

UNIVERZITA KARLOVA

Právnická fakulta



Petr Pochman

**Bankovní identita a elektronická identifikace
podle AML zákona**

Diplomová práce

Vedoucí diplomové práce: prof. JUDr. Radim Boháč Ph.D.

Katedra finančního práva a finanční vědy

Datum vypracování práce (uzavření rukopisu): 30.11.2023

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 132 572 znaků včetně mezer.

V Praze dne _____

Petr Pochman

diplomant

Obsah

Úvod.....	1	
1	Potřeba identifikace osob	3
1.1	Vymezení pojmu identifikace osoby	3
1.2	Potřeba identifikace.....	3
1.3	Identifikace v historii.....	4
1.4	Prolnutí identifikace do každodenního života.....	6
2	Legislativní základ Bankovní identity.....	8
2.1	Identifikace podle AML zákona.....	8
2.2	Nařízení eIDAS	9
2.2.1	Okolnosti vzniku a přijetí nařízení eIDAS	9
2.2.2	Předmět nařízení eIDAS.....	11
2.2.3	Elektronická identifikace	11
2.2.3.1	Úrovně záruky systému elektronické identifikace	14
2.2.3.2	Oznámení a působnost systému pro elektronickou identifikaci	15
2.2.3.3	Vzájemné uznávání elektronické identifikace.....	17
2.2.3.4	Interoperabilita a spolupráce systémů elektronické identifikace.....	17
2.2.3.5	Zpětný přezkum Evropské komise.....	19
2.2.4	Postupná inkorporace nařízení eIDAS do českého právního řádu	20
2.3	Zákon o elektronické identifikaci.....	21
2.3.1	Předmět zákona o elektronické identifikaci.....	21
2.3.2	Užívané pojmy a specifické aspekty ZoEI.....	21
2.4	Zákon o bankovní identitě	25
2.4.1	Předmět zákona a podrobnosti jeho změn	25
2.4.1.1	Vybrané aspekty změny zákona o bankách.....	25
2.4.2	Dopad do AML zákona	30
2.4.3	Okolnosti přijetí ZoBI a jeho některé praktické důsledky	31
2.4.4	Proces přijetí ZoBI	32
2.5	Bankovní identita, a.s.	36
3	Elektronická identifikace a bankovní identita.....	39
3.1	Vymezení způsobu fungování systémů	39
3.1.1	Státní e-ID	39
3.1.1.1	Příklad elektronické identifikace ve státním e-ID	40
3.2	Bankovní e-ID	41
3.2.1	Příklad elektronické identifikace v Bank-ID	41

3.3	Interoperabilita státního a bankovního e-ID	42
3.3.1	Příklad využití Bank-ID při přihlašování do státem poskytovaných služeb	42
4	Alternativy bankovní identity pro elektronickou identifikaci	44
4.1	Fyzická přítomnost	44
4.2	Zprostředkovaná identifikace	45
4.3	Převzatá identifikace	45
4.4	Penny Transfer	46
4.5	Bring-your-own-identity	47
4.6	Video/fotografie	48
5	Možné využití elektronické a bankovní identifikace v budoucnosti a očekávaný vývoj legislativy	48
5.1	eDIAS 2.0	48
6	Závěr.....	53
7	Seznam používaných zkratk.....	54
8	Seznam zdrojů	55

Úvod

Cílem této diplomové práce je zhodnotit fungování elektronické bankovní identifikace v prostředí České republiky a za účelem naplnění cíle práce poskytnout jednoduché a srozumitelné vysvětlení celého procesu elektronické a bankovní identifikace, legislativního základu identifikace včetně nové možnosti identifikace podle zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (dále jako „**AML zákon**“) a vysvětlení opodstatnění takové služby a její posouzení. A to i s ohledem na plánovanou aktualizaci evropské regulace v podobě eIDAS 2.0 (podrobněji níže).

Pro dosažení cíle práce je v první části použita metoda deskripce, kde definuji používané pojmy a zasazuji identifikaci do historického kontextu, v druhé a ve třetí části práce jsou použity zejména metody analýzy a logické indukce. Dále ve čtvrté části práce používám metodu komparace, kterou porovnává aktuální stav podle platných norem s jinými možnostmi. V závěrečné páté části uplatňuji svou predikci budoucího stavu identifikace a zhodnocení praktické účinnosti a užitečnosti současné právní úpravy v rámci její aplikační praxe.

V první části se práce soustředí na samotnou identifikaci, na potřebu identifikace v každodenním životě, historické využití identifikace a postupné prolnutí potřeby identifikace do mnohých procesů v běžném životě lidí.

Druhá část podrobně popisuje legislativu relevantní pro existenci Bankovní identity. Základním právním předpisem je nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jako „**Nařízení eIDAS**“), které bylo inkorporováno do českého právního řádu, mimo jiné, v podobě zákona č. 49/2020 Sb., o bankovní identitě (dále jako „**ZoBI**“) a rovněž mělo dopad na podobu AML zákona; na jejich základě vznikla služba Bankovní identita. V této části je taktéž podrobně popsán proces přijetí ZoBI a úprav, kterým zákon prošel v samotném legislativním procesu.

V třetí části jsou popsány jednotlivé služby elektronické identifikace a bankovní identity a jejich fungování v českém a evropském právním prostředí, tj. také v situaci identifikace se zahraničním prvkem. Pro přehlednost je použití těchto služeb vždy uvedeno na několika praktických příkladech.

Ve čtvrté části je služba elektronické identifikace a Bankovní identity porovnávána s jinými prostředky pro identifikaci, a to „*penny transfer*“, „*ID scan*“, video, fyzickou přítomností nebo dalšími alternativami, pomocí nichž může dojít k identifikaci osoby, a s ohledem na

provedenou komparaci jsou posuzována možná rizika využívání Bankovní identity.

V páté části se snažím nastítnit možné budoucí a očekávané kroky ohledně elektronické a bankovní identifikace.

Bankovní identita, elektronická identifikace ale nakonec i AML je téma, které česká jurisprudencce příliš nezkoumá a byl jsem tak nucen velkou část znalostí a vědomostí získat z různých krátkých publikací na internetu, stenozáznamů a běžně dostupných právních předpisů a neopírat se tak např. o rozsáhlou judikaturu, četné komentáře či závěry různých konferencí. Uplatnitelných právních pramenů je i před zajímavost a aktuálnost tématu nedostatek. Přes tento nedostatek jsem se snažil sepsat srozumitelnou práci, která posune chápání a znalosti práva a právní vědy.

1 Potřeba identifikace osob

1.1 Vymezení pojmu identifikace osoby

Identifikaci osoby lze v mezích práva definovat jako proces porovnání (či někdy také ztotožnění) jednotlivé fyzické nebo právnické osoby s konkrétní sadou dat, jež jsou trvale zaznamenané na uznávané formě nosiče dat, například na občanském průkazu nebo výpisu z obchodního rejstříku.¹

Od obecného pojmu identifikace lze identifikaci osob odlišit jejich sadou dat k porovnání. U osobní identifikace dochází k porovnání osoby a její charakteristiky s údaji na trvalém nosiči dat o charakteristikách identifikované osoby. Tj. porovnávají se dva externí soubory dat, které jsou hmatatelné a viditelné, kdežto u obecného pojmu identifikace nedochází k porovnání dvou externích sad dat, ale k porovnání hmotné složky dat se složkou dat domnělou (např. vidíte-li předmět, spojíte jeho charakteristické prvky se svou představou o sledovaném předmětu a dedukujete, že viděný předmět je hokejka, nikoli autobus).

Dnes lze proces identifikace osob provádět za fyzické přítomnosti identifikované osoby, například na pobočce banky nebo při dopravní kontrole příslušníkem policie, nebo na dálku za pomoci techniky, například formou videopřenosu apod.

V českém právním řádu není pojem přesně identifikace definován, je pouze užíván ve svém běžném slovníkovém významu; jedná se tedy o neurčitý právní pojem. Využití pojmu identifikace lze najít zejména v AML zákoně, který vymezuje, kdy nastane povinnost identifikace a jakým způsobem k jejímu provedení dojde.²

1.2 Potřeba identifikace

Právní řád umožňuje domáhat se některých práv a povinností v případě dosažení určitého věku, získání různých osobních oprávnění či držení potřebných kvalifikací. K doložení splnění těchto atributů je nutné být schopen prokázat svou identitu. Bez identifikace osoby, která se těchto práv a povinností domáhá, nelze prokázat splnění těchto atributů, aniž by o nich bylo pochyb.

Bez možnosti identifikace osoby není např. možné ověřit, zda pan Šťastný splnil zákonem požadovanou věkovou hranici pro účast na hazardních hrách, zda je oprávněn vykonávat advokátní činnost nebo zda splnil požadavky pro výkon funkce ústavního soudce. Nástrojem pro identifikaci a ověření splnění požadovaných atributů u zde uvedených příkladů bude pro splnění věkové hranice občanský průkaz, pro výkon advokacie identifikační průkaz ČAK a pro

¹ Vlastní definice.

² § 7 a 8 AML zákona.

prokázání (alespoň jednoho) z požadavků pro výkon funkce ústavního soudce univerzitní diplom z oboru právo a právní věda.

Identifikace a rozvoj služeb poskytovaných přes internet³ jsou s ohledem na rozvoj přeshraničního trhu, a to nejenom v Evropské unii, kde platí volný pohyb (osob, kapitálu, zboží a služeb) ale i celosvětově, klíčovým prvkem při poskytování zboží a služeb, zejména u těch, u nichž platí určitá restrikce poskytování (věková hranice, umístění na sankčních seznamech aj.).

1.3 Identifikace v historii

Identifikace je proces, který je prokazatelně přítomen v lidské společnosti již od starověku a pravděpodobně i mnohem déle. Jak je vidět na níže uvedených příkladech, postupně docházelo k rozvoji identifikace, jejím zpřesňování a zkvalitňování a časem i zjednodušování. Identifikace prodělala řadu změn, které reagovaly na rozvoj technologií, potřeby společnosti nebo na bezpečnostní rizika.

