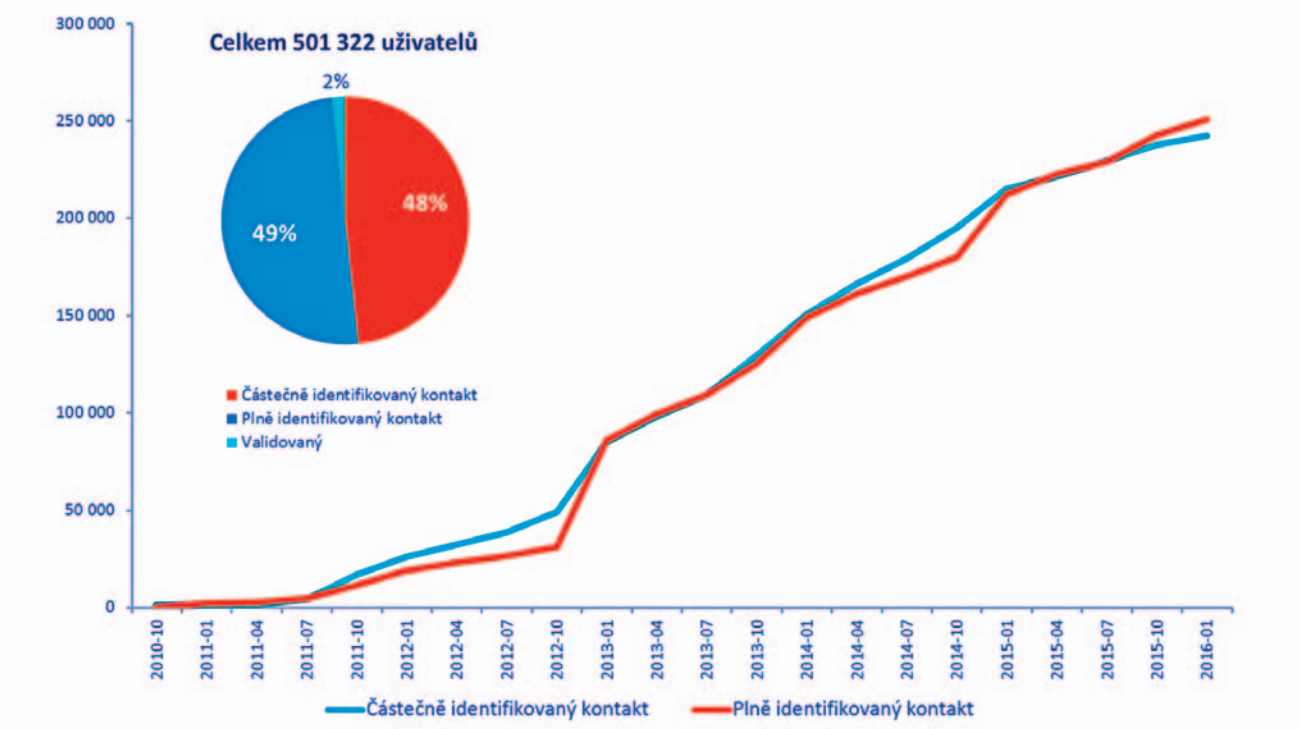
Na pozadí uvedených změn stojí především Nařízení Evropského parlamentu a Rady EU o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (tzv. eIDAS), podle kterého mají od 29. září 2018 členské státy povinnost zajistit vzájemné uznávání elektronických nástrojů (tj. především elektronických občanských průkazů). Díky zprovoznění Národní identifikační autority a projektům STORK 2.0 a CZ.PEPS by dodržení tohoto termínu neměl být pro Českou republiku problém.

