1038—1053

Potenciál a úskalí identifikačních služeb bankovní identity

Pavel Loutocký* – František Kasl**

Abstrakt: V rámci tohoto článku přibližujeme důvody a způsob zavedení bankovní identity v českém právu. Přestože byl potenciál pro vyšší využívání elektronických dokumentů obecně podpořen nařízením eIDAS, zejména možnosti elektronické identifikace nebyly v České republice prozatím příliš vhodně využity. Bankovní identita v tomto směru přináší příslib zásadnější změny. Potenciální uživatelské výhody jsou spojovány zejména s jednoduchostí zřízení této elektronické identity a jejího následného užívání. Přesto je vhodné upozornit na jistá úskalí, která je nutno mít na zřeteli. Naším cílem je vytyčit a analyzovat problematické aspekty fungování bankovní identity a diskutovat, jak by šlo popsané překážky eliminovat. V tomto směru je přiblíženo též technologicky inovativní řešení tzv. systému atributové autentizace a možný přínos jeho nasazení v rámci identifikačních služeb.

Klíčová slova: bankovní identita, elektronická identifikace, nařízení eIDAS, kybernetická bezpečnost, systém atributové autentizace

Úvod

Bezprecedentní zkušenosti s vynuceným režimem celospolečenského fungování v maximální míře „na dálku" z posledních dvou let zvýraznily obecné tendence stále se zvyšujícího podílu využívání moderních technologií. Klíčovým aspektem pro bezkontaktní řešení řady životních situací, ať již s orgány veřejné moci, bankami či pojišťovnami, je přitom funkční mechanismus ztotožnění jednající osoby. Přes tuto rostoucí potřebu využívat nástroje pro elektronickou identifikaci však přetrvává zásadní překážka v podobě jejich uživatelské nepřívětivosti, dále kriticky zesílená mnohostí dostupných nástrojů a nepřehledností jejich vzájemného vztahu a parametrů pro běžného uživatele.

Dlouhodobě přitom platí, že klíčovým nástrojem sloužícím k elektronické identifikaci při právním jednání je elektronický podpis, jehož existuje více typů (od „prostého" podpisu[1] až po na základě certifikovaných postupů vydaného a ověřovaného kvalifikovaného elektronického podpisu[2]). Technologie a možnosti využití elektronického podpisu byly popsány již v 70. letech 20. století. Od té doby se nástroje pro identifikaci dále vyvíjely a v současné době existuje dostatečná nabídka cenově dostupných řešení pro elektronickou identifikaci osob v zašifrované podobě.[3]

* JUDr. Pavel Loutocký, Ph.D., BA (Hons), Ústav práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: loutocky@muni.cz. ORCID: https://orcid.org/0000-0002-4965-1467. Tento článek byl zpracován za podpory Technologické agentury ČR v rámci projektu *Právní a technické prostředky pro ochranu soukromí v kyberprostoru* (TL02000398).

** JUDr. Ing. František Kasl, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: frantisek.kasl@law.muni.cz. ORCID: https://orcid.org/0000-0001-6675-9528. Tento článek byl zpracován za podpory Technologické agentury ČR v rámci projektu *Právní a technické prostředky pro ochranu soukromí v kyberprostoru* (TL02000398).

1 Viz čl. 3 odst. 10 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 a o zrušení směrnice 1999/93/ES (nařízení eIDAS).

2 Viz čl. 3 odst. 12 nařízení eIDAS.

3 Srov. LOUTOCKÝ, Pavel. eIDAS Regulation: A Step Forward? In: BALTHASAR, Alexander et al. *CEE eDem and eGov Days 2015: Independence Day: Time for a European Internet?* 2015, s. 105.

Legislativa na možnost využití této technologie však reagovala se zpožděním[4] a poměrně roztříštěně upravovala jen některé z relevantních nástrojů.[5] V rámci EU bylo významným průlomem přijetí nařízení eIDAS, které etablovalo nové mechanismy elektronické identifikace, včetně úpravy služeb vytvářejících důvěru a nástrojů pro elektronické ověření totožnosti, které jsou od elektronických podpisů koncepčně i účelem odlišné.

Jednotlivé členské státy pak využívají tohoto legislativního základu na unijní úrovni, a kromě elektronických podpisů ve smyslu nařízení eIDAS zřizují specifické způsoby identifikace, zejména v souvislosti s napojením na služby poskytované v rámci e-Governmentu, které jsou uznávány všemi členskými státy.[6] Typické je ale rovněž zavádění vlastních řešení, která jsou lokálně specifická – v rámci České republiky je takovým příkladem informační systém datových schránek. V jeho rámci se považuje datová zpráva za podepsanou (tedy držitel datové schránky je dostatečně elektronicky identifikován) v případě, že datová zpráva byla odeslána jeho jménem prostřednictvím datové schránky zřízené na jeho jméno.[7]

Spolehlivým přehledem o existujících možnostech elektronické identifikace je Portál národního bodu pro identifikaci a autentizaci (Portál NIA).[8] Tento portál umožňuje skrze napojení na NIA připojení se k elektronickým službám státu (tj. Portál občana[9]). Pro tento účel nabízí hned 7 základních možností přihlášení a identifikace.[10] Tento fakt podtrhuje, že paralelně existujících nástrojů pro elektronickou identifikaci v českém právním prostředí je značné množství,[11] což vzhledem k jejich různým parametrům a možnostem využití vytváří značně nepřehledné a uživatelsky nepřívětivé prostředí (to se pak odráží i ve značně omezeném využívání těchto možností zejména fyzickými osobami).

To je jeden z důvodů, který postupně vedl k úvahám o širším využití bankovní identity, která poskytuje *„digitální ověření totožnosti osoby pomocí bezpečnostních metod, které nabízí její elektronické bankovnictví“*.[12] V České republice disponuje na základě vlastnictví

---

4 Na úrovni Evropské unie se jednalo o směrnici Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy, Komise OSN pro mezinárodní obchodní právo (UNCITRAL) poskytla vzorové UNCITRAL Model Law on Electronic Signatures [cit. 2021-09-23]. Dostupné z: <https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures>. Česká právní úprava byla zakotvena v zákoně č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

5 K tomu více viz například v LOUTOCKÝ, Pavel. *eIDAS Regulation: A Step Forward?*, s. 105–106.

6 Viz KIROVA, Marina – EICHHOLTZER, Marie. Overview of pre-notified and notified eID schemes under eIDAS. In: *eID User Community* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS>.

7 Tomu odpovídá stávající právní úprava, kdy nastává fikce podpisu, konkrétně pak dle § 18 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, respektive úkon učiněný osobou, které byla zřízena datová schránka *„má stejné účinky jako úkon učiněný písemně a podepsaný“*. Dané potvrzuje dále rovněž například stanovisko Nejvyššího soudu ze dne 5. 1. 2017, sp. zn. Plsn 1/2015.

8 Viz Portál národního bodu pro identifikaci a autentizaci. In: *eidentita.cz* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.eidentita.cz/Home>.

9 Viz Portál občana. In: *gov.cz* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://portal.gov.cz/caste-dotazy/portal-obcana>.

10 Jedná se o možnost využít Mobilní klíč eGovernmentu, eObčanku, NIA ID (dříve „Jméno, Heslo, SMS“), IIG – International ID Gateway, I.CA identitu s kartou Starcos, mojeID, bankovní identitu či se přihlásit pomocí datové schránky. Srov. Přihlášení. In: *Portál občana*. 2021 [cit. 2021-09-23]. Dostupné z: <https://obcan.portal.gov.cz/prihlaseni>.

11 Tento úvod přitom nemá sloužit jako komplexní přehled všech aktuálně dostupných možností, ale poukázat na mnohost a nepřehlednost alternativ.

12 Viz Nejčastější dotazy ...a odpovědi na ně. In: *Bankovní identita* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://bankovni-identita.cz/nejcastejsi-dotazy/>.

bankovního účtu bankovní identitou velká část společnosti.[13] Sama o sobě bankovní identita představuje značně spolehlivou formu identifikace jednotlivce a především je její vytvoření i využívání výrazně přívětivější, jelikož zde působí konkurenční prostředí bankovního sektoru při získávání nových klientů.