Mezi jedny z nejstarších a pro nás právně relevantních řadíme identifikaci ve starověkém Římě, kde se mimo jiné používala pečeť, která měla vygravírovaný osobní emblémem či symbol spojený s konkrétní osobou (a to typicky na bronzové destičce označované *signacula*), nebo železné prsteny s pečetním kamenem, jejichž účelem byla právě identifikace. Pečeť sloužila jako znamení, které určovalo konkrétní osobu a indikovalo právní závaznost a správnost písemnosti. Pečetě bylo možné připojit k různým dokumentům, například ke smlouvám, prohlášením, jmenováním aj., ale bylo možné je použít také pro tzv. zapečetění majetku, např. amfor s vínem (paralelu v dnešním světě můžeme nalézt u zapečetění bytů policií při zajištění místa činu).⁴

Ve středověku se s rozvojem písemnictví začal pro identifikaci osoby, respektive jejího jednání využívat kombinace pečetě a podpisu, který se stal rovnocenným nástrojem autentizace dokumentů vedle pečetí. Dalším typicky středověkým prvkem identifikace byl erb a erbovní štít, který sloužil zejména k určení příslušnosti ke šlechtě nebo označení jejího vlastnictví.

S vynálezem fotografie a fotografování v první polovině 19. století došlo rozmachu identifikace osob podle podobizny. Značné využití se našlo zejména v trestním právu a kriminalistice. Již v druhé polovině 19. století vznikaly první sbírky fotografií pachatelů. V Československé republice vznikla první sbírka fotografií zločinců v roce 1925 a postupem času obsahovala více

³ Informační společnost v číslech 2022, Kapitola D: Podniky a digitální technologie [online]. Česká republika: Český statistický úřad, 2022 [cit. 23.06.2023]. Dostupné z: <https://www.czso.cz/csu/czso/informační-společnost-v-číslech-2020>

⁴ MARÁZ, Karel. *Sfragistika: studijní texty pro posluchače pomocných věd historických a archivnictví*. Masarykova univerzita, 2014. str. 13. ISBN: 978-80-210-7143-8

než deset tisíc snímků.⁵

Osobní identifikace tak, jak ji známe dnes, má své prvopočátky v 19. století, v němž došlo ke vzniku různých celonárodních či celostátních registrů, seznamů a archivů, v nichž byly zaznamenány data narození, sňatky či data úmrtí a s jejichž pomocí státy vydávaly rodné a oddací listy či různé předchůdce dnešních občanských průkazů. Tyto registry a seznamy se postupně transformovaly do dnes známého Registru obyvatel, či zkráceně ROB.

S rozvojem sociálního státu, zaměstnanosti ale zejména s precizací výběrů daní vznikla potřeba státu jednoznačně identifikovat osoby. K tomu stát využíval různé číselné řady, na území Československa byla nejprve využívána obdoba dnešního rodného čísla, v zahraničí je používána jeho obdoba *social security number* (doslova číslo sociálního pojištění), pomocí níž stát eviduje například odvody u jednotlivých obyvatel za účelem správy daní a následného výpočtu důchodu u jednotlivce. V Československu byla tato povinnost poprvé zavedena zákonem č. 29/1946 Sb., kterým se zavádějí pracovní průkazy.

Přirozeným pokračovatelem jsou plnohodnotné občanské průkazy, které v Československu zavedl zákon č. 198/1948 Sb., o občanských průkazech. Ten občanský průkaz označuje za veřejnou listinu, která je všeobecným osvědčením totožnosti osoby.⁶ Zajímavostí je, že tento zákon nestanovil povinnost mít občanský průkaz, ale pouze nárok na občanský průkaz osobám starších patnácti let; povinnost přišla až v následujících letech s vyhláškou Ministerstva vnitra.⁷

S rozvojem vědeckého poznání a moderních technologií ve 20. a na počátku 21. století došlo k výraznému kvalitativnímu posunu identifikace osob, od využití biometrických údajů po digitální identifikaci. Dnes je tak možné jednotlivé fyzické osoby identifikovat pomocí otisku prstů, DNA, skenu sítnic, systémů rozpoznání obličeje aj.

S rozšířením internetu též vznikla potřeba digitální identifikace, tj. identifikace osoby operující v prostředí internetu, „online“. V minulosti vznikla celá řada způsobů, jak osobu identifikovat (podrobněji jsou nastíněny v části 4 této práce), ale pravděpodobně jedna z nejmodernějších a technologicky nejvyspělejších je možnost identifikace a identifikace osob online je pomocí technologie *blockchain*. *Blockchain* oproti centralizovaným autoritám, jako jsou státy nebo korporace, disponuje unikátní decentralizovanou technologií, pomocí níž lze jednotlivce

⁵ STRAUS Jiří a kol. *Dějiny Československé kriminalistiky slovem i obrazem*. Praha: POLICE HISTORY, 2003, s. 102-105. ISBN: 80-86477-18-5

⁶ § 1 zákona č. 198/1948 Sb., o občanských průkazech.

⁷ § 2 zákona č. 198/1948 Sb., o občanských průkazech.

identifikovat bez potřeby třetích stran.⁸

Vedle technologie *blockchain*, která nepodléhá žádné centralizované autoritě, nemá přímou oporu v právním řádu České republiky a k jejímuž využívání se mnohé vlády staví negativně, existuje Bankovní identita, která za pomoci identifikačních údajů (jimiž disponuje banka z předešlých interakcí se svým klientem) identifikuje osobu v online prostředí při jejím jednání s třetí stranou, například státem nebo provozovatelem online hazardních her.

Jak je z výše uvedených ukázek patrné, způsob identifikace, její opodstatnění a využití se v průběhu doby měnily a tento proces neustále probíhá. Lze tak očekávat, že v budoucnu dojde k dalším posunům ve způsobech, jakými bude identifikace osob prováděna, ale i za jakým účelem bude identifikace činěna.

1.4 Prolnutí identifikace do každodenního života

Jak je zmíněno výše, identifikace osob, a to jak fyzických, tak právnických, je klíčovou složkou naší každodenní činnosti. Postupem času se stala výrazně častějším a méně nápadným aspektem našich životů, než tomu bylo v minulosti. Průvodním jevem zvyšování četnosti identifikace je neustále rostoucí počet elektronických identit v České republice.⁹

Globalizací se jednotlivcům dostává produktů a služeb, kterých v minulosti nebylo, a to nejenom z pohledu rozvoje technologií jako je internet a digitálních technologií obecně ale i rozsáhlého odstraňování mezistátních bariér, například v podobě volného pohybu osob, zboží, služeb a kapitálu v Evropské unii nebo odstranění různých cel, kvót a jiných omezení. Tyto změny mají za důsledek vznik potřeby zabezpečení těchto poměrně nových kanálů, například aby došlo k zamezení možnosti nákupu zbraní a střeliva do rukou osob bez potřebného oprávnění, došlo k zamezení přístupu k hazardním hrám v online prostředí osobám mladších 18 let apod.

Společnost, a to nejenom ta evropská, dlouhodobě směřuje k přesunu významné části svých činností do online prostředí. Tohoto jevu si lze povšimnout na namátkou vybraných segmentech jako zábavě (hry, filmy, koncerty apod.) nebo mezilidské komunikaci (různé sociální sítě), ale také na interakci s institucemi jako jsou banky, pojišťovny nebo dokonce stát.¹⁰

Jen v poslední dekádě je možné sledovat prudký nárůst počtu uživatelů internetu v České

⁸ Technologie blockchain se ovšem může významně lišit projekt od projektu.

⁹ Počet elektronických Identit občanů překonal hranici 10 milionů [online]. Česká republika: Ministerstvo vnitra České republiky, 2022 [cit. 23.06.2023]. Dostupné z: <https://www.mvcr.cz/clanek/pocet-elektronickyh-identit-obcanu-prekonal-hranici-10-milionu.aspx>

¹⁰ Towards Digital Decade targets for Europe, část Digital transformation of businesses a část Digitalization of public services [online]. Brusel: Eurostat, květen 2022 [cit. 23.06.2023]. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Towards_Digital_Decade_targets_for_Europe#Digitalisation_of_public_services

republike, a to napříč všemi věkovými skupinami.¹¹ Sledovat lze také postupnou proměnu právních řádů po celém světě, které tyto změny reflektují. Nárůst počtu uživatelů internetu s sebou nese zásadní potřebu alespoň částečné regulace online prostředí při konkrétním jednání osob, a to takové regulace, která zajistí vymahatelnost a dostupnost práva i v online prostředí ekvivalentně k tomu, jak je tomu v běžných situacích mimo internet.

V důsledku těchto společenských změn se proces identifikace tak rozšiřuje z „offline“ prostředí, z většiny známého požadavku o předložení dokladu totožnosti u bankovní přepážky nebo ztotožnění při policejní kontrole do dosud ne až tak ozkoušeného on-line prostoru, v podobě okna internetového prohlížeče v počítači, mobilním telefonu nebo tabletu vyžadujícího sadu osobních údajů, pomocí níž identifikace proběhne. Pro tuto online identifikaci se užívá pojem elektronická identifikace.

Na území České republiky je jednou z nejmodernějších a státem uznávaných možností elektronické identifikace Bankovní identita, služba vyvinutá v soukromém sektoru, která vstupuje do nedávno především státem vykonávané činnosti. Jejím cílem je zjednodušit a zautomatizovat celý proces identifikace, čímž dává dosud poměrně rigidnímu a zdlouhavému postupu možnost stát se běžným a rychlým a zůstat přitom vysoce bezpečným. Lze oprávněně říci, že se zlepšuje zabezpečení osobních dat proti jejich zneužití, zjednodušuje se přístup jednotlivců k produktům a službám, u kterých je identifikace vyžadována zákonem, a výrazně se zvyšuje dostupnost veřejnoprávních služeb pro občany. Z ekonomického pohledu tak dochází k odstranění bariér.

Umožněním elektronické identifikace za využití Bankovní identity dochází k výraznému posunu digitalizace postupů, a to jak soukromoprávních, tak veřejnoprávních, čímž se otevírá celá řada možností k zefektivnění fungování státu, ale také běžné společnosti v jejich digitální propojenosti a fungování. Dochází tak k digitalizaci státu a jím poskytovaných služeb za pomoci soukromého sektoru, resp. za pomoci bank.