	Bez čipu	S čipem	Celkem
2012	1 315 128	14 247	1 329 375
2013	1 350 773	5 933	1 356 706
2014	1 495 006	5 313	1 500 319
2015	1 863 500	3 872	1 867 372

Tab. 1: Počet vydaných občanských průkazů s čipem a bez něj. Zdroj: Ministerstvo vnitra ČR

Spolupráce státu se soukromým sektorem na elektronické autentizaci

Zkušenosti ze zemí, jako je Estonsko, Švédsko, ale i Lucembursko či Velká Británie, ukazují, že úspěšný nástroj pro elektronickou autentizaci by měl umožňovat nejen přihlášení ke službám e-Governmentu, ale



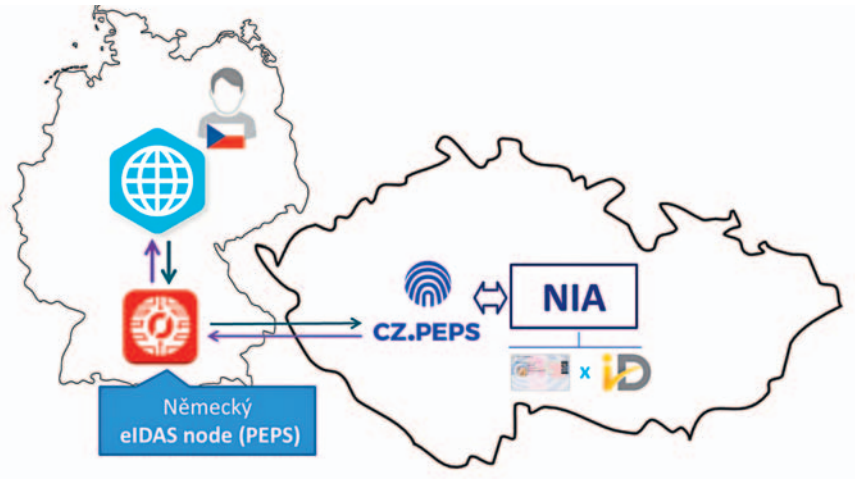
Obr. 1: Počet uživatelů mojeID. Zdroj CZ.NIC

též k elektronickým službám soukromého sektoru, jako jsou např. e-shopy, zpravodajské a komunitní portály nebo elektronické bankovnictví.

Z této myšlenky vychází rovněž budoucí technická architektura NIA, která by měla vedle elektronických občanských průkazů pracovat i s dalšími autentizačními nástroji. Mezi vážné zájemce patří služba mojeID (www.mojeid.cz), která již dnes umožňuje přihlášení ke stovkám webů a je vedle soukromého sektoru využívána i veřejnou správou – např. v rámci systému eAmbulance pro přihlášení k návštěvě u lékaře v některé z nemocnic na Vysočině. S ohledem na implementaci eIDAS je pak již nyní možné přihlášení přes mojeID

též k vybraným elektronickým službám Evropské komise.

Obr. 2: PEPS (Pan-European Proxy Services) fungují jako národní brány, které jsou v rámci Evropy vzájemně propojeny a komunikují prostřednictvím protokolu SAML 2.0. V každém státě jsou na PEPS napojeny další autentizační nástroje a systémy, nejen elektronické občanské průkazy.



Jak propojit různé eID systémy v Evropě?

Právě při zprovozňování možnosti přihlašování ke službám Evropské komise, resp. ke službě ECAS (European Commission Authentication Service), jsme v CZ.NIC prošli procesem a implementací velmi podobné té, která čeká Českou republiku v rámci eIDAS.

V této souvislosti je třeba zmínit, že nařízení eIDAS nevzniklo na „zelené louce“, ale jeho vzniku předcházel již od roku 2008 projekt STORK (Secure idenTity acrOss boRders linKed), resp. později projekt STORK 2.0, jehož cílem bylo ověřit právě možnosti přeshraniční elektronické identifikace a autentizace. Na řešení tohoto projektu se za Českou republiku podílel i CZ.NIC, a to nejen díky službě mojeID, která byla pro tento pilotní projekt vybrána jako národní identita, ale též i zprovozněním tzv. PEPS (Pan-European Proxy Services), které hrají v rámci propojování různých národních systémů klíčovou roli.