Zvláště relevantním parametrem bankovní identity, který nabyl na významu v období omezení pohybu z důvodu pandemické situace, ale obecně přispívá k uživatelskému pohodlí, je možnost zřízení bankovní identity „na dálku" bez nutnosti fyzické návštěvy za účelem prvotního ověření identity.[14] Obecně je pak provázanost bankovní identity s vlastnictvím bankovního účtu předpokladem pro její rozšířené využívání, jelikož je z tohoto důvodu mnohem dostupnější než např. zřízení kvalifikovaného elektronického podpisu. V rámci tohoto článku přiblížíme tento způsob elektronické identifikace,[15] zhodnotíme jeho potenciál a rovněž identifikujeme problematické aspekty, pro které se pokusíme nastínit vhodná budoucí řešení.

1. Právní úprava a důvody zavedení bankovní identity

Právní úprava, kterou bylo založeno využití bankovní identity jako nástroje elektronické identifikace, je změnový zákon č. 49/2020 Sb.,[16] kterým došlo mimo jiné ke změně zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů (zákon o bankách) a který nabyl účinnosti dne 1. 1. 2021. Dle důvodové zprávy změnový zákon vytváří podmínky pro vznik bankovní identity, která *„představuje jednoduchou a bezplatnou formu přístupu ke službám e-Governmentu i on-line službám soukromého sektoru pro přibližně 5 milionů občanů, kteří používají internetové bankovnictví"*.[17] Zajímavostí je, že právní úprava byla iniciativou soukromých subjektů sdružených pod Českou bankovní asociací navazující na projekt pod názvem SONIA[18] (jde o základ současné služby BankID, o které pojednáváme dále).[19]

Bankovní identita se tak stala jednotným přihlašovacím nástrojem pro prokazování totožnosti s využitím elektronické identifikace, který spadá pod obecné vymezení *lex generalis* zákona č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů (zákon o elektronické identifikaci). V § 2 tohoto zákona je stanoveno, že *„[v]yžaduje-li*

---

13 V současné době se jedná o 5,5 milionů lidí. Jedná se asi o 95 % klientů, kteří touto možností disponují. Viz ibidem.

14 Viz PETERKA, Jiří. Jak překonat omezení bankovní identity? In: *Lupa.cz* [online]. 29. březen 2021 [cit. 2021-09-23]. Dostupné z: <https://www.lupa.cz/clanky/jak-prekonat-omezeni-bankovni-identity/>.

15 Dle vymezení v čl. 3 odst. 1 nařízení eIDAS je pod elektronickou identifikací myšlen *„postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu"*.

16 Zákon č. 49/2020 Sb., zákon, kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a některé další zákony.

17 Důvodová zpráva k zákonu č. 49/2020 Sb., kterým se mění zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, a zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a některé další zákony (důvodová zpráva).

18 Pro upřesnění uvádíme, že nyní BankID (dříve SONIA – SOukromoprávní NIA) slouží v rámci zřízení či ověření identity ryze v rámci soukromého sektoru, o kterém pojednáváme dále. K tomu více viz například PETERKA, Jiří. Jak se pomocí BankID (ne)přihlašuje ke službám komerčních poskytovatelů? In: *Lupa.cz* [online]. 28. červen 2021 [cit. 2021-09-23]. Dostupné z: <https://www.lupa.cz/clanky/jak-se-pomoci-bankid-ne-prihlasuje-ke-sluzbam-komercnich-poskytovatelu/>.

19 Viz O projektu. In: *Bankovní identita* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://bankovni-identita.cz/o-projektu/>.

právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace […]". Právě toto ustanovení je tak legislativním podkladem umožňujícím zavedení bankovní identity, která je pak konkrétně upravena na základě výše zmíněného změnového zákona v zákoně o bankách.

Před touto změnou bylo možné elektronické identifikace v tomto smyslu dosáhnout za pomoci elektronického občanského průkazu, který je jako součást fyzického občanského průkazu nahrán na příslušném čipu.[20] K využití elektronického občanského průkazu za tímto účelem je však nutné použít speciální čtečky[21] a specifické ověření probíhá za pomoci až šesti různých číselných kódů (BOK, IOK, DOK, PIN, QPIN, PUK).[22] Tento způsob ověření tudíž nelze označit ani za příliš uživatelsky přívětivý, ani za snadno rozšiřitelný a vítaný ze strany poskytovatelů služeb. I proto se dle našeho názoru setkáváme s velmi omezeným rozsahem faktického využívání elektronického občanského průkazu.[23] Stejně tak ostatní výše zmíněné nástroje pro elektronickou identifikaci kýžené uživatelsky přívětivé prostředí neposkytly.[24] Logickým krokem motivovaným tlakem ze soukromého sektoru tak byly snahy o nalezení jiného, uživatelsky přístupného nástroje, kterým bude možno totožnost prokazovat. Vzhledem k tomu, že elektronické bankovnictví dnes využívá většina obyvatel, tak se využití této platformy jevilo jako vhodné, a to i vzhledem k vysoké úrovni důvěry v záznamy v rámci bankovního sektoru založené tradiční striktní regulací těchto subjektů.[25]

Je významné uvést, že vedle jednoznačného prokázání identity při přístupu ke službám e-Governmentu směřuje bankovní identita výrazně šířeji, a to k tomu *„poskytovat důvěryhodné identifikační údaje osoby třetím stranám (samozřejmě se souhlasem dané osoby), vytvářet zaručené elektronické podpisy, jednoduše se přihlašovat do uživatelských účtů napříč internetem (tzv. single sign-on) nebo v budoucnu provádět i související bankovní transakce v rámci jediného nástroje, který každý aktivní klient banky již zná a umí jej bez*

---

20 K tomu více viz zákon č. 269/2021 Sb., o občanských průkazech, ve znění pozdějších předpisů.

21 Viz eObčanka. In: *eidentita.cz* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://info.eidentita.cz/eop/>.

22 Viz PETERKA, Jiří. Jaké jsou a jak fungují nové elektronické občanky? In: *Lupa.cz* [online]. 4. červenec 2018 [cit. 2021-09-23]. Dostupné z: <https://www.lupa.cz/clanky/jake-jsou-a-jak-funguji-nove-elektronicke-obcanky/>. Dále jsou další konkrétní nástroje pro elektronickou identifikaci rozebrány rovněž v PETERKA, Jiří. Český eGovernment v roce 2020: nové klíče k NIA, spam v datových schránkách i plán na jejich automatické zřizování. In: *Lupa.cz* [online]. 28. prosinec 2020 [cit. 2021-09-23]. Dostupné z: <https://www.lupa.cz/clanky/cesky-egovernment-v-roce-2020-nove-klice-k-nia-spam-v-datovych-schrankach-i-plan-na-jejich-automaticke-zrizovani/>.

23 Poměrně vehementně je propagováno „vysoké" množství vydaných elektronických občanských průkazů. Je nicméně nutno podotknout, že každý nový občanský průkaz v sobě již potřebný čip obsahuje, to však nedokládá nic o tom, kolik uživatelů reálně elektronický občanský průkaz využívá. Údaje z roku 2019 uvádí, že k potřebné aktivaci čipu přistoupil jen zlomek jejich uživatelů. Viz ZASIDKOVYČOVÁ, Ilona. Občanku s čipem má přes 650 tisíc lidí. Nově otevře dveře i do registru řidičů. In: *ČT24* [online]. 7. únor 2019 [cit. 2021-09-23]. Dostupné z: <https://ct24.ceskatelevize.cz/domaci/2727224-obcanku-s-cipem-ma-pres-650-tisic-lidi-nove-otevre-dvere-i-do-registru-ridicu>.

24 V tomto kontextu pro upřesnění uvádíme rozdíl mezi elektronickou identifikací a prokázáním totožnosti. *De facto* je možno prokázání totožnosti podřadit pod pojem elektronické identifikace, jelikož elektronickou identifikací se dle čl. 3 odst. 1 nařízení eIDAS myslí *„postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu"*, konkrétní nástroje elektronické identifikace pak souvisí dle bodu odůvodnění 16 nařízení eIDAS s danou mírou *„spolehlivosti prostředků pro elektronickou identifikaci při určování totožnosti osob, a tím poskytovat záruku, že osoba deklarující konkrétní totožnost je skutečně osobou, s níž je tato totožnost spojena"*.