¹¹ Internet používá přes 80 % obyvatel Česka [online]. Česká republika: Český statistický úřad, 2020 [cit. 23.06.2023]. Dostupné z: <https://www.czso.cz/csu/czso/internet-pouziva-pres-80-obyvatel-ceska>

2 Legislativní základ Bankovní identity

Elektronická identifikace je upravena na evropské úrovni nařízením eIDAS, které bylo pro účely elektronické identifikace a později i Bankovní identity inkorporováno do českého právního řádu zákonem č. 250/2017 Sb., o elektronické identifikaci (dále jako „ZoEI“) a ZoBI, který novelizuje zákon č. 21/1992 Sb., o bankách (dále jako „ZoB“), AML zákon, zákon č. 277/2009 Sb., o pojišťovnictví (dále jen jako „ZoP“) a zákon č. 168/1999 Sb., o pojištění odpovědnosti za újmu způsobenou provozem vozidla a o změně některých souvisejících zákonů (zákon o pojištění odpovědnosti z provozu vozidla).

2.1 Identifikace podle AML zákona

Ústředním prvkem Bankovní identity je identifikace osoby. Bankovní identita je ale založená na do té doby existujícím způsobu identifikace, který je převážně popsán v AML zákoně. Proces identifikace podle níže popsané Bankovní identity tak pro banky není nic nového a jedná se spíše o modifikaci uplatňovaného postupu, a to vzhledem k ustanovení § 2 odst. 1 písm. a) AML zákona, který banky a další úvěrové instituce označuje jako povinné osoby.

Cílem AML zákona je zabránění zneužití finančního systému k legalizaci výnosu z trestné činnosti a k financování terorismu a vytvoření podmínek pro odhalování takového jednání.¹² S ohledem na vymezený cíl a obecnou podobu celého zákona je tak třeba vnímat, že i elektronická identifikace (a to ať už státní nebo soukromá elektronická identifikace – viz níže) identifikuje osobu v sobě inherentně obsahuje využití aspektu finančního systému a svým způsobem tak nesprávná identifikace může vést k legalizaci výnosu z trestné činnosti.

AML zákon v ustanovení § 5 definuje identifikační údaje u fyzických a právnických osob a jedná se o soubor dat pomocí nichž jsme schopni jednoznačně rozpoznat jednotlivé osoby od jiných, tj. jméno a příjmení, rodné číslo, datum narození, pohlaví, pobyt a státní občanství, resp. obchodní firma, sídlo a identifikační číslo u právnických osob a v opodstatněných případech se může také jednat o telefonní číslo či údajích o zaměstnání nebo zaměstnavateli.

Zjistit výše uvedené údaje je nutné v případech, který uvádí § 7 AML zákona, kdy povinná osoba (ve smyslu AML zákona) provádí identifikaci v případě, kdy má hodnota obchodu překročit hranici 1000 EUR nebo v případech kdy se jedná podezřelý obchod ve smyslu § 6 AML zákona, vznik obchodního vztahu, nákup nebo prodej kulturních památek, předmětů kulturní hodnoty, výplat zůstatku zrušeného vkladu z vkladní knížky na doručitele, osobu oprávněnou ze životního pojištění, která není pojistníkem. Povinná osoba dle AML zákona si

¹² § 1 AML zákona

pak ve svém systému vnitřních zásad dle § 21 AML zákona může stanovit hraniční hodnotu obchodu, při které identifikuje klienta i přísnější (ne volnější), tedy, že klienta identifikuje už když hodnota obchodu dosáhne např. 10 000 EUR.

Samotná identifikace podle AML zákona je upravená primárně v § 8. V případě fyzických i právnických osob, resp. fyzických osob jednajících jejich jménem, je první identifikace prováděna za fyzické přítomnosti. Při uvážení podstaty a cíle AML zákona je identifikace za fyzické přítomnosti identifikovaného ústředním požadavkem, který je nutné dodržet a dbát na něj. Z pohledu AML zákona se jedná o základní způsob identifikace a AML zákon připouští možné derivace u navazujících, či převzatých (ve slovníkovém smyslu) identifikací.¹³

Při identifikaci fyzické osoby povinná osoba zaznamenává a ověří údaje z průkazu totožnosti včetně typu a čísla použitého dokladu, vydavatele dokladu, platnost a v případě přítomnosti fotografie provede i kontrolu shody uvedené fotografie s identifikovanou osobou. V případě právnické osoby provádí obdobnou identifikaci z dokladu o existenci takové právnické osoby, typicky výpisu z obchodního rejstříku.

Společně s obecnou identifikací je povinná osoba povinna zjistit a zaznamenat, zda identifikovaná osoba není skutečným majitelem právnické osoby, která je součástí plánovaného obchodu či zda není politicky exponovanou osobou či osoba ve vlastnické nebo řídicí struktuře klienta povinné osoby.

Jak již bylo uvedeno výše, identifikace za fyzické přítomnosti je základním způsobem identifikace a AML zákon připouští jiné možnosti postupu, a to zejména využití prostředků pro elektronickou identifikaci podle § 8a AML zákona, zprostředkovaná identifikace podle § 10 AML zákona a převzatá identifikace podle § 11 AML zákona (vše podrobněji níže).

2.2 Nařízení eIDAS

2.2.1 Okolnosti vzniku a přijetí nařízení eIDAS

Evropská unie si již v době před přijetím nařízení eIDAS uvědomovala výrazný rozvoj online prostředí s jeho neustále se rozvíjející škálou služeb a produktů, které je možné pořídit online, zároveň registrovala nedůvěru veřejnosti v online prostředí minimálně u části obyvatel EU. Evropská komise ve svém sdělení „Digitální agenda pro Evropu“ z 26. srpna 2010 označila za primární nedostatky online prostředí jeho roztříštěnost, kyberkriminalitu a nedostatečné propojení online prostředí mezi členskými státy, tedy k nedostatečné využití jednotného

¹³ HLAVINOVÁ, Markéta. § 8 [Provádění identifikace]. In: HLAVINOVÁ, Markéta, PILÍKOVÁ, Jaroslava, KABEŠ, Viktor. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. 3. vydání. Praha: C. H. Beck, 2022, s. 69.

digitálního trhu.¹⁴

Evropská unie do té doby upravovala online interakci občanů převážně selektivně bez dlouhodobě prosazované a široké koncepce a snahy využít potenciálu jednotného trhu, resp. jednotného digitálního trhu. Evropské právo v oblasti vzdálené identifikace, respektive kontrahování¹⁵ dokumentu znalo pouze elektronický podpis pomocí směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy (dále jako „směrnice ZpEP“), který se v době diskusí o nařízení eIDAS jevil jako nedostatečný pro potřeby doby. Nařízení eIDAS tak směrnici ZpEP zcela nahradilo.¹⁶

Evropská rada na základě svých závěrů z února a května 2011 vyzvala Evropskou komisi k realizaci jednotného digitálního trhu. Cílem mělo být nastolit jednotný digitální trh, který zjednoduší využívání přeshraničních online služeb a zejména zajistí existenci bezpečné elektronické identifikace a autentizace.¹⁷ Záměr Rady vycházel z čl. 114 Smlouvy o fungování Evropské unie (dále jen „SFEU“), který určuje ústřední cíl nařízení, a to odstranění překážek fungování vnitřního trhu prosazováním právních předpisů sblížující členské státy. Tento aspekt lze pozorovat již od prvních návrhů nařízení, v nichž se uplatňuje zásada vzájemného uznávání mezi jednotlivými členskými státy, aby došlo k zefektivnění jednotného digitálního trhu.¹⁸

Snahou o narovnání prostředí digitálního trhu v oblasti elektronické identifikace a jeho zpřístupnění veřejnosti v EU je také text recitálu č. 49 nařízení eIDAS, který navrhuje rovnocennost elektronického podpisu s podpisem vlastnoručním.¹⁹ V recitálu č. 63 nařízení eIDAS se zase stanovuje rovnocennost dokumentace elektronické a tištěné.²⁰

Zajímavostí je, že již nařízení eIDAS předpokládalo možné zapojení soukromého sektoru do procesu elektronické identifikace, tak jak se tomu nakonec stalo v České republice a několika dalších zemích EU.²¹ Smysl tohoto recitálu lze tak interpretovat jako snahu o co nejširší využití nástrojů podle nařízení eIDAS.

Reakcí na výše uvedené požadavky a náměty byl předložený návrh nařízení eIDAS z června 2012, který posléze prošel celým legislativním procesem Evropské unie a byl přijat a uveřejněn

¹⁴ Sdělení Evropské komise, Digitální agenda pro Evropu, 26. srpna 2010 [online] Brusel: Evropská komise, 2010 [cit. 23.06.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/cs/ALL/?uri=CELEX:52010DC0245>

¹⁵ Kontrahování je ve smyslu právního řádu a jeho pravidel určitou derivací identifikace, kdy osoba svým podpisem jedná a potvrzuje svou identitu.

¹⁶ Podle čl. 50 nařízení eIDAS se směrnice 1999/93/ES ruší s účinkem ode dne 1. července 2016.

¹⁷ Nařízení eIDAS, recitál č. 5. a 6., 28. dubna 2014 [online] Brusel 2014 [cit. 23.06.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910>

¹⁸ Tamtéž, recitál č. 14.

¹⁹ Tamtéž, recitál č. 49.

²⁰ Tamtéž, recitál č. 63.

²¹ Tamtéž, recitál č. 13.

v Úředním věstníku Evropské unie v srpnu 2014. Platnost nařízení eIDAS nastala s výjimkami 1. července 2016.²²

2.2.2 Předmět nařízení eIDAS

Nařízení eIDAS stanovuje podmínky pro využívání služby elektronické identifikace jednotlivými osobami (jak fyzickými, tak právnickými osobami), určuje členským státům povinnost oznámit své systémy elektronické identifikace Komisi a stanovuje jejich mezistátní uznávání uvnitř EU (v textu nařízení eIDAS se pro tyto účely používá pojem interoperabilita), ale také stanovuje jednotlivé úrovně záruky systémů elektronické identifikace (pojem vymezen v části 2.2.3.1 této práce).

Nařízení eIDAS vedle samotné elektronické identifikace dále určuje pravidla pro služby vytvářející důvěru, jejichž součástí je právní rámec pro elektronické podpisy, elektronické pečete, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikaci služby pro autentizaci internetových stránek. V porovnání se směrnicí ZpEP tak lze vidět výrazné rozšíření množství instrumentů a snahu o saturaci nově existujících potřeb online trhu (srov. část 2.2.1 této práce).

Nařízení eIDAS je rozděleno do tří základních částí, a to obecných ustanovení (kapitola I. nařízení eIDAS), elektronické identifikace (kapitola II.) a služeb vytvářejících důvěru (kapitola III.). Vzhledem ke svému předmětu a cíli se tato práce částí služeb vytvářejících důvěru nebude podrobně zabývat.