PEPS fungují jako národní brány (rozhraní), které jsou v rámci Evropy vzájemně propojeny a komunikují prostřednictvím protokolu SAML 2.0. V každém státě jsou pak na tyto PEPS napojeny další systémy a národní autentizační nástroje, kterými nemusí být v souladu s eIDAS nutně pouze elektronické občanské průkazy.

Na workshopu k CZ.PEPS uspořádaném CZ.NIC na začátku ledna se zástupci Ministerstva vnitra ČR i krajů shodli na tom, že CZ.PEPS by měl spolupracovat s Národní

mojeID

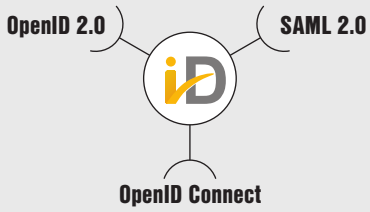
Jaromír Talíř

Služba mojeID vznikla jako reakce na několik problémů vypozorovaných v internetové komunikaci. Jedním z těchto problémů je nutnost opakovaných registrací. Uživatelé jsou s každou novou službou nuceni znovu zadávat své kontaktní informace, vytvářet si nové účty a pamatovat si nová hesla. Pokud libovolná internetová služba využije mojeID, přenesou se informace o uživateli s jeho souhlasem a odpadne tak vytváření nové sady přihlašovacích údajů. S každým přihlášením ke službě přes mojeID může navíc dojít k synchronizaci údajů o uživateli a jejich aktualizaci. Stačí, aby si uživatel své údaje aktualizoval v mojeID, a změny se zpřístupní (tzv. odpropagují) jednotlivým službám.

Dalším problémem internetu, na který mojeID reaguje, je obecně nízká bezpečnost přihlašování na jednotlivých službách. Běžná služba na internetu obvykle umožňuje pouze přihlášení přes uživatelské jméno a heslo. Hesla jsou přitom obecně považována za ne příliš bezpečný způsob přihlášení. Metody jako phishing nebo sofistikované hádání jsou nejčastější způsob, jak hesla prolomit a dostat se do cizího účtu. Proto přihlášení přes mojeID umožňuje využívat moderní mechanismy, které jsou proti těmto útokům odolné, jako SSL certifikáty nebo jednorázová hesla generovaná v mobilních telefonech. Internetová služba tak propojením s mojeID může nabídnout vyšší zabezpečení procesu ověření totožnosti uživatele.

Za službou mojeID stojí správce domény CZ.NIC, nezávislá organizace, která v ČR provozuje kritické systémy pro fungování internetu. Vedle mojeID nabízejí alternativní řešení zmíněných problémů také některé zahraniční služby, jako Google nebo Facebook. Oproti nim má mojeID zásadní výhodu v ověřování vložených údajů. Při registraci je kontrolována e-mailová adresa, telefonní číslo a poštovní adresa uživatele zasláním tří kódů přes e-mail, SMS a dopis. Uživatel, který tyto kódy vloží do mojeID, je označen jako ověřený, tuto informaci se může služba propojená s mojeID dozvědět.

Obdobně je ověřována každá změna těchto údajů. Je možné tímto způsobem například zabránit falešným objednávkám nebo zamezit verbálním útokům anonymních diskutérů. Kromě tohoto automatického ověření vložených údajů je možné navíc dobrovolně provést ověření totožnosti porovnáním údajů v osobním dokladu s údaji v mojeID, takzvanou validaci. Ověření totožnosti se tak přibližuje tomu, na co jsou uživatelé zvyklí například při jednání s certifikačními autoritami. Validaci lze provést na celé řadě validačních pracovišť. Kromě kanceláří CZ.NIC existují nyní tato pracoviště v každém krajském městě.