25 *„Elektronické bankovnictví v Česku využívá 97 % Čechů s internetem, současně Češi mají v banky a jejich řešení co do bezpečnosti a uživatelské přívětivosti velkou důvěru."* Srov. O projektu. In: *Bankovní identita* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://bankovni-identita.cz/o-projektu/>.

problémů používat“.[26] Díky tomuto spektru funkcí pak roste její atraktivita pro jednotlivce, zvláště ve srovnání s jinak dostupnými nástroji s užším uplatněním. Ostatně vodítkem může být časté využívání bankovní identity v podobné šíři v zahraničí.[27]

Nová úprava zákona o bankách pro zajištění jednoznačné identifikace dále stanovuje bankám a zahraničním pobočkám bank v České republice (a poskytovatelům identifikačních služeb) podmínky a způsob pro přístup do základních registrů[28] tak, aby byly schopny ověřovat v konkrétní situaci potřebné údaje (a bránily tak rovněž případnému zneužívání dané identity). V rámci novelizace se tak jedná o kýžený krok vedoucí k odstranění překážek bankám při přístupu do základních registrů a souvisejících informačních systémů tak, aby mohly ověřovat taxativně vymezené údaje v souvislosti s identifikací klienta [mimo jiné pro potřeby identifikace dle zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (AML zákon)]. Mezi tyto údaje dle § 38af odst. 2 a násl. zákona o bankách spadá především jméno, příjmení, adresa místa pobytu či trvalého pobytu, datum, místo a okres narození, datum úmrtí, pohlaví, rodné číslo, státní občanství, čísla a druhy elektronicky čitelných identifikačních dokladů atp.

2. Jak bankovní identita prakticky funguje?

Bankovní identita je tedy na základě výše uvedeného nástrojem, který slouží jednak k přihlášení do internetových bankovních služeb (tato složka je využívána v bankovním sektoru již dlouhodobě), jednak nově jako nástroj elektronické identifikace umožňující online přístup do systémů veřejné správy či ke službám soukromého sektoru. Bankovní identita je uživateli zpravidla zřízena spolu se založením bankovního účtu, jako identifikační nástroj ji pak může využít na základě vlastní volby (v příslušné chvíli při přístupu do daného elektronického systému jednoduše potvrdí, že chce k tomuto účelu využít bankovní identitu a po zadání příslušných údajů pro přihlášení do internetového bankovnictví je do systému přihlášen).[29] Vlastník účtu může též identifikační funkce bankovní identity nad rámec přístupu do internetového bankovnictví za využití opt-out režimu odmítnout, respektive již zřízenou „rozšířenou“ funkci bankovní identity nechat pozastavit.[30]

V rámci nové právní úpravy bankovní identity lze identifikovat čtyři roviny jejího rozšířeného uplatnění. Jsou jimi: 1) nástroj pro přístup do portálů e-Governmentu;[31] 2) soukromoprávní poskytování identifikačních služeb;[32] 3) podklad pro nové modely identifikace

---

26 Viz KORBEL, František – KOVÁŘ, Dalibor. Právní úprava tzv. bankovní identity. *Bulletin Advokacie*. 2021, č. 4, s. 17.

27 Jako příklad lze uvést Dánsko, Švédsko, Kanadu, Indii či Estonsko. Viz Nejčastější dotazy ...a odpovědi na ně. In: *Bankovní identita* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://bankovni-identita.cz/nejcastejsi-dotazy/>.

28 Dle § 38af zákona o bankách je bance (a dalším v zákoně uvedeným subjektům) umožněn přístup do základního registru obyvatel, informačního systému evidence obyvatel, informačního systému cizinců, informačního systému evidence občanských průkazů a do informačního systému evidence cestovních dokladů.

29 Jednotlivé banky ale ke zřízení bankovní identity nepřistupují zcela unifikovaně. K tomu více viz ZMEŠKAL, Kamil. Bankovní identita je dobrý sluha. Existují ale i důvody, proč ji nechtít. In: *Lupa.cz* [online]. 19. leden 2021 [cit. 2021-09-23]. Dostupné z: <https://www.lupa.cz/clanky/bankovni-identita-je-dobry-sluha-existuji-ale-i-duvody-proc-ji-nechtit/>.

30 Viz DUOFINANCE. Co je to bankovní identita, a jaké výhody a nevýhody jsou s jejím užíváním spojené? In: *statnisprava.cz* [online]. 30. červen 2021 [cit. 2021-09-23]. Dostupné z: <https://www.statnisprava.cz/rstsp/clanky.nsf/i/co_je_to_bankovni_identita_a_jake_vyhody_a_nevyhody_jsou_s_jejim_uzivanim_spojene__21062909_05284199>.

31 Srov. § 38ab odst. 1 ve spojení s § 38ad odst. 1 a 2 zákona o bankách.

32 Srov. § 38ab ve spojení s definicí „identifikačních služeb“ v § 1 odst. 4 písm. c) zákona o bankách.

klienta dle požadavků AML zákona;[33] a 4) možnost využití jako identifikačního nástroje v rámci veřejného sektoru mimo NIA.[34] Bodům 1) a 2) se věnujeme podrobněji dále, jelikož představují hlavní složky rozšířeného potenciálu tohoto nástroje. Body 3) a 4) zmiňujeme především pro lepší orientaci ve vlastním textu zákona z důvodu značné nepřehlednosti příslušných ustanovení § 38ac a 38ad zákona o bankách. Přitom bod (3) je nutno vnímat jako pouhé neuzavření si cesty k možným alternativním modelům identifikace klienta[35] a bod 4) slouží *„pouze jako pojistka pro případ legislativní změny nastavení tzv. zaručené identity"*.[36] Z hlediska fungování bankovní identity je tudíž namístě soustředit pozornost na její využití v rámci veřejného sektoru na straně jedné a komercializační potenciál jako služby soukromému sektoru na straně druhé.

3. Nástroj pro přístup do portálů e-Governmentu

Klíčovou podmínkou pro užití bankovní identity nad rámec přihlášení do online bankovnictví nalezneme v § 38ab odst. 1 zákona o bankách. Zde je stanoveno, že pro využívání bankovní identity jako prostředku pro elektronickou identifikaci v dále popisovaných intencích „identifikačních služeb"[37] je nezbytné, aby byla vydána a používána také jako prostředek pro elektronickou identifikaci v rámci kvalifikovaného systému.[38] To znamená, že bankovní identita je v tomto případě vydávána na základě specifických podmínek ukládaných kvalifikovanému správci (kterým jsou v konkrétním případě právě jednotlivé banky). Kvalifikovaným systémem je důvěryhodné státní a akreditované soukromé prostředí, které je spravováno kvalifikovanými správci, *„a které některým poskytovatelům online služeb (dle § 18 odst. 1 ZoEI, někdy též service provideři) umožňují prostřednictvím Národního bodu pro identifikaci a autentizaci (dále „NIA") identifikovat jejich koncové zákazníky. Jelikož jde primárně o regulaci pro veřejný sektor, obecné užití komerční elektronické identifikace v soukromém sektoru ponechává ZoEI na vůli stran a nijak tuto identifikaci nereguluje."*[39] Kvalifikovaný správce je pak akreditován na základě postupu dle § 5 a násl. zákona o elektronické identifikaci[40] (musí tak naplnit nejen podmínky nařízení eIDAS, ale také v tomto případě zejména prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 eIDAS).

---

33 Srov. § 38ac zákona o bankách.

34 Srov. § 38ad odst. 1 zákona o bankách.

35 Viz s. 27 důvodové zprávy ve spojení se s. 14–15 Komplexního pozměňovacího návrhu poslankyně Barbory Kořanové ze dne 19. 11. 2019 ke sněmovnímu tisku 554 č. 3714 [cit. 2021-09-23]. Dostupné z: <https://www.psp.cz/sqw/text/orig2.sqw?idd=166177&pdf=1> (komplexní pozměňovací návrh).

36 Viz s. 15 komplexního pozměňovacího návrhu.

37 Dle § 1 odst. 4 písm. c) zákona o bankách jde o podnikatelskou činnost spočívající v poskytování elektronické identifikace, autentizace a služeb vytvářejících důvěru (dle nařízení eIDAS), jakož i souvisejících služeb, zejména poskytování nebo potvrzování osobních identifikačních údajů klienta, informací o klientovi souvisejících s jeho osobními identifikačními údaji, informací o bankovních obchodech klienta a vytváření a uchování elektronických dokumentů.

38 Jedná se o takový systém elektronické identifikace, který umožňuje poskytnutí služby národního bodu pro identifikaci a autentizaci podle zákona o elektronické identifikaci.

39 Viz KORBEL, František – KOVÁŘ, Dalibor. Právní úprava tzv. bankovní identity. *Bulletin Advokacie*. 2021, č. 4, s. 18.