2.2.3 Elektronická identifikace

Nařízení eIDAS **elektronickou identifikaci** definuje jako „*postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu*“.²³ Lze si tak všimnout, že se jedná o technicky složitější a vyvinutější definici identifikace osoby oproti té uvedené v úvodu této práce, která je založena na obecném popisu definice identifikace a identifikace osoby na základě porovnání dvou typicky fyzických souborů dat (fyzicky přítomná osoba a hmotný nosič dat – občanský průkaz).

Osobní identifikační údaje jsou nařízením eIDAS definovány jako „*soubor údajů umožňující*

²² Postup v legislativním procesu Nařízení eIDAS [online]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/HIS/?uri=CELEX:32014R0910>.

²³ Nařízení eIDAS, čl. 3 bod č. 1, 28. dubna 2014 [online] Brusel 2014 [cit. 24.06.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910>.

*určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující právnickou osobu“.*²⁴

Pro identifikaci osobních údajů v elektronické podobě je třeba využít specifického **prostředku pro elektronickou identifikaci**, který je vymezen jako „*hmotná či nehmotná jednotka obsahující osobní identifikační údaje, která se používá k autentizaci pro účely on-line služby*“.²⁵

Nejčastěji užívaným prostředkem pro elektronickou identifikaci v České republice je soukromoprávní Bankovní identita (podrobněji k pojmu v části 2.5 této práce), dalším z řad veřejnoprávních prostředků pro elektronickou identifikaci jsou Mobilní klíč eGovernmentu nebo NIA ID, které jsou státem poskytované zdarma.²⁶

Jako prostředek pro elektronickou identifikaci ale dle dnešních legislativních pravidel a aplikovaných technologií nelze využít běžně fungující prostředky jako průkaz pojištění, řidičský průkaz nebo jiný užívaný identifikační průkaz, a to vzhledem k absenci obsahu osobních identifikačních údajů ve formátu (podobě) údajů potřebném pro elektronickou identifikaci. Výjimkou jsou občanské průkazy vydané po 1. červenci 2018, jež obsahují čip pro elektronickou identifikaci a lze je využít jako prostředek pro elektronickou identifikaci pomocí zvláštní čtečky karet, která umožňuje přečíst data uložená v čipu.

Vzhledem k výše uvedenému musí identifikovaná osoba nejprve prostředek pro elektronickou identifikaci někde získat a posléze mít možnost jej někde používat. Nařízení eIDAS pro tento účel zavádí pojem **system elektronické identifikace**, který definuje jako „*system pro elektronickou identifikaci na jehož základě jsou fyzickým osobám či právnickým osobám nebo fyzickým osobám zastupujícím právnické osoby vydávány prostředky pro elektronickou identifikaci*“.²⁷

Jedním ze zdrojů získání prostředku pro elektronickou identifikaci v systémech elektronické identifikace může být v případě Bankovní identity samotná banka, která disponuje osobními údaji svého klienta nebo z veřejnoprávní oblasti, např. z registru obyvatel.

Samotný proces elektronické identifikace osoby je nařízením eIDAS nazýván **autentizací**. Ta je vymezena jako „*elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě*“.²⁸ Podrobněji

²⁴ Tamtéž, čl. 3 bod 3.

²⁵ Tamtéž, čl. 3 bod 2.

²⁶ Identifikační prostředky [online] Praha [cit. 09.07.2023]. Dostupné z: <https://info.identitaobcana.cz/idp/>

²⁷ Nařízení eIDAS, čl. 3 bod č. 4, 28. dubna 2014 [online] Brusel 2014 [cit. 24.06.2023]. Dostupné z:

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910>

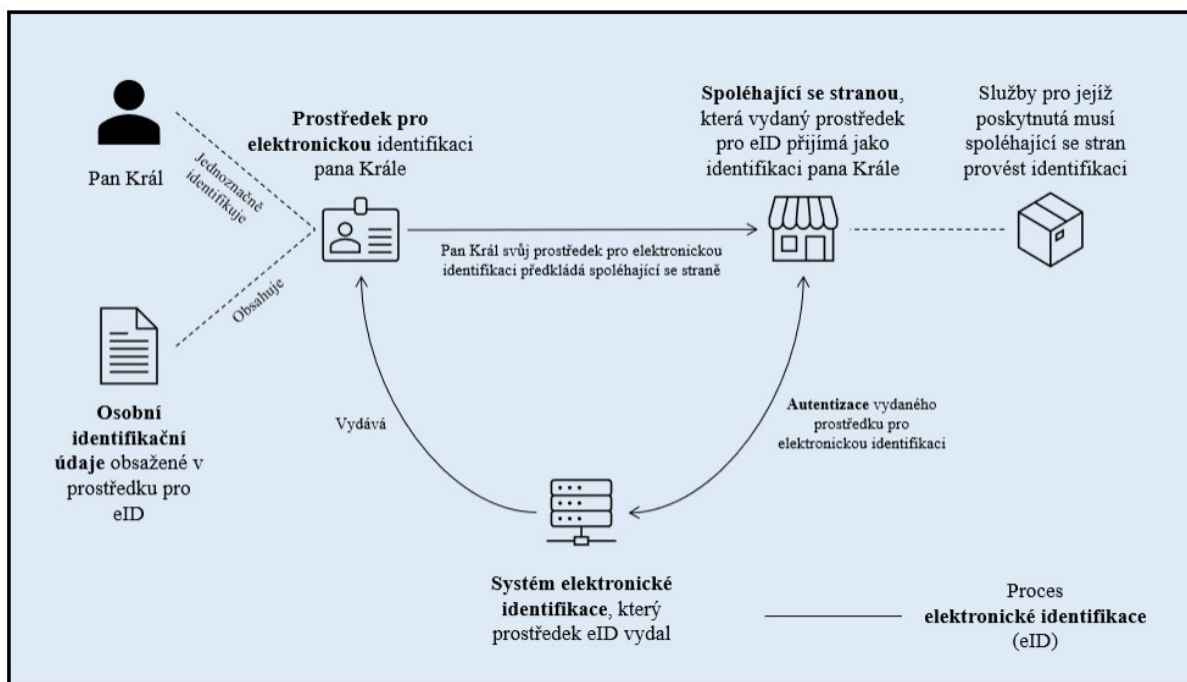
²⁸ Tamtéž, čl. 3 bod 5.

o procesu autentizace v části 3 této práce.

Posledním podstatným pojmem, který nařízení eIDAS vymezuje, je **spoléhající se strana**, jež je definována jako „*fyzická nebo právnická osoba, která se spoléhá na elektronickou identifikaci nebo službu vytvářející důvěru*“.²⁹

Celý proces lze za využití zde popsaných pojmů graficky znázornit na níže uvedeném příkladu pana Krále, který si chce zakoupit službu, pro jejíž poskytnutí musí nejprve proběhnout elektronická identifikace (eID):

²⁹ Tamtéž, čl. 3 bod 6.



2.2.3.1 Úrovně záruky systému elektronické identifikace

Systémy elektronické identifikace jsou dle nařízení eIDAS rozděleny do tří bezpečnostních úrovní podle jejich spolehlivosti. Jedná se o systémy elektronické identifikace s:

1. **nízkou úrovní záruky**, využívající prostředek elektronické identifikace, který má omezenou spolehlivost prokázání totožnosti identifikované osoby,
2. **značnou úrovní záruky**, využívající prostředek elektronické identifikace, který má značnou spolehlivost prokázání totožnosti identifikované osoby, a
3. **vysokou úrovní záruky**, využívající prostředek elektronické identifikace, který má vysokou spolehlivost prokázání totožnosti identifikované osoby.

Ve všech úrovních systému elektronické identifikace jsou pro identifikaci využívány technické specifikace, normy a postupy, jejichž účelem je snižovat rizika zneužití nebo záměny osob v jejich identifikaci.

Podrobné vymezení specifik pro jednotlivé úrovně záruky je vymezeno prostřednictvím prováděcího nařízení Evropské 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 nařízení eIDAS (dále jako „**prováděcí akt MTS**“).

Prováděcí akt MTS rozlišuje 4 základní prvky podle nichž dochází k rozčlenění procesu

elektronické identifikace na jednotlivé úseky deklarované záruky, a to:

- i. přihlášení,
- ii. správu prostředků pro elektronickou identifikaci,
- iii. autentizaci, a
- iv. řízení organizace.

Tyto základní prvky pak člení a rozpracovává dál na jednotlivé oblasti jako např. zveřejnění oznámení a informace pro uživatele, řízení bezpečnosti rizik, vedení záznamů, zařízení a personál a technické kontroly, pro které vždy stanovuje požadavky na každou jednotlivou úroveň (nízká, značná a vysoká).³⁰

Cílem rozčlenění do jednotlivých úrovní záruky je zajistit dostatečnou míru zabezpečení pro takové služby, u nichž se Evropská komise domnívá, že pro jejich online zpřístupnění je třeba vyšší míry zabezpečení. V praktické rovině se jedná zejména o služby poskytované státem nebo využití identifikace za pomoci prostředku elektronické identifikace vydaného jiným členským státem (podrobněji v části 2.2.3.3 této práce).

Zajímavostí ohledně výše zmíněného prováděcího předpisu je, že po dobu více než šesti let obsahoval chybu v české mutaci, kterou odborná veřejnost přehlížela. Chyba spočívala v možnosti prokázání elektronické identifikace fyzických osob v systému elektronické identifikace s vysokou úrovní záruky pomocí prostředku se značnou mírou záruky, tj. nižší, než by logicky měla být požadována. Dne 20. června 2022 došlo k vydání prováděcího nařízení Evropské komise (EU) 2022/960, kterým se opravuje české znění prováděcího nařízení (EU) 2015/1502, jímž se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení eIDAS, které mění oddíl 2.1.2 původního českého znění prováděcího předpisu.³¹

Vzhledem k přijetí českého ZoBI, vzniku Bankovní identity a jejímu rozmachu se lze domnívat, že ke zjištění výše uvedené chyby v českém znění došlo v důsledku přípravy přijetí ZoBI, vzniku Bankovní identity a s tím spojeným pročítání těchto norem.