A jak mojeID vlastně funguje? Z technického hlediska řeší uvedené problémy internetové komunikace takzvanými autentizačními protokoly. Jejich smyslem je nastavit pravidla tak, aby obě strany, jak internetová služba, tak poskytovatelé identity (mojeID), měly jasný postup vzájemné komunikace. Autentizačních protokolů vzniklo v historii několik a některé z nich byly formálně standardizovány. V mojeID byly doposud implementovány tři protokoly, a to OpenID 2.0, SAML 2.0 a OpenID Connect. Pro poskytovatele služeb tak existují tři možnosti, jak se s mojeID propojit. Rozhodnutí závisí zejména na tom, zdali již některý z těchto protokolů služba implementuje třeba vůči jinému poskytovateli služeb. Pokud je například služba součástí federace akademických identit eduID, je přirozené sáhnout po protokolu SAML 2.0. Tento protokol je také využíván pro implementaci přeshraniční autentizace řešené v evropském projektu STORK a využívaném pro komunikaci národních bran (PEPS či eIDAS node) dle nařízení eIDAS. Pokud zatím služba žádný protokol neimplementuje, je asi nejlepší sáhnout po nejnovějším protokolu a tím je OpenID Connect. Jeho implementace je také ze všech podporovaných protokolů nejjednodušší. Tento protokol využívá například i Google, takže pokud již ve službě existuje propojení s účty Google, propojení s mojeID může být velice jednoduché. ■

identifikační autoritou (NIA). Koncoví uživatelé by si pak mohli v rámci NIA vybrat, zda budou chtít provést ověření své identity prostřednictvím nového občanského průkazu, nebo mojeID. Výhodou občanských průkazů přitom bude především možnost získat dle eIDAS nejvyšší stupeň důvěry. MojeID zatím disponuje tzv. značným stupněm důvěry.
V rámci podpory implementace eIDAS a dostatečné přípravy se Evropská komise rozhodla v loňském roce podpořit prostřednictvím Connecting Europe Facility (Nástroje pro propojení Evropy) zřízení národních PEPS. Za Českou republiku byl vybrán návrh předložený sdružením CZ.NIC.

V průběhu roku 2016 tak bude probíhat implementace národního řešení PEPS nazývaného dle terminologie evropského nařízení jako „eIDAS node“ (eIDAS uzel). V rámci kontraktu s Evropskou komisí pak bude CZ.NIC provoz českého národního uzlu PEPS zajišťovat až do konce roku 2019.
Evropská komise sice uvádí, že v jednom členském státě může fungovat i více než jeden uzel PEPS, v praxi je však třeba si uvědomit, že zahraniční PEPS může přesměrovávat vždy pouze na jeden konkrétní PEPS v každé zemi a koexistence více uzlů PEPS v jedné zemi tak nedává smysl a zbytečně by mohla mást konečné uživatele. Při implementaci STORK 2.0 se zároveň ukázala i značná časová náročnost, díky které musel být původně tříletý projekt o půl roku prodloužen.

Elektronická identifikace se v ČR začíná vydávat správnou cestou

Po několika letech velmi omezené funkčnosti občanských průkazů s čipem se zdá, že se Česká republika v oblasti elektronické identifikace začíná vydávat správnou cestou a nové občanské průkazy spolu se zprovozněním Národní identifikační autority zřejmě nahradí současné přihlašování prostřednictvím informačního systému datových schránek (ISDS). Na pozadí těchto změn je třeba hledat i tlak v podobě eIDAS, a to i přesto, že přeshraniční ověření uživatelů bude představovat pravděpodobně pouze malé procento uživatelů. ■

Mgr. Jiří Průša

Autor článku se dlouhodobě věnuje problematice evropského eGovernmentu a ve sdružení CZ.NIC má na starost realizaci a zapojování do evropských projektů.