40 Seznam udělených akreditací pro správu kvalifikovaného systému elektronické identifikace vede Ministerstvo vnitra České republiky na: <https://www.mvcr.cz/clanek/seznam-udelenych-akreditaci-pro-spravu-kvalifikovaneho-systemu-elektronicke-identifikace.aspx>.

Předpokladem pro širší využívání bankovní identity od dané bankovní instituce je tedy možnost jejího využívání pro přístup ke kvalifikovanému systému. Ustanovení § 38ad odst. 2 a 3 zákona o bankách přitom stanoví limity, které ve výsledku znamenají, že této funkce bankovní identity jako identifikačního nástroje lze využít pouze při přístupu do portálů e-Governmentu, respektive pouze ze strany kvalifikovaných poskytovatelů služeb, kteří jsou státním orgánem nebo orgánem územního samosprávného celku. Za klíčovou službu je zde přitom namístě považovat Portál občana, který slouží jako rozcestník do řady portálů státní správy a územních samospráv. Dále je významné, že lze bankovní identitu využít k přístupu do portálu datových schránek, portálu Moje daně, ePortálu ČSSZ, portálu eRecept či očkovacího portálu občana. Jde tedy o nástroj, který umožňuje snadný přístup k hlavním elektronickým službám veřejného sektoru. Z prvotních statistik využívání této možnosti v průběhu roku 2021 je znatelný značný zájem o přístup ke službám státu právě za pomoci bankovní identity.[41]

Vzhledem ke stále narůstajícímu počtu subjektů zapsaných na seznamu kvalifikovaných poskytovatelů (ať již jde o nemocnice, pojišťovny či vzdělávací instituce) ovšem vyvstává otázka, proč je využívání bankovní identity pro identifikaci skrze NIA takto specifikováno. Toto omezení se jeví být zvoleno v zájmu zachování přiměřenosti rizik spojených se službou bankovní identity, kterou je banka příslušným subjektům povinna poskytovat.[42] Jelikož je přístup ke zmíněným službám skrze NIA na základě bankovní identity koncipován zákonnou úpravou tak, že náklady s ním spojené jdou na vrub příslušné bankovní instituci,[43] je uvedené omezení nepřekvapivé. Nelze přehlédnout, že je tímto rozšířen okruh subjektů, kterým může banka nabízet službu bankovní identity na komerční bázi (pojišťovny, nemocnice apod.).[44] Jak bylo naznačeno výše, komerční rovina poskytování identifikačních služeb stála u samotného zrodu předmětné úpravy v podobě projektu SONIA.

4. Soukromoprávní poskytování identifikačních služeb

V této rovině se má do budoucna materializovat plný potenciál, který je s bankovní identitou spojován. Identifikační služby, dle výše zmíněné definice § 1 odst. 4 písm. c) zákona o bankách přesahují pouhé ověření identity a pokrývají nejen služby vytvářející důvěru (zejména elektronický podpis, jak rozebráno dále), ale i další související služby, ať již se jedná o informace o bankovních obchodech klienta či správu elektronických dokumentů. Za klíčový moment na trhu s těmito službami přitom platí okamžik z počátku roku 2021, kdy došlo ke sjednání společného postupu klíčových bankovních subjektů na českém trhu, jehož výsledkem je sjednocený standard bankovní identity vtělený do společně provozované entity.[45]

41 Viz ADAMCOVÁ, Pavla. Bankovní identita. Co to vlastně je a jak díky ní můžete zjistit, co o vás stát ví. In: *Aktuálně.cz* [online]. 25. květen 2021 [cit. 2021-09-23]. Dostupné z: <https://zpravy.aktualne.cz/finance/bankovni-identita-rozhovor/r~1385ea4ab4a911eb89ccac1f6b220ee8/>.

42 Viz s. 19 důvodové zprávy ve spojení se s. 16 komplexního pozměňovacího návrhu.

43 Viz s. 8 důvodové zprávy.

44 Konkrétní příklady jsou uvedeny zde: PETERKA, Jiří. Kam všude se s bankovní identitou (přes NIA) nedostanete? In: *Lupa.cz* [online]. 15. březen 2021 [cit. 2021-09-23]. Dostupné z: <https://www.lupa.cz/clanky/kam-vsude-se-s-bankovni-identitou-pres-nia-nedostanete/>. Tento článek rovněž charakterizuje kostrbatost bankovní identity v této oblasti a poměrně složité legislativní zázemí celé problematiky, jak již bylo zmiňováno výše.

45 Viz HOVORKA, Jiří – KUČERA, Petr. Bankovní identitu nabídneme společně, dohodly se banky. In: *Peníze.cz* [online].

Vůči soukromoprávním poskytovatelům služeb, kteří chtějí využít bankovní identity tak smluvně nevystupují jednotlivé banky, ale tzv. poskytovatel identifikačních služeb, tzn. subjekt dle § 38aa odst. 2 zákona o bankách. Ten je odlišný od bank (či zahraničních poboček) a je jím právnická osoba, která *„je na základě jiného právního předpisu oprávněna poskytovat identifikační služby a ve které mají podíl pouze banky nebo pobočky zahraničních bank; tyto banky nebo pobočky zahraničních bank jsou povinny zajistit, že poskytovatel identifikačních služeb bude zachovávat získané údaje v tajnosti a chránit je před zneužitím"*. Touto právnickou osobou je společnost Bankovní identita, a. s., která sdružuje v současné době deset největších bank (které jsou akcionáři této akciové společnosti).[46] Identifikační služby pro soukromé firmy a jejich klienty jsou tak poskytovány jednotně v rámci služby BankID.[47]

Využití služby BankID je mezi poskytovatelem identifikačních služeb (Bankovní identita, a. s.) a firemními zákazníky (poskytovatelé služeb využívající identifikačních služeb ve vztahu ke svým klientům či uživatelům) založeno smluvně a zpoplatněno dle platného ceníku.[48] Každý firemní zákazník je povinen uhradit jednorázový poplatek za aktivaci služby a následně využívat minimálně služby CONNECT, která zajišťuje přihlášení k firemním službám či do klientské zóny.[49] Další úroveň služeb, IDENTIFY, umožňuje získat informace pro ověření klienta či sjednání smlouvy přes internet v několika úrovních podrobnosti. Nejnovější službou je pak služba SIGN, tedy zaručený elektronický podpis (k té více níže). BankID tímto způsobem *„přináší velký potenciál jednotné identifikace zejména v oblasti finančních služeb, energetiky, telekomunikací a obecně v e-Commerce. Nabízí komfortní a jednotnou přihlašovací metodu do desítek uživatelských účtů napříč internetem (tzv. single sign-on) na základě dobrovolnosti a vlastní aktivity subjektů. Může se jednat o jednotné přístupy do různých e-shopů, internetových stránek poskytujících specifické služby nebo o zastřešení autorizace jednoduchých plateb."*[50]

Využití BankID v soukromém sektoru tedy představuje konkurenci službám jednotného přihlášení (single sign-on, zkráceně SSO[51]), kdy je přístup do aplikací či služeb třetích stran zajištěn skrze přihlášení do služby příslušného poskytovatele služby informační společnosti a uživateli tudíž odpadá potřeba spravovat množinu přihlašovacích údajů pro jednotlivé portály. Za nejvýznamnější příklady této služby platí Google Account[52] a Facebook Login,[53] kdy je zřejmé, že tito poskytovatelé těží ze svého významného tržního postavení a existující báze uživatelů. Geneze těchto služeb je pak podobná, jako geneze identifikačních služeb vázaných na bankovní identitu.

---

18. únor 2021 [cit. 2021-09-23]. Dostupné z: <https://www.penize.cz/osobni-ucty/424583-bankovni-identitu-nabidneme-spolecne-dohodly-se-banky>.

46 Viz Otázky, na které se často ptáte. In: *Bank ID* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.bankid.cz/faq>.

47 Viz Vaše digitální občanka. In: *Bank ID* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.bankid.cz>.

48 Viz Ceník. In: *Bank ID* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.bankid.cz/cenik>.

49 Srov. Smluvní dokumentace pro firmy. In: *Bank ID* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.bankid.cz/smluvni-dokumentace-pro-firmy> ve spojení s Ceník. In: *Bank ID* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.bankid.cz/cenik>.

50 Viz KORBEL, František – KOVÁŘ, Dalibor. Právní úprava tzv. bankovní identity. *Bulletin Advokacie*. 2021, č. 4, s. 22.