2.2.3.2 Oznámení a způsobilost systému pro elektronickou identifikaci

³⁰ Prováděcího nařízení Evropské 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 nařízení eIDAS, [online] Brusel 2015 [cit. 24.06.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32015R1502&qid=1687616476454>

³¹ Prováděcí nařízení Evropské komise (EU) 2022/960 ze dne 20. června 2022, kterým se opravuje české znění prováděcího nařízení (EU) 2015/1502, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení eIDAS, [online] Brusel 2022 [cit. 24.06.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022R0960&qid=1687616476454>

S ohledem na cíle, které si EU včele s Komisí předsevzala, zařadila do nařízení eIDAS oznamovací povinnost pro všechny členské státy, které musí Komisi hlásit celou řadu informací o elektronické identifikaci uvnitř státu samotného.³²

Tato ohlašovací povinnost zajišťuje vzájemnou interoperabilitu jednotlivých soustav elektronické identifikace a přiblížení se potenciálu jednotného digitálního trhu. Ohlášením dojde k zajištění jednotnosti základních prvků celé soustavy elektronické identifikace upravené v každém členském státě EU individuálně.

Pro zajištění vzájemné interoperability systémů mezi členskými státy a zajištění parity těchto systémů nařízení eIDAS svým čl. 9 ukládá všem členským státům povinnost oznámit Komisi mimo jiné popis systému elektronické identifikace uplatňovaného v tom kterém členském státě, a to společně s jeho úrovní záruky. Popisem systému jsou míněny jeho technické specifikace tak, jak je vyžadováno celou škálou prováděcích aktů. Dále musí členské státy oznámit všechny vydavatele prostředků pro elektronickou identifikaci, režim dohledu nad vydávajícími a stranou provozující autentizaci, orgán nadaný odpovědností za uplatňovaný systém elektronické identifikace, popis postupu autentizace a informace o entitě spravující evidenci jedinečných osobních identifikačních údajů.

Veškeré tyto údaje či jejich případné změny jsou uveřejňovány Komisí v Úředním věstníku Evropské unie, počínaje uplynutím lhůty jednoho roku ode dne zveřejnění potřebných prováděcích aktů podle čl. 9 odst. 2 nařízení eIDAS.

Než však členské státy oznámí Komisi veškeré informace ve výše uvedeném rozsahu, musí systém splňovat kritéria vymezená v čl. 7 nařízení eIDAS. Těmito kritérii jsou zejména následující požadavky:

- prostředky pro elektronickou identifikaci v mezích jednotlivého systému elektronické identifikace vydává oznamující stát či jsou vydávány z jeho pověření (například soukromoprávním subjektem, který je pověřen státem k naplňování takového úkolu) nebo jsou vydávány nezávisle na státu, avšak oznamující stát tyto prostředky pro elektronickou identifikaci uznává;
- v rámci systému lze elektronickou identifikaci využít pro alespoň jednu službu z veřejného sektoru;
- systém elektronické identifikace splňuje požadavky alespoň jedné z úrovní záruk

³² Nařízení eIDAS, čl. 9, 28. dubna 2014 [online] Brusel 2014 [cit. 25.07.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910>.

- vymezených nařízením eIDAS (viz 2.2.3.1 této práce);
- oznamující stát zajistí dostupnost autentizace on-line tak, aby bylo možné potvrdit osobní údaje identifikované osoby v elektronické podobě;
 - systém elektronické identifikace splňuje podmínky určené v prováděcím aktu podle čl. 12 odst. 8 nařízení eIDAS (Spolupráce a interoperabilita).³³

2.2.3.3 Vzájemné uznávání elektronické identifikace

Nařízení eIDAS stanovuje, že pro případ služby poskytované veřejným sektorem dostupné online v členském státě, která vyžaduje elektronickou identifikaci, lze pro takovou identifikaci při procesu autentizace využít prostředek pro elektronickou identifikaci vydaný podle vnitrostátního práva jiného členského státu v případě splnění následujících podmínek:³⁴

- prostředek pro elektronickou identifikaci musel být vydán systémem elektronické identifikace, který je uveden v seznamu zveřejněném ve Úředním věstníku Evropské unie dle čl. 9 nařízení eIDAS (viz 2.2.3.2 této práce);
- úroveň záruky prostředku pro elektronickou identifikaci podle čl. 8 nařízení eIDAS musí odpovídat stejné nebo vyšší úrovni záruky stanovený subjektem, který službu provozuje;
- subjekt provozující službu musí pro danou službu používat záruku značnou nebo vysokou.

Tímto je zaručena interoperabilita jednotlivých státních soustav elektronické identifikace mezi členskými státy, a lze tak hovořit minimálně o částečném odstranění problému, který Evropská komise v Digitální agendě pro Evropu označila (viz 2.2.1 této práce).

2.2.3.4 Interoperabilita a spolupráce systémů elektronické identifikace

Požadavek nařízení eIDAS se nevztahuje jen na vzájemné uznávání prostředků k elektronické identifikaci, interoperabilitu systémů elektronické identifikace vnímá v širším smyslu. Pro zajištění vzájemné interoperability stanovuje EU v čele s Evropskou komisí v čl. 12 nařízení eIDAS kritéria pro minimální rámec.

Mezi základní prvky rámce interoperability řadíme primárně požadavky na:

- i. technologicky neutrální řešení, tj. takové řešení, které není státem, respektive jeho

³³ Prováděcí nařízení Evropské 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 [online] Brusel 2015 [cit. 09.07.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32015R1501&qid=1688910774916>

³⁴ Nařízení eIDAS, čl. 6, 28. dubna 2014 [online] Brusel 2014 [cit. 24.06.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910>

právním řádem preferované nebo dokonce výhradní (pozn. snaha o předejití monopolizace soustavy elektronické identifikace, resp. umožnění vstupu soukromého subjektu do provozování elektronické identifikace),

ii. soulad s evropskými a mezinárodními normami, a

iii. soulad zpracování osobních údajů v souladu se směrnicí 95/46/ES, respektive jejím nástupcem.³⁵

Podrobnosti a přesné vymezení samotného rámce interoperability jsou vymezeny v prováděcím aktu Evropské komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 nařízení eIDAS (dále jako „**prováděcí akt INT**“).

Prováděcí akt INT je tedy podpůrným a doplňujícím aktem, který umožňuje vzájemné uznávání prostředků elektronické identifikace, jak stanovuje čl. 6 nařízení eIDAS a jak bylo řečeno v 2.2.3.3 této práce.

Prováděcí akt INT upravuje minimální technické požadavky ohledně úrovní záruky a mapování vnitrostátních úrovní záruky oznámených prostředků pro elektronickou identifikaci vydaných v rámci oznámených systémů elektronické identifikace podle čl. 8 nařízení eIDAS, dále minimální soubor osobních dat identifikačních údajů identifikující osobu, normy zajišťující provozní bezpečnost a minimální technické požadavky na interoperabilitu (formát zpráv a uzly) a pravidla pro řešení sporů.

Nejpodstatnější částí prováděcího aktu INT je vymezení tzv. uzlů, které fungují jako centrální bod elektronické identifikace při elektronické identifikaci za použití přeshraničního prvku.

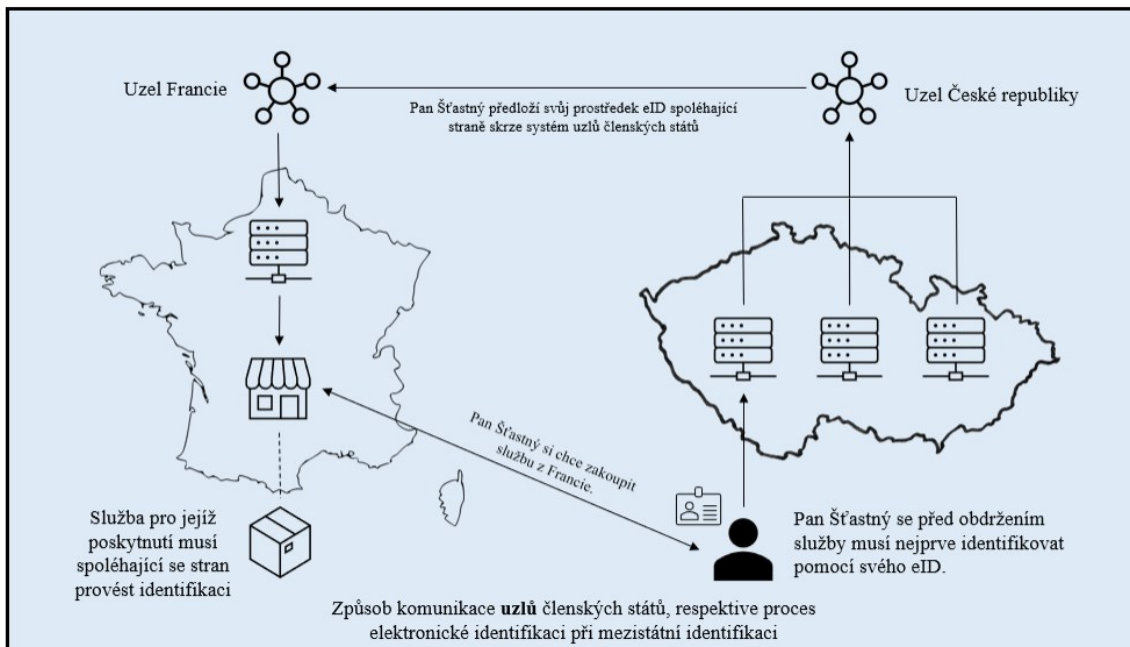
Uzel je definován v čl. 2 prováděcího aktu INT jako „*místo připojení, které je součástí architektury interoperability elektronické identifikace a je zapojeno do přeshraniční autentizace osob a které je schopno rozeznat a zpracovávat přenosy údajů nebo je předávat na jiné uzly tím, že umožňuje propojení vnitrostátní infrastruktury elektronické identifikace jednoho členského státu s vnitrostátními infrastrukturami elektronické identifikace ostatních členských států*“.³⁶ Tyto uzly lze označit jako síť národních bodů, skrze které jsou jednotlivé národní systémy elektronické identifikace propojeny se systémy elektronické identifikace

³⁵ Směrnice byla zrušena nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), tzv. GDPR.

³⁶ Prováděcí nařízení Evropské 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 [online] Brusel 2015 [cit. 09.07.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32015R1501&qid=1688910774916>

ostatních členských států.

Tyto uzly a jejich interoperabilitu lze přiblížit na níže uvedeném příkladu pana Šťastného, který chce využít služby poskytované ve Francii uvnitř jiné soustavy elektronické identifikace, kterou může využít pouze za pomoci uzlů zapojených států:



Pozn.: samotný uzel nemusí vždy být zcela samostatnou jednotkou, jak naznačuje výše uvedený zjednodušený graf, ale může se jednat o součást státního eID, jako je tomu například v České republice, kde funkci uzlu splňuje Národní identitní autorita.

2.2.3.5 Zpětný přezkum Evropské komise

Čl. 49 nařízení eIDAS ukládá Evropské komisi přezkoumat výsledky nařízení eIDAS do 1. července 2020 a podat o stavu fungování zprávu Evropskému parlamentu a Radě. Cílem je posoudit, zda s ohledem na získané zkušenosti a pokračující vývoj v oblasti technologií, práva a trhu je třeba úměrným způsobem znění nařízení eIDAS upravit, nebo je ponechat ve stavu, v jakém bylo Nařízení eIDAS přijato v roce 2014.

Zprávu Evropská komise publikovala v Úředním věstníku Evropské unie 3. června 2021, tedy skoro rok po lhůtě.³⁷

Evropská komise ve své zprávě shrnuje své cíle odstranit překážky vnitřního trhu a prosadit sblížení právních rádu členských států, aby se předešlo možným nekonzistentnostem mezi

³⁷ Úřední věstník Evropské unie [online] Brusel 2021 [cit. 24.06.2023]. Dostupné z: https://eur-lex.europa.eu/search.html?lang=cs&SUBDOM_INIT=ALL_ALL&DTS_DOM=ALL&type=advanced&DTS_SUBDOM=ALL_ALL&qid=1687642490244&LB=32014R0910&SELECT=LB_DISPLAY&sortOne=LEGAL_RELEVANCE_SORT&sortOneOrder=desc&page=2

soustavami elektronické identifikace jednotlivých států, a to rozvojem digitálního trhu, rozvojem přeshraničních veřejných služeb a zvýšením uživatelské přívětivosti pro občany a podniky v online službách. Dle závěru Evropské komise se mnohé cíle podařilo dosáhnout, avšak získané zkušenosti poukazují na různá bílá místa, například v podobě absence povinnosti oznámení, těch systémů elektronické identifikace, které nejsou zapojeny do interoperabilní sítě skrze EU (povinnost platí pouze pro systémy elektronické identifikace zapojené do interoperabilní sítě) a zejména nedostatečná motivace využití nástrojů nařízení v soukromém sektoru, jako tomu například je v České republice v případě Bankovní identity (podrobněji v části 2.5 této práce).

Evropská komise se také zaobírala závažnou problematikou „*bring-your-own-identity*“ (podrobněji v 4.5 části této práce), která ve své podstatě nutí uživatele k vytváření nových a nových identit, čímž dochází ke zvýšení rizika ztráty nebo zneužití osobních dat a samotné identity osoby. Evropská komise dále komentuje již vznikající navazující legislativní počín Evropské digitální identifikace či také e-ID, který bude reagovat na dnes již podstatně posunutou realitu online prostředí, v němž dochází k mnohonásobně většímu počtu interakcí, a tedy i elektronických identifikací.³⁸

2.2.4 Postupná inkorporace nařízení eIDAS do českého právního řádu

Nařízení eIDAS se do českého právního řádu propsalo hned do několika zákonů upravujících jeho fungování. Mezi první inkorporace můžeme zmínit zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, který primárně upravuje některé postupy poskytovatelů služeb vytvářejících důvěru, vybrané náležitosti služeb vytvářejících důvěru, působnost Digitální informační agentury (dále jako „**Agentura**“) spadající pod Ministerstvo vnitra a případné sankce za porušení. S ním byl přijat i doprovodný zákon č. 298/2016 Sb., fungující jako novela zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů.

Druhým podstatným legislativním počinem, reagujícím na nařízení eIDAS bylo přijetí ZoEI, který upravuje základní prvky využití elektronické identifikace podle nařízení eIDAS, působnost Agentury v oblasti elektronické identifikace a případné sankce za porušení zákona.

ZoEI je prvním a zároveň základním zákonem upravujícím elektronickou identifikaci v českém

³⁸ Zpráva Evropské komise Evropskému parlamentu a Radě o hodnocení nařízení eIDAS [online] Brusel 2021 [cit. 24.06.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52021DC0290&qid=1687642490244>

právním řádu. Vymezuje základní pojmy jako kvalifikovaný systém (který je přibližným ekvivalentem pojmu systém elektronické identifikace), kvalifikovaný správce, kvalifikovaný poskytovatel, národní bod (ten je ekvivalentem pojmu uzel), ale také upravuje pojmy, které nařízení eIDAS nezná, jako např. držitele prostředku pro elektronickou identifikaci nebo pověřenou osobu.

Třetí a dosud poslední výraznou inkorporací nařízení eIDAS do českého právního řádu je ZoBI, který umožnil provozování obchodní činnosti spočívající v poskytování elektronické identifikace, autentizace a služeb vytvářející důvěru včetně navazujících služeb (poskytování nebo potvrzování osobními identifikačními údaji a další) pro držitele bankovních licencí, tj. bank.³⁹

2.3 Zákon o elektronické identifikaci

2.3.1 Předmět zákona o elektronické identifikaci

ZoEI v úvodním ustanovení vymezujícím předmět zákona uvádí, že v návaznosti na nařízení eIDAS upravuje využití elektronické identifikace, působnost Agentury na úseku elektronické identifikace a přestupy na úseku elektronické identifikace.⁴⁰

Jedná se tak o zákon, který celistvě upravuje problematiku elektronické identifikace, navazuje na evropské nařízení eIDAS a provazuje prvky evropského práva do národní úpravy.

2.3.2 Užívané pojmy a specifické aspekty ZoEI

ZoEI dává na roveň možnost prokázání totožnosti dosud běžným způsobem, tedy s občankou či jiným průkazem, a využití elektronické identifikace, a to všude tam kde je to možné. Taková elektronická identifikace je ale možná pouze pomocí kvalifikovaného systému.⁴¹

Zákonodárce tak omezil možnost prokázání totožnosti tím systémem, který nesplňuje alespoň minimální požadavky nízké úrovně záruky ve smyslu čl. 8 nařízení eIDAS, tj. systém elektronické identifikace, který není propojení s uzlem členského státu (podrobněji k této problematice v části 4.5 této práce).

Český zákonodárce v procesu přijetí zákona převzal část pojmů z českého znění nařízení eIDAS, avšak také zavedl některé vlastní pojmy a kategorie, s nimiž nařízení eIDAS nepracuje, například kvalifikovaný systém, kvalifikovaný správce, kvalifikovaný poskytovatel, národní bod, akreditace, držitel či správce národního bodu.

³⁹ Ustanovení § 1 odst. 4 písm. c) ZoBI.

⁴⁰ Ustanovení § 1 ZoEI.

⁴¹ Ustanovení § 2 ZoEI.

Kvalifikovaný systém vychází z pojmu systém elektronické identifikace a je systém, který splňuje technická specifika, normy a postupy alespoň jedné z úrovní záruk (čl. 8 nařízení eIDAS), umožňuje využití služby uzlu, resp. národního bodu (čl. 12 nařízení eIDAS). Taktéž je to systém, v němž vydaný prostředek pro elektronickou identifikaci splňuje požadavky dle dané úrovně záruky (čl. 7 nařízení eIDAS). Národním specifikem je požadavek aby kvalifikovaný systém byl spravován kvalifikovaným správcem (podrobněji dále) a stanovil minimální úroveň záruky u oznámených zahraničních kvalifikovaných systémů elektronické identifikace „*v jehož rámci je vydáván a používán prostředek pro elektronickou identifikaci s úrovní záruky alespoň značnou*“.⁴²

Zákonodárce tak zpřísnil požadavek na systémy, které mohou být označeny jako kvalifikované, a vyřadil tím systémy elektronické identifikace s nízkou úrovní záruky.

Pravděpodobně se jedná o reakci na požadavek čl. 6 nařízení eIDAS, které pro uznávání prostředků elektronické identifikace vydaných v systému elektronické identifikace jiného členského státu vyžaduje alespoň úroveň záruky značné u těch služeb, které poskytuje veřejný sektor, pokud není konkrétním subjektem určeno jinak. Zákonodárce tím dosáhl faktického omezení dispozice rozhodnout o míře úrovně záruky na úrovni jednotlivých orgánů veřejné správy a těch soukromoprávních systémů elektronické identifikace, které chtějí být propojeny s uzlem, resp. národním bodem v případě, že nesplňují požadavky alespoň značné úrovně záruky.

ZoEI taktéž pracuje s pojmem systém elektronické identifikace, který zahrnuje všechny tři úrovně záruky, tak jak vymezuje nařízení eIDAS.

Kvalifikovaný správce (taktéž označován angl. pojmem „**identity provider**“) je pojem označující správce kvalifikovaného systému a dle ZoEI se může jednat o státní orgán nebo o osobu, které byla udělena příslušná akreditace pro takovou správu.⁴³

Akreditace – jak lze dovodit z předešlého pojmu, jedná se o proces, kterým musí osoba projít u Agentury v případě, že má zájem o výkon funkce kvalifikovaného správce systému elektronické identifikace. Vedle požadavků plynoucích již z nařízení eIDAS (splnění technických specifik, norem a postupů stanovených nařízením eIDAS a připojení systému elektronické identifikace k uzlu, resp. národnímu bodu) musí žadatel o akreditaci splňovat další

⁴² Ustanovení § 3 odst. 2 ZoEI.

⁴³ Ustanovení § 4 ZoEI.

povinnosti:

- i. bezúhonnost,
- ii. disponovat pojištěním odpovědnosti za škodu způsobenou při správě kvalifikovaného systému,
- iii. mít zpracován plán ukončení činnosti,
- iv. způsobilost z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob.⁴⁴

O udělení akreditace rozhoduje Agentura ve lhůtě 3 měsíců ode dne podání žádosti. V případě správy více kvalifikovaných systémů musí žadatel, resp. akreditovaná osoba žádat a prokázat splnění podmínek pro každý systém zvlášť.