51 Blíže viz např. ALACA, Furkan – OORSCHOT, Paul C. Van. Comparative Analysis and Framework Evaluating Web Single Sign-on Systems. *ACM Computing Surveys*. 2020, roč. 53, č. 5.

52 Srov. Přihlašování do jiných aplikací a služeb pomocí účtu Google. In: *Nápověda Účet Google* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://support.google.com/accounts/answer/112802?>.

53 Srov. Facebook Login. In: *Facebook for Developers* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://developers.facebook.com/products/facebook-login/>.

Zahraniční autoři jako Pasquale[54] poukazují na srovnatelné problémy u poskytovatelů služeb informační společnosti a bankovních institucí vztahující se k netransparentní koncentraci podrobných údajů o profilech velké části společnosti u omezeného množství klíčových poskytovatelů služeb. Přesto zastáváme názor, že ve vztahu k bankovním institucím obecně, a specificky pak při nakládání s údaji klientů a jejich zabezpečení (mimo jiné skrze institut bankovního tajemství), je právní úpravou bankovního sektoru (včetně nové úpravy vztahující se k identifikačním službám) založena významně vyšší úroveň důvěry, zaručená transparentností a vynucená dozorovou činností České národní banky, respektive Úřadu pro ochranu osobních údajů.

Za uživatelský benefit lze též shledávat jednotný postup a koordinaci bankovních institucí, díky čemuž nedochází ke štěpení na konkurenční nástroje bankovní identity (což byla reálná hrozba v přípravné fázi před účinností změnového zákona[55]) a zvyšuje se přehlednost a dostupnost služby. Nedochází přitom dle našeho názoru k přehnané koncentraci a „monopolizaci" této služby, jelikož je nutné vnímat konkurenci ze strany výše zmíněných služeb jednotného přihlášení, ke kterým naopak BankID přináší čerstvou alternativu.

Hned druhým dechem je však namístě dodat, že sjednocený přístup přes BankID má alespoň v jednom poměrně častém případě pro koncového uživatele podobu „nejednotné jednotnosti". V případě, kdy je jednotlivec klientem více bank sdružených v subjektu Bankovní identita, a. s., pro poskytování služby BankID, musí mu být umožněno identifikovat se na portálech či službách třetích subjektů skrze kteroukoliv z bankovních identit, které má u příslušných bank aktivované. V praxi tak při volbě přihlášení skrze BankID v druhém kroku volí banku, jejíž záznam o své bankovní identitě chce pro daný účel využít, přičemž může při každém přihlášení zvolit jinou ze svých bankovních identit.[56] Samozřejmě jde v daném kontextu o pozitivum, které přispívá k uživatelské přívětivosti, současně může jít i o cestou pro odhalení možného zneužití nástroje v případě náhlé změny využívané bankovní identity.

Významnou výhodou je pak též záruka nezbytné institucionalizované úrovně důvěry v identifikační služby ve smyslu potřebné úrovně důvěry upravené v čl. 13 a násl. nařízení eIDAS. To je přitom ožehavé téma ve vztahu ke službám SSO,[57] které jsou vzhledem k tomu, ale především pro svou roli v posilování problematického profilování uživatelů stran enigmatických nadnárodních gigantů, Frigatem a Santos-Arteagem označovány za „politováníhodné nezbytnosti" (*regrettable necessities*).[58]

Podobně jako u služeb významných poskytovatelů SSO je pak potenciál snadného rozšíření mezi uživateli dán faktickou povahou „doplňku" k existujícím hlavním službám, tedy zde přístupu do online bankovnictví a využívání bankovních služeb. Tím je nejen zajištěno kritické množství uživatelů, které činí službu relevantní pro firemní klienty,

---

54 Viz PASQUALE, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge a Londýn: Harvard University Press, 2015.

55 Viz SOUČEK, Ondřej. Velké banky opět lákají menší hráče do ambiciózního projektu bankovní identity. In: *E15.cz* [online]. 13. listopad 2020 [cit. 2021-09-23]. Dostupné z: <https://www.e15.cz/byznys/technologie-a-media/velke-banky-opet-lakaji-mensi-hrace-do-ambicioziho-projektu-bankovni-identity-1375026>.

56 Viz Otázky, na které se často ptáte. In: *Bank ID* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.bankid.cz/faq>.

57 Viz například XIE, Tian et al. Exploring the Insecurity of Google Account Registration Protocol via Model Checking. In: *2019 IEEE Symposium Series on Computational Intelligence (SSCI): 2019 IEEE Symposium Series on Computational Intelligence (SSCI)*. 2019.

58 Srov. FRIGATO, Pietro – SANTOS-ARTEAGA, Francisco J. Facebook and Google as Regrettable Necessities. *International Journal of Strategic Decision Sciences (IJSDS)*. 2020, roč. 11, č. 1.

ale přináší to současně rozložení nákladů na správu a rozvoj tohoto nástroje (ve srovnání s alternativami sloužícími pouze jako nástroje pro elektronickou identifikaci). O úspěšné adopci tohoto nástroje svědčí rostoucí seznam subjektů, které této identifikační služby využívají (např. SAZKA a. s., Generali Česká pojišťovna a. s., či MallPay s. r. o.) či se k jejímu využívání připravují (např. ČEZ ICT Services, a. s., či Pražská plynárenská, a. s.).[59]

5. BankID a elektronický podpis

Z výše popsaného spektra služeb, které jsou v rámci BankID nabízeny, vyplývá, že vedle ověření identity uživatele pro přístup ke službě či portálu třetí strany (CONNECT) a případného sdílení ověřených informací o identitě uživatele (IDENTIFY) je od září 2021 poskytována služba zaručeného elektronického podpisu (SIGN).[60] Tato služba má ambici přinést do elektronické kontraktace vyšší míru důvěryhodnosti o identitě jednající osoby a slouží tedy především poskytovatelům služeb k tomu, aby snížila rizika plynoucí z možného nepřikázaného jednatelství či vadného plnění v důsledku mylného ztotožnění jednající osoby, ať již v podobě ztížené vymahatelnosti vzniklé pohledávky či potenciálním škodním nárokem poškozené osoby.

Obecně platí, že forma zachycení soukromoprávního jednání je zásadně volná,[61] zpravidla se však smluvní strany v rámci kontraktačního procesu zavazují k formě písemné. Jak upozorňuje Polčák, jedná se přitom o způsob zachycení projevu vůle, nikoliv jeho podstatu: *„Písemnost není ani projevem vůle, ale pouze jeho vnější jevovou formou. Je-li tedy vůle projevena písemně, znamená to, že její projev má formu textu, tj. slov zachycených za užití písma.*“[62] Tato forma je při elektronickém právním jednání naplněna zachycením obsahu do podoby písemného elektronického dokumentu a umožnění určení jednající osoby, veskrze za pomoci elektronického podpisu. V zásadě přitom postačuje i prostý elektronický podpis, který je nařízením eIDAS definován jako *„data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání“*.[63] Příkladem může být připojení jména k textu e-mailu (případně pak ve spojení s metadaty identifikujícími adresu odesílatele), případně ověření osoby zadávající požadavek (např. na nákup zboží) do online portálu skrze heslo zaslané na e-mail či mobilní číslo.

Problematické pro tento nejprostší způsob identifikace jednající osoby je nízká úroveň záruky skutečného ztotožnění, což může (ať již v důsledku omylu či na základě úmyslného klamavého jednání uživatele) znamenat překážku pro poskytovatele při smluvním plnění či přímo finanční újmu. I proto se postupně v soukromoprávním styku prosazují a rozšiřují nástroje pro ověření identity jednající osoby odpovídající vyšším úrovním důvěryhodnosti dle nařízení eIDAS. Část uživatelů, kteří si ze své vůle a na své náklady zřídili

---

59 Srov. Pro firmy. In: *Bank ID* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.bankid.cz/pro-firmy>.

60 Viz CHVÁTAL, Dalibor Z. Bankovní identita se rozrostla o zaručený digitální podpis „BankID SIGN“. In: *Měšec.cz* [online]. 17. září 2021 [cit. 2021-09-23]. Dostupné z: <https://www.mesec.cz/aktuality/bankovni-identita-se-rozrostla-o-zaruceny-digitalni-podpis-bankid-sign/>.

61 *„Každý má právo zvolit si pro právní jednání libovolnou formu, není-li ve volbě formy omezen ujednáním nebo zákonem.“* § 559 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

62 Viz POLČÁK, Radim. Elektronické právní jednání – změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. *Bulletin Advokacie*. 2013, roč. 2013, č. 10, s. 36.