Držitel je osobou, která prostředkem pro elektronickou identifikaci disponuje, tj. osoba, která o vydání prostředku pro elektronickou identifikaci požádala.⁴⁵ Zákonodárce přesnou definici držitele v zákoně neuvádí a pouze vymezuje jeho povinnosti.⁴⁶

Kvalifikovaný poskytovatel (taktéž označován angl. pojmem „**service provider**“) je dle ZoEI „*ten, kdo umožňuje prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace*“. Jedná se tak o přibližný ekvivalent pojmu spoléhající se strany používaného v nařízení eIDAS. ZoEI uvaluje na kvalifikované poskytovatele povinnost nahlásit správci národního bodu (uzlu) umožnění využití elektronické identifikace při poskytování online služby nebo jiné činnosti společně s požadovanou úrovní záruky, kterou pro danou elektronickou identifikaci vyžaduje.⁴⁷

Agentura – působnost v rámci elektronické identifikace je podle ZoEI udělena Digitální a informační agentuře.⁴⁸ Agentuře je dle ZoEI udělena povinnost plnit všechny požadavky podle čl. 9 a 10 nařízení eIDAS, zejména nahlašování systémů elektronické identifikace a případných narušení bezpečnosti Komisi. Dále Agentura vykonává dohled nad kvalifikovanými správci a poskytovateli a vede evidenci udělených akreditací, které zveřejňuje na svém webu⁴⁹ a je ze zákona kvalifikovaným správcem, který vydává prostředky pro

⁴⁴ Informace ohledně způsobilosti může pro Agenturu, na její žádost, poskytnout Policie České republiky, zpravodajská služba nebo jiný orgán.

⁴⁵ V ukázkách uvedených v této práci je držitelem ve smyslu ZoEI pan Král nebo pan Šťastný.

⁴⁶ Ustanovení § 17 ZoEI.

⁴⁷ Ustanovení § 18 ZoEI.

⁴⁸ Ustanovení § 1 písm. b) ZoEI.

⁴⁹ Seznam udělených akreditací pro správu kvalifikovaného systému elektronické identifikace [cit. 2023-7-27]. Dostupné zde: <https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/povinne-zverejnovane-informace/seznam-udelenych-akreditaci-pro-spravu-kvalifikovaneho-systemu-elektronicke-identifikace/>

elektronickou identifikaci.⁵⁰ Agentura dále vede seznam kvalifikovaných správců a kvalifikovaných poskytovatelů usazených v České republice, který taktéž uveřejňuje na svých webových stránkách.^{51, 52}

Národní bod je ekvivalentem pojmu uzlu podle nařízení eIDAS.

Zvláštností je přistoupení českého zákonodárce k vymezení činnosti, respektive úkolů národního bodu. Nařízení eIDAS, respektive jeho prováděcí akt INT popisuje uzlu jako místo propojující jednotlivé národní systémy elektronické identifikace se systémy elektronické identifikace jiných členských států.⁵³ Z vymezení pojmu dovozují, že uzlu je pouze jakýmsi kanálem a tlumočnickem mezi datovým uložištěm každého jednotlivého systému elektronické identifikace mezi členskými státy. Jediným požadavkem na uchování určitých dat je v čl. 9 odst. 3 prováděcího aktu INT uvedená povinnost provozovatele uzlu zachovat ty údaje, které v případě incidentu umožní rekonstrukci sledu výměn zpráv potřebnou ke zjištění místa a povahy incidentu; konkrétně uvádí identifikaci uzlu, zprávy a datum a čas zprávy. Proti tomu zákonodárce do § 21 odst. 1 ZoEI uvádí povinnost vést identifikátor prostředku pro elektronickou identifikaci včetně údaje o úrovni záruky prostředku, identifikátor držitele v rámci kvalifikovaného systému a identifikátor držitele v rámci on-line služby nebo jiné činnosti.

Dle mého názoru se tak jedná o překročení litery nařízení eIDAS, kdy národní úprava nastaveným postupem bezdůvodně zvyšuje riziko zneužití citlivých dat držitelů prostředků pro elektronickou identifikaci. Postup totiž fakticky tvoří kopie již existujících dat v datovém centru samotného systému elektronické identifikace, který vydal prostředek pro elektronickou identifikaci, na samotném uzlu, který nemusí disponovat takovou ochranou jako jednotlivé systémy elektronické identifikace. Argument lze podtrhnout i zněním čl. 6 odst. 2 prováděcího aktu INT, který zakazuje v uzlu uchovávat jakékoli osobní údaje s výjimkou údajů pro účely stanovené v čl. 9 odst. 3 prováděcího aktu INT, tato výjimka ale vyžaduje zachování pouze těch údajů, které jsou nutné pro rekonstrukci sledu výměn zpráv nikoli identifikaci jejího držitele. Za protiargument nelze považovat fakt, že funkci národního bodu v prostředí České republiky plní Národní identitní agentura, která je spojnicí mezi kvalifikovanými správci a kvalifikovanými poskytovateli a která je v některých případech kvalifikovaným správcem systému elektronické

⁵⁰ Ustanovení § 19 písm. a) až h) ZoEI.

⁵¹ Ustanovení § 23 odst. 1 a 2 ZoEI.

⁵² Seznam kvalifikovaných správců a kvalifikovaných poskytovatelů usazených v České republice vedených v seznámech Agentury lze najít je dostupný z odkazu: <https://info.identitaobcana.cz/sep/>.

⁵³ Přesné vymezení pojmu v čl. 2 bodu č. 1 prováděcího aktu Evropské komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 Nařízení eIDAS.

identifikace (k postavení Agentury v procesu elektronické identifikace podrobněji v části 3.1.1 této práce). Agentura tak fakticky agreguje některé data, které by v postavení národního bodu agregovat neměla.

Lze si tak všimnout, že ZoEI má snahu o vyplnění bílých míst, kde nařízení eIDAS zanechalo prostor k uvážení jednotlivým zákonodárcům členských států, a dosáhnout tak kvalitnějšího a přístupnějšího systému elektronické identifikace. Jak je ale patrné z výše uvedeného textu, v některých případech zákonodárce překročil mez pro něj stanovenou a někdy i bezdůvodně zasahuje do nastavené soustavy elektronické identifikace. Pro úplnost lze doplnit, že ZoEI nebyl v legislativním procesu Parlamentem České republiky (sněmovní tisk 1069⁵⁴) jakkoli upraven a prošel bez, byť jen jediného pozměňovacího návrhu. Na půdě Poslanecké sněmovny proběhl legislativní proces bez vystoupení jakéhokoli poslance s návrhem úpravy či jakéhokoli komentáře s výjimkou zástupců příslušných výborů, kteří návrh bez dalšího podpořili, a lze tak říci, že se jedná o jednoznačný záměr navrhovatele, kterým bylo v tomto případě Ministerstvo vnitra.⁵⁵

2.4 Zákon o bankovní identitě

2.4.1 Předmět zákona a podrobnosti jeho změn

ZoBI je jako adaptační zákon v určitém ohledu doplněním a rozšířením ZoEI. U ZoEI absentuje úprava směrem k soukromoprávním subjektům, které chtějí vykonávat podnikatelskou činnost v oblasti elektronické identifikace. Na základě ZoBI byl bankám a zahraničním bankám působícím na území České republiky umožněn výkon podnikatelské činnosti spočívající v poskytování elektronické identifikace, autentizace a služeb vytvářejících důvěru dle nařízení eIDAS a s tím souvisejících služeb.

ZoBI je rozdělen do čtyř částí podle jednotlivých zákonů, které novelizuje. Jedná se o část I. změna zákona o bankách, část II. změna zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, část III. změna zákona o pojišťovnictví a část IV. změna zákona o pojištění odpovědnosti z provozu vozidla. Vzhledem k povaze změn obsažených v částech III. a IV. ZoBI se nebudu touto částí novel podrobně v této práci zabývat s výjimkou legislativního procesu.

2.4.1.1 Vybrané aspekty změny zákona o bankách

⁵⁴ Sněmovní tisk 1069 – Vládní návrh zákona o elektronické identifikaci – EU. 21.03.2017. Dostupné z: <https://www.psp.cz/sqw/historie.sqw?o=7&T=1069>

⁵⁵ Stenozáznam části jednání 57. schůze Poslanecké sněmovny ke sněmovnímu tisku 1069. Dostupné z: <https://www.psp.cz/eknih/2013ps/stenprot/057schuz/bqbs/b20001401.htm>

Banky⁵⁶ jsou pro svou klíčovou úlohu ve fungování moderní společnosti v evropském prostoru podrobeny jedné z nejpřísnějších regulací vůbec a v českém právním prostředí jsou nastavené restriktive v takové míře, že jsou banky ze své podstaty vyjmuty z obecně platného principu legální licence, tj. banky mohou činit jen to, co jim zákon dovoluje.⁵⁷ To se projevuje tak, že banky mohou činit jen takovou obchodní činnost, kterou mají zapsanou ve své bankovní licenci. Tak zásadní omezení svobody podnikat by bylo pro jiné subjekty vykonávající obchodní činnost nepředstavitelné.

S ohledem na výše uvedené bylo jednou ze zásadních změn prolomení výše popsaného licenčního principu, kdy došlo k vložení písm. c) pod § 1 odst. 4, který držitelům bankovní licence umožňuje vykonávat činnost mimo tuto licenci. Novela zavádí pojem „**identifikační služby**“, pod které řadí obchodní činnost poskytování elektronické identifikace a autentizace, poskytování služeb vytvářejících důvěru a poskytování tzv. souvisejících služeb.⁵⁸

Zajímavostí je, že ač se jedná o podnikatelskou činnost, která není zapsaná v licenci banky, není třeba pro činnost identifikačních služeb získat jakékoli jiné podnikatelské oprávnění a banky si taktéž tuto činnost nemusí nikde ohlásit či zapsat.^{59, 60, 61} Nad absencí povinnosti získat potřebné podnikatelské oprávnění podle zákona č. 455/1991 Sb., o živnostenském podnikání (dále jako „**ZoŽP**“), se taktéž pozastavuje i komentář k ZoB, který však na tuto situaci upozorňuje v případě, že držitel bankovní licence vykonává některou z činností podle §1 odst. 4 sám pro sebe a nikoli pro třetí osoby.⁶² Je však nutné vzít v potaz, že by případná novela měla pouze formalistické důsledky a nezměnila by přístup k podnikání či bezpečnost klientů bank, a zároveň že osoba vykonávající identifikační služby musí projít Akreditací ve smyslu ZoEI. Lze se tak domnívat, že byť jsou banky v teoreticky zvýhodněném postavení proti zbytku podnikatelů, je regulace jejich činnosti natolik přísná, že se nejedná o zhoršení stavu pro jejich

⁵⁶ Pro zjednodušení a přehlednost zařazují pod pojem banky nejenom banky s vlastní bankovní licenci udělenou ČNB, ale taktéž zahraniční banky vykonávající činnost banky na území České republiky na základě notifikace vůči ČNB dle jednotného evropského pasu a také pobočky z nečlenských zemí na základě povolení vydaného ČNB. K datu uzavření této práce se jedná např. o Oberbank (Rakousko) nebo mBank (Polsko).