63 Viz čl. 3 odst. 10 nařízení eIDAS.

nejdůvěryhodnější, tzv. kvalifikovaný elektronický podpis[64] (zřejmě především za účelem elektronické komunikace s veřejným sektorem[65] či přeshraniční komunikace), jej mohou využívat také pro jednoznačné ztotožnění v rámci soukromoprávního jednání. Plošný rozmach tohoto nástroje však nelze nad rámec vybraných segmentů společnosti (např. podnikatelů, advokátů či členů statutárních orgánů) příliš očekávat. Obdobně lze vyhodnotit rozšíření a uplatnění českého specifika, tzv. uznávaného elektronického podpisu,[66] který taktéž pro užití vyžaduje především proaktivní přístup jednotlivce a kroky na jeho straně směřující k prvotnímu ověření identity kvalifikovaným poskytovatelem služby.

Příslušná služba BankID SIGN dosahuje nižšího, avšak stále z hlediska důvěryhodného ověření identity jednající osoby funkčního stupně tzv. zaručeného elektronického podpisu. Zaručený elektronický podpis musí splňovat požadavky na jednoznačné spojení s podepisující osobou a umožnit její identifikaci. *„Je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a […] je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.“*[67]

BankID SIGN nedosahuje na úroveň uznávaného elektronického podpisu, nelze ji tudíž využít přímo při komunikaci s veřejnou správou,[68] což uplatnění tohoto prostředku omezuje pouze na soukromoprávní jednání. Bankovní identita, a. s., přitom v současné chvíli teprve buduje síť subjektů, u kterých bude možné BankID SIGN využít. Pro rozšíření využívání služby je přitom významné, že je pro koncové uživatele zdarma a proces získání je maximálně uživatelsky přívětivý, jelikož se váže na bankovní identity zřízené klientům sdružených bankovních institucí a chová se pro ně tudíž jako dílčí funkční rozšíření jejich interakce s online bankovnictvím.[69] Zde přitom může být do budoucna užití dále zpříjemněno skrze využívání mobilních aplikací pro přístup do online bankovnictví, které v poslední době významně nabývají na popularitě.[70] Právě v tom, že koncový uživatel může pro podpis využít údaje, které již beztak využívá při kontaktu s bankovní institucí, je namístě vnímat hlavní přednost tohoto nástroje, která může při dostatečné adopci ze strany firemních klientů vést k jeho plošnému rozšíření.

Rovněž výhledově je spíše nepravděpodobné, že by bylo možno službu BankID SIGN využít přímo pro komunikaci s veřejnou správou, jelikož BankID představuje službu poskytovatele identifikačních služeb (Bankovní identita, a. s.), která je technicky zprostřed-

64 Viz čl. 3 odst. 12 nařízení eIDAS.

65 Viz § 6 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů (zákon o službách vytvářejících důvěru), ten však ukládá pouze povinnost uznávaného elektronického podpisu pro komunikaci s veřejnoprávním podepisujícím ze strany uživatele. Na jeho základě je tak kvalifikovaný elektronický podpis pouze jednou z variant řešení.

66 Viz § 6 odst. 2 zákona o službách vytvářejících důvěru. Příkladem je elektronický podpis založený kvalifikovaným certifikátem PostSignum od České pošty, pokud je použit bez kvalifikovaného prostředku (např. USB token či čipová karta). Srov. Kvalifikované certifikáty. In: *Certifikační autorita PostSignum* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <http://www.postsignum.cz/kvalifikovane_certifikaty.html>.

67 Viz čl. 26 nařízení eIDAS.

68 Bankovní identita slouží k ověření identity uživatele přes NIA při přístupu do portálů e-Governmentu. Ke komunikaci s veřejnou správou ji tudíž lze využít nepřímo, v kombinaci s datovou schránkou, ke které umožňuje přihlášení.

69 Viz SKALKOVÁ, Olga. Smlouvu potvrdíte jako heslo do banky. Startuje Sign. In: *Peníze.cz* [online]. 16. září 2021 [cit. 2021-09-23]. Dostupné z: <https://www.penize.cz/ucty-karty/428949-smlouvu-potvrdite-jako-heslo-do-banky-startuje-sign>.

70 Srov. BACHURA, Jan. Zájem o mobilní bankovnictví raketově roste. Jaké produkty lze sjednat online přes mobilní aplikace jednotlivých bank? In: *Finparada.cz* [online]. 29. říjen 2020 [cit. 2021-09-23]. Dostupné z: <http://m.finparada.cz/6634-Zajem-o-mobilni-bankovnictvi-raketove-roste.aspx>.

kována skrze sdružené banky. I proto je v současné chvíli služba BankID SIGN sice dostupná firemním klientům, avšak stále probíhá její implementace do systémů správy bankovní identity jednotlivých bankovních institucí, a neplatí tudíž, že by byla v současné chvíli dostupná pro všechny klienty bank stojících za subjektem Bankovní identita, a. s.[71] Není vyloučeno, aby do budoucna došlo ke zvýšení úrovně elektronického podpisu poskytovaného touto cestou, ovšem pro naplnění požadavků kladených na uznávaný elektronický podpis by musely být zákonné podmínky (konkrétně zápis do seznamu kvalifikovaných poskytovatelů služeb vytvářejících důvěru pro službu vydávání kvalifikovaných certifikátů pro elektronické podpisy dle nařízení eIDAS[72]) splněny ze strany všech sdružených bank, skrze jejichž bankovní identity je služba poskytována. Přínos tohoto potenciálního vylepšení je pak umenšen i vzhledem k výše zmíněné již dnes dostupné možnosti využít bankovní identity pro přihlášení do portálu datových schránek.

Druhotnou limitací, která je však společná všem formám elektronického podpisu vyjma kvalifikovaného, je absence přeshraniční uznatelnosti. Nařízení eIDAS je založeno na myšlence vedoucí k vzájemnému uznávání elektronických podpisů v rámci členských států. Ty jsou ale uznávány až na úrovni kvalifikovaného elektronického podpisu,[73] zaručený elektronický podpis, na kterém je založeno BankID tak uznatelný bez změny rámce nařízení eIDAS nebude.

6. Přeshraniční uznávání bankovní identity a návrh digitální identity pro všechny Evropany

Zde si dovolíme cimrmanovský „úkrok stranou" a podotýkáme, že samotná bankovní identita jako prostředek pro identifikaci jedince (tedy nikoliv ve smyslu elektronického podpisu) při přístupu do portálů veřejné správy může být uznána přeshraničně ve chvíli, kdy je uznána na základě notifikace Evropské komise (dle č. 9 odst. 1 nařízení eIDAS). V současné chvíli je takto schválen pro přeshraniční uznávání jediný systém elektronické identifikace a tím je od 13. září 2019 elektronický občanský průkaz.[74] Dle našich informací pak takový krok v rámci bankovní identity není plánován.

Naopak Evropská komise zveřejnila v červnu 2021 záměr úpravy současného rámce nařízení eIDAS s cílem založit jednotnou úpravu digitální identity pro všechny občany, rezidenty a podniky v rámci EU.[75] Evropská peněženka digitální identity má být pro každý subjekt ústředním prvkem této plně přeshraniční struktury pro důvěryhodnou a bezpečnou správu identit. Ta je přitom připravována jako nástroj s funkcemi, které se překrývají

71 Viz CHVÁTAL, Dalibor Z. Bankovní identita se rozrostla o zaručený digitální podpis „BankID SIGN". In: *Měšec.cz* [online]. 17. září 2021 [cit. 2021-09-23]. Dostupné z: <https://www.mesec.cz/aktuality/bankovni-identita-se-rozrostla-o-zaruceny-digitalni-podpis-bankid-sign/>.

72 Viz Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru. In: *mvcr.cz* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx>.

73 Viz čl. 6 a čl. 27 odst. 3 nařízení eIDAS.

74 Viz KIROVA, Marina – EICHHOLTZER, Marie. Overview of pre-notified and notified eID schemes under eIDAS. In: *eID User Community* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS>.

75 Viz VLKOVA, Natalie. Komise navrhuje důvěryhodnou a zabezpečenou digitální identitu pro všechny Evropany. In: *Czech Republic – European Commission* [online]. 3. červen 2021 [cit. 2021-09-23]. Dostupné z: <https://ec.europa.eu/czech-republic/news/210603_safe_digital_identity_cs>.

s bankovní identitou, ať již jde o ztotožnění, poskytnutí údajů k identifikaci subjektů či podepisování elektronických dokumentů. Byť je přijetí a vlastní implementace tohoto rámce zatím značně vzdálená, předpokládáme, že pokud by skutečně došlo k jejímu plnohodnotnému zavedení, alternativní nástroje elektronické identifikace ztratí většinu prostoru pro uplatnění. Tento předpoklad lze do značné míry vztáhnout i na bankovní identitu, včetně služby BankID, která ovšem paradoxně vzhledem k provázanosti s primární funkcí nástroje pro zpřístupnění a správu služeb online bankovnictví a z ní plynoucích výhod nad alternativními nástroji čistě pro elektronickou identifikaci může přetrvat i vedle evropské digitální identity. Vzhledem ke službě BankID to však do značné míry závisí na dosud nespecifikovaném modelu financování provozu evropské digitální identity, respektive její budoucí české implementace. Jelikož je předvídána bezplatnost pro koncové uživatele,[76] lze očekávat, že bude zvolen podobný přístup jako u bankovní identity, tedy odlišný model financování pro užití ve vztahu k veřejné správě a v rámci soukromoprávního jednání.

7. Bezpečnost a úvahy nad potenciálem atributové autentizace

V závěru našeho příspěvku bychom chtěli blíže pojednat o bezpečnostních otázkách ve spojení s technickou realizací systému elektronické identifikace za pomoci bankovní identity a předložit úvahy o možném technickém řešení vybraných problematických aspektů.

Přestože bankovní identita poskytuje poměrně jednoduše uživatelsky přístupný způsob identifikace, nelze ignorovat potenciální rizika, která mohou při využití tohoto nástroje nastat. V případě (faktického) pochybení náležitého ověření není příliš pochyb o rozsahu odpovědnosti, která připadá příslušné bankovní instituci provozující příslušný nástroj elektronické identifikace.[77]

Z technologického hlediska je přitom namístě uvést, že architektura systému bankovní identity není zpravidla koncipována pro naplnění nejvyšších bezpečnostních standardů, respektive vyjma validace skrze mezinárodně uznávané certifikáty nedochází k notifikaci ověření úrovně zabezpečení (což pro srovnání platí u výše zmíněného elektronického občanského průkazu, který je však i z důvodu maximální úrovně zabezpečení uživatelsky značně nepřívětivý). Samotná absence hardwarového nosiče bankovní identity přitom není překážkou, jelikož nástroje elektronické identity fungující na softwarové bázi pro mobilní zařízení (bez nutnosti využívání specifických hardwarových nosičů či čteček) byly ověřeny a schváleny Komisí.[78] Nemusel by to tedy být problém ani pro bankovní identitu.

---

76 Viz RINALDI, Gian Marco – BRESCHI, Marta. Proposal to amend the eIDAS regulation: New horizon for the European electronic identification. In: *Bird & Bird* [online]. červenec 2021 [cit. 2021-09-23]. Dostupné z: <http://www.twobirds.com/en/news/articles/2021/global/proposal-to-amend-the-eidas-regulation>.

77 To mimo jiné nepřímo potvrdilo rovněž rozhodnutí Soudního dvora Evropské unie – v případě, že je prokázána ztráta identifikačního nástroje (například nahlášením či objektivně zneužitím údajů), riziko ztráty pak nese bankovní instituce. Analogicky pak lze dané dle našeho názoru přenést rovněž na související zneužití bankovní identity. K charakteristikám odpovědnostnímu režimu bankovní instituce více viz rozsudek SDEU, C-287/19, 11. 11. 2020.

78 Jedná se o belgického poskytovatele Itsme. Více viz EICHHOLTZER, Marie. Belgium – Itsme. In: *eID User Community* [online]. 2020 [cit. 2021-09-23]. Dostupné z: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Belgium+-+Itsme>.

Limity bezpečnosti bankovní identity a značný potenciál zneužití skrze techniky sociálního inženýrství, jako je vishing či phishing,[79] výstižně popsal Zmeškal již s počátkem účinnosti nové úpravy.[80] V tomto směru je znepokojivým momentem užití bankovní identity jako nástroje pro přístup do portálu e-Governmentu netransparentní uzavřenost ověřování identity skrze NIA. Na jedné straně dochází k ověřování identity a toho, jestli je daný poskytovatel (bankovní) identity důvěryhodný, uživatel však může být snadno zlákán podvodným odkazem na falešný portál veřejné služby, kde po něm bude vyžadováno sdílení přihlašovacích údajů do bankovní identity. Slovy Zmeškala si přitom uživatel *„nemůže nijak ověřit, že stránka, která po něm požaduje přihlášení, je opravdu službou registrovanou v NIA jako kvalifikovaný poskytovatel služby"*.[81] Pokud se tedy potenciálnímu útočníkovi podaří uživatele zmást a přesvědčit ho o tom, že daná stránka je napojena na služby e-Governmentu (což pokládáme vzhledem k nepřehlednosti a nejednotnosti konceptu a struktury českého přístupu k e-Governmentu za poměrně snadné), má v rukou velmi účinný nástroj pro získání přístupu k plnému profilu jednotlivce, včetně jeho údajů ze základních registrů.[82]

A zde narážíme na druhý problematický aspekt související s bezpečností nástroje bankovní identity. Rozšířením funkcí bankovní identity do podoby identifikační služby dochází k propojení řady dosud oddělených databází a portálů s klíčovými údaji o jednotlivci pod jeden set přihlašovacích údajů. Případný únik přihlašovacích údajů tak ohrožuje jak aktiva jednotlivce v podobě online bankovnictví, tak citlivé údaje zpřístupnitelné skrze služby e-Governmentu (a další portály).

Zarážející je pak v tomto ohledu skutečnost, že oproti stávajícím požadavkům pro využití elektronických identifikačních prostředků, kde nástroje musely dosahovat úrovně důvěry „vysoká", je bankovní identita založena na technologických nástrojích, které dosahují „jen" úrovně „značná" (podléhají tedy nižším bezpečnostním standardům a nižšímu stupni ověření identity, jak jsme zmínili výše).[83] Tento aspekt je poměrně relevantní například ve vztahu k portálu datové schránky, ke kterému lze přistupovat za pomoci bankovní identity, ale jednotlivci lze rovněž případně datovou schránku za pomocí přihlašovacích údajů do bankovní identity zřídit,[84] i se všemi důsledky ohledně doručování písemností stran veřejné správy, které se s touto skutečností pojí.[85]

---

79 Sociální inženýrství je pojem pro podvodné jednání směřující na manipulaci s uživateli či administrátory za účelem překonání zabezpečení systému či služby. V případně vishingu se jedná o podvodné telefonní hovory zaměřené na citlivé či přihlašovací údaje, v případě phishingu se jedná o podvodné e-maily s podobným cílem. Viz NÚKIB. Upozornění na vishing zneužívající identitu bankovních institucí. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 20. duben 2021 [cit. 2021-09-23]. Dostupné z: <https://nukib.cz/cs/infoservis/hrozby/1705-upozorneni-na-vishing-zneuzivajici-identitu-bankovnich-instituci/>.

80 Viz ZMEŠKAL, Kamil. Bankovní identita je dobrý sluha. Existují ale i důvody, proč ji nechtít. In: *Lupa.cz* [online]. 19. leden 2021 [cit. 2021-09-23]. Dostupné z: <https://www.lupa.cz/clanky/bankovni-identita-je-dobry-sluha-existuji-ale-i-duvody-proc-ji-nechtit/>.

81 Zmeškal dále uvádí konkrétní příklady přihlašování například na daňový portál a několikeré přinejmenším podezřelé přesměrovávání na jiné adresy. Viz ibidem.

82 Ty jsou uvedeny taxativně v § 38af zákona o bankách.

83 K rozdílným požadavkům na tyto úrovně viz čl. 8 odst. 2 nařízení eIDAS.

84 Viz Co nabízí bankovní identita uživatelům datových schránek? In: *Datové schránky.info* [online]. 2021 [cit. 2021-09-23]. Dostupné z: <https://www.datoveschranky.info/-/co-nabizi-bankovni-identita-uzivatelum-datovych-schranek-?>.

85 Toto „ponížení" záruky bylo zavedeno na základě § 21 zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů.

Zmeškalem a dalšími formulované obavy byly posíleny březnovým incidentem, se kterým se v rámci testování bankovní identity potýkala Komerční banka.[86] *„Důvodem (dočasné blokace služby) je bezpečnostní incident spočívající v pravděpodobné záměně identity […]"* v souvislosti s osobními údaji klientů.[87] Je přitom nevyhnutelné, že systémy s hodnotnými daty budou častým cílem více či méně sofistikovaných útoků, což platilo pro bankovní systémy i v minulosti. Skrze systém identifikačních služeb na bázi bankovní identity se však rozšířením jejího uplatnění a značným nárůstem subjektů, které mohou po koncovém uživateli či po bance požadovat údaje s bankovní identitou související, výrazně rozšířilo pole zranitelnosti, které je v rámci systému bankovní identity nutné pokrýt.

Jsme si vědomi obecné nevyhnutelnosti tendencí ke koncentraci identifikačních služeb, ať již skrze bankovní identitu, služby jednotného přihlášení internetových gigantů či připravovanou evropskou digitální identitu. Sledují totiž základní ekonomické hybné síly, jsou v souladu se zájmy veřejné správy na regulaci a regulovatelnosti těchto služeb a souzní též s preferencemi uživatelů, pro které je jednotný přihlašovací portál nejpřívětivějším řešením, ke kterému sami přirozeně směřují více (např. software pro správu hesel) či méně (např. opakování stejného hesla napříč službami) sofistikovanými metodami. Uznáváme tudíž, že za těchto okolností je namístě bankovní identitu stále vítat jako pozitivní posun k uživatelsky přívětivému nástroji s vyšší úrovní zabezpečení oproti dnes běžné praxi, postaveném na službách striktně regulovaných a důvěryhodných subjektů. Současně si však dovolíme i vzhledem k výše nastíněným nedostatkům a bezpečnostním rizikům spojovaným s řešením identifikace skrze bankovní identitu nastínit možný další technologický stupeň, díky kterému lze uvažovat alespoň o částečném zmírnění těchto hrozeb napříč řešeními pro elektronickou identifikaci.

Domníváme se, že je namístě do budoucna i v rámci identifikace a autentizace maximalizovat potenciál nepřímých, respektive odvozených údajů a připouštět přístup k přímým údajům identifikujícím či profilujícím jednotlivce skutečně pouze v situacích, kdy je to pro daného poskytovatele nezbytně nutné. V kontextu ochrany osobních údajů se o tomto procesu zpravidla hovoří jako o pseudonymizaci,[88] konkrétně pak může jít např. o využití tokenů[89] (tzn. zástupných vyjádření citlivých dat) či atributů[90] (tzn. dílčí charakteristiky reprezentovaných dat relevantní pro daný kontext). Právě omezení zpracování citlivých údajů skrze vymezené atributy (tedy za využití tzv. atributové autentizace) pokládáme za jednu ze slibných budoucích cest.[91]

---

86 Srov. Klienti Komerční banky nemohou přechodně využívat bankovní identitu. In: *Správa základních registrů* [online]. 1. březen 2021 [cit. 2021-09-23]. Dostupné z: <https://www.szrcr.cz/cs/archiv-novinek/e-identita/220-klienti-komer%C4%8Dn%C3%AD-banky-nemohou-p%C5%99echodn%C4%9B-vyu%C5%BE%C3%ADvat-bankovn%C3%AD-identitu>.

87 Viz MAŠEK, Adam. Komerční banka má dočasně zablokovanou službu poskytování elektronických identit. In: *Hospodářské noviny (HN.cz)* [online]. 1. březen 2021 [cit. 2021-09-23]. Dostupné z: <https://hn.cz/c1-66890280-komercni-banka-ma-docasne-zablokovanou-sluzbu-poskytovani-elektronickych-identit>.

88 Viz FLEGEL, Ulrich, ed. An Architectural Model for Pseudonymous and Secure Authorizations. In: FLEGEL, Ulrich (ed.). *Privacy-Respecting Intrusion Detection*. Boston, MA: Springer US, 2007.

89 Viz VAGADIA, Bharat. Data Integrity, Control and Tokenization. In: VAGADIA, Bharat (ed.). *Digital Disruption : Implications and opportunities for Economies, Society, Policy Makers and Business Leaders*. Cham: Springer International Publishing, 2020.

90 Viz LI, Jin et al. Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security*. 2018, roč. 72.

91 Viz HANSEN, Marit et al. Legal Data Protection Considerations. In: RANNENBERG, Kai – CAMENISCH, Jan – SABOURI, Ahmad (eds). *Attribute-based Credentials for Trust: Identity in the Information Society*. Cham: Springer International Publishing, 2015.

Atributová autentizace je založena na ideji, že přestože je pro potřeby identifikace či obecně ověření nutno pracovat s přímo identifikujícími údaji, cílem je s těmito údaji nakládat minimálně a pokud je to možné, pracovat jen s vydefinovanými atributy (např. do které z obecnějších kategorií jednotlivec spadá, případně zda disponuje oprávněním či parametrem, který je pro danou službu relevantní či specifický).[92] Konkrétní schémata v rámci atributové autentizace (tedy zvolené přístupy k prokázání hodnoty konkrétního atributu) tak nejsou primárně založena na ověření plné identity uživatele, ale na ověření naplnění znaků požadovaných v rámci nastaveného atributu. Dalším benefitem, který atributová autentizace nabízí, je kontrolovaná nespojitelnost jednotlivých přístupů, jelikož v rámci ověření identity se pouze prokáže prostřednictvím důvěryhodné služby, že uživatel naplňuje stanovené atributové požadavky. Pokud ale nastane potřeba zpětně odhalit jeho identitu (ať už při nejistotě daného oprávnění, pochybení systému či k navazujícímu dokazování), lze využít revokace skrze autorizovanou revokační autoritu, která je v rámci oddělení rolí odlišná od vydavatele atributů, na základě které lze údaje o konkrétním přístupu zpětně rekonstruovat.[93]

Závěr

V rámci tohoto příspěvku bylo naším cílem přiblížit čtenářům současné prostředí nástrojů pro elektronickou identifikaci, s důrazem na novou službu bankovní identity, která od letošního roku umožňuje uživatelsky přívětivý přístup do portálů e-Governmentu bankovním klientům za využití jejich přihlašovacích údajů do online bankovnictví. Popsali jsme nejen strukturu a právní úpravu tohoto nového nástroje elektronické identifikace, ale zaměřili jsme se podrobně i na identifikační služby, které jsou skrze sjednocený přístup bankovních institucí nabízeny v soukromoprávním kontextu skrze službu BankID. Snažili jsme se přitom kriticky zhodnotit silné a slabé stránky především ve srovnání s významnými existujícími (Google Account, Facebook Login) i předvídanými budoucími (evropská digitální identita) alternativami. Pozornost jsme věnovali také nedávnému rozšíření služby BankID SIGN v podobě zaručeného elektronického podpisu. Dále jsme pak diskutovali úroveň bezpečnosti bankovní identity jako nástroje pro přístup do širokého spektra portálů s citlivými údaji jednotlivce a zdůraznili odhalené limity a problematické aspekty. V závěru jsme se pak snažili nastínit možný budoucí vývoj a přínos, který by mohla mít slibná technologie atributové autentizace nejen pro bankovní identitu, ale pro nástroje elektronické identifikace obecně.

92 Viz GU, Ke – WANG, Keming – YANG, Lulu. Traceable attribute-based signature. *Journal of Information Security and Applications*. 2019, roč. 49.

93 Viz WEI, Jianghong et al. Practical Attribute-based Signature: Traceability and Revocability. *The Computer Journal*. 2016, roč. 59, č. 11.

The Promise and Pitfalls of Identification Services through Bank Identity

Pavel Loutocký (https://orcid.org/0000-0002-4965-1467) –
František Kasl (https://orcid.org/0000-0001-6675-9528)

Abstract: In this article, we present the reasons for and the way of introducing bank identity in Czech law. Although the potential for increased use of electronic documents has been generally supported by the eIDAS Regulation, in particular the possibilities of using electronic identification have not yet been well exploited in the Czech Republic. Banking identity holds the promise of more fundamental change in this respect. Potential user benefits are associated in particular with the simplicity of setting up this electronic identity and its subsequent use. Nevertheless, there are certain pitfalls to be borne in mind. Our aim is to identify and analyse the problematic aspects of the functioning of the banking identity and to discuss how the described obstacles could be eliminated. In this direction, a technologically innovative solution of the so-called attribute authentication system and the possible benefits of its deployment in the context of identification services are also presented.

Keywords: bank identity, electronic identification, eIDAS Regulation, cyber security, attribute authentication system