⁵⁷ Ustanovení § 1 odst. 1, 3 a 4 ZoB.

⁵⁸ Ustanovení § 1 odst. 4 písm. c) ZoB.

⁵⁹ Výpis ze systému JERRS ČNB – Komerční banka a.s., IČO: 453 17 054, se sídlem Na příkopě 969/33, Staré Město, PSČ: 110 00, v evidenci České národní banky (systém JERRS) o udělení licence a povolených činnostech banky. 25.06.2021. Dostupné z: https://apl.cnb.cz/apljerrsdad/JERRS.WEB10.VIZITKA?p_lang=cz&p_SEQ_ID=160&p_VER_ID=1025&p_DATUM=25.06.2023&p_ROL_KOD=

⁶⁰ Výpis z obchodního rejstříku – Komerční banka a.s., IČO: 453 17 054, se sídlem Na příkopě 969/33, Staré Město, PSČ: 110 00. [online] Obchodní rejstřík [cit. 30.07.2023]. Dostupné z: <https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=68415&typ=PLATNY>

⁶¹ Výpis z živnostenského rejstříku – Komerční banka a.s., IČO: 453 17 054, se sídlem Na příkopě 969/33, Staré Město, PSČ: 110 00. [online] Živnostenský rejstřík [cit. 30.07.2023]. Dostupné z: https://www.rzp.cz/cgi-bin/aps_cacheWEB.sh?VSS_SERV=ZVWSBJVYP&OKRES=&CASTOBCE=&OBEC=&ULICE=&CDOM=&COR=&COZ=&ICO=45317054&OBCHJM=&OBCHJMATD=0&ROLES=P&JMENO=&PRIJMENI=&NAROZENI=&ROLE=&VYPIS=1&type=&PODLE=subjekt&IDICO=969fb61b9c710b&HISTORIE=0

⁶² SMUTNÝ, Aleš, PIHERA, Vlastimil, CUNÍK, Tomáš. § 1 [Vymezení pojmů]. In: SMUTNÝ, Aleš, PIHERA, Vlastimil, SÝKORA, Pavel, CUNÍK, Tomáš. Zákon o bankách. 2. vydání. Praha: C. H. Beck, 2019, s. 88, marg. č. 234.

klienty či zvýšené ohrožení osobních dat těchto klientů nebo zvýhodnění pozice bank vůči ostatním podnikatelským subjektům.

ZoBI tak úpravou § 1 ZoB umožnil v rámci českého právního prostředí vznik druhého samostatného světa elektronické identifikace, lze ji nazvat jako soukromoprávní elektronickou identifikaci či také jako bankovní e-ID. Dle ZoEI již existovala a fungovala elektronická identifikace provozovaná státem v rámci kvalifikovaného systému elektronické identifikace, tj. systém státní elektronické identifikace (podrobněji o rozdílech, propojení a fungování těchto soustav v části 3.2 této práce). Tato změna není výmyslem českého zákonodárce nebo bank působících v České republice, jedná o soustavu, která je předpokládána již v nařízení eIDAS (viz 2.1 této práce). ZoBI je tak pouze realizací myšlenky, která přišla společně s evropskou regulací.

ZoBI v této části taktéž uvaluje na informace získané v procesu identifikačních služeb bankovní tajemství podle § 38 ZoB, které je nad rámec požadavku nařízení eIDAS, ale v souladu se stanoviskem vlády k návrhu zákona (viz 2.4.4 této práce). Banky tak pro jakékoli poskytování získaných informací musí mít souhlas svého klienta. To by na první pohled mohlo vypadat jako znesnadnění výkonu takové činnosti pro potřebu vyššího zabezpečení nebo složitějšího nakládání s daty, ale není tomu tak. Banky ve své běžné bankovní činnosti již postupy podřízené pravidlům bankovního tajemství aplikují, a pro ně i pro jejich klienty se tak jedná o běžný postup. Naopak na uplatnění bankovního tajemství se lze z klientského pohledu dívat jako na konkurenční výhodu oproti ostatním kvalifikovaným poskytovatelům elektronické identifikace, kteří pravděpodobně nejsou schopni garantovat takovou míru ochrany dat jako banky. V praktické rovině se s tím klient setká při přihlašování se pomocí Bankovní identity, která se ho nejprve zeptá, zda může klientská data (tj. osobní identifikační údaje) zpřístupnit pro účely autentizace.

Poskytovatel identifikačních služeb je pojem, který ZoBI nově zavádí v § 38aa odst. 2. Jedná se o „osobu, která není bankou, 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“.⁶³ Jde tedy o možnost vykonávat identifikační služby za pomoci jednoho subjektu, který bude vlastněn a řízen více bankovními domy. Jak se později ukázalo stal se tento model uplatňovaným

⁶³ Ustanovení § 38aa odst. 2 ZoB.

v případě Bankovní identity, a.s. (viz část 362.5 této práce).

Ve vztahu k výše uvedenému omezení legální licence pro banky je vhodné podotknout, že pro poskytovatele identifikačních služeb ve smyslu §38aa odst. 2 ZoB tato restrikce neplatí, jedná se totiž o běžnou obchodní korporaci zřízenou podle zákona č. 90/2012 Sb., o obchodních korporacích.

Zavedením výše uvedeného modelu došlo k umožnění zbavení se přísného režimu bankovního tajemství v případě předání získaných údajů z banky poskytovateli identifikačních služeb ve smyslu § 38aa odst. 2 ZoB.

Ustanovením § 38ab odst. 1 ZoB je bankám umožněno povolit využití jimi vydaného prostředku elektronické identifikace i mimo rámec kvalifikovaného systému elektronické identifikace, tj. v rámci soukromoprávní soustavy elektronické identifikace, např. při přihlašování se do online klientské zóny poskytovatele energií, s podmínkou, že tento prostředek splňuje požadavky a je ho tak možné použít i v rámci onoho kvalifikovaného systému, tedy v rámci veřejnoprávních služeb poskytovaných státem (např. při sčítání osob, kontrola stavu bodového konta řidiče aj.). Díky tomu je dosaženo situace, v níž všechny vydané prostředky elektronické identifikace podléhají správnímu doзору.

Ustanovení § 38ac ZoB zavádí možnost prostředek pro elektronickou identifikaci použít také pro prokázání totožnosti v situacích, v nichž to vyžaduje právní předpis nebo výkon působnosti mimo kvalifikovaný systém. Pro takové využití je ale nastaveno několik podmínek:

- I. splnění technických specifik, norem a postupů alespoň pro úroveň záruky značnou podle evropských předpisů;
- II. banka nebo poskytovatel identifikačních služeb, kteří vydali klientův prostředek pro elektronickou identifikaci, identifikovali osobu postupem podle AML zákona, a to buďto:
 - a. za její fyzické přítomnosti,
 - b. pomocí prostředku elektronické identifikace, který splňuje technické specifikace, normy a postup pro úroveň vysokou a který je vydán (např. e-občanka) a používán v rámci jakéhokoliv kvalifikovaného systému nebo byl vydán a používán jiným (zahraničním) systémem elektronické identifikace, který taktéž splňuje alespoň úroveň záruky vysoké, nebo
 - c. pomocí prostředku elektronické identifikace, který splňuje technické specifikace, normy a postup pro úroveň značnou a který je vydán (např.

e-občanka) a používán v rámci státního kvalifikovaného systému, pokud došlo ke ztotožnění pomocí národního bodu pro identifikaci a autentizaci nebo v systému veřejné správy a banka má údaje o tom kdo identifikaci v minulosti provedl; jedná se o informaci, která není součástí samotného prostředku elektronické identifikace je tak nutné, aby banka tento údaj získala separátně.

Jedním z důvodů tohoto přepsání povinností z AML zákona do ZoBI, respektive příslušné části ZoB, je, že poskytovatel identifikačních služeb ve smyslu ZoB není povinnou osobou podle AML zákona. Nevztahovala by se na něj tak povinnost uplatňovat tento způsob identifikace.

Ustanovení § 38ac odst. 2 ZoB umožňuje bankám se nechat v při identifikování osoby za fyzické přítomnosti identifikovaného zastoupit. Osoba identifikující za banku musí identifikaci provádět v souladu s AML zákonem, být vázána vnitřními předpisy banky, za níž identifikaci provádí, a údaje získané při identifikaci se musí uložit u banky nebo poskytovatele identifikačních služeb ještě před vystavením prostředku pro identifikaci pro identifikovanou osobu.

Propojení státní elektronické identifikace a soukromé elektronické identifikace představuje mimo jiné ustanovení § 38ad ZoB, které nastavuje povinnost bank umožnit využít jimi vydaný prostředek elektronické identifikace při identifikaci u státních orgánů a orgánů územně samosprávných celků, a to pro klienta bezúplatně, stejně jako tomu je v případě elektronické identifikace uvnitř státního, respektive kvalifikovaného systému elektronické identifikace.

V ustanoveních § 38ae a § 38af ZoB došlo k provázání bank a poskytovatele identifikačních služeb s informačními systémy veřejné správy, včetně údajů v základních registrech, a to formou zřízení vlastního informačního systému, který plní veškeré stanovené technologické a bezpečnostní podmínky pro své využití. Bankám a poskytovatelům identifikačních služeb je taktéž zamezen neomezený přístup do registrů a jsou stanoveny mantinely v podobě vybraných údajů, na které se banky a poskytovatele identifikačních údajů mohou nahlédnout a ověřit si jejich správnost. Propojení je praktickým a logickým vyústěním povinnosti obezřetné péče bank podle § 12 ZoB a tím umožňuje lepší výkon povinností, které banka má podle AML zákona.

Banky a poskytovatelé identifikačních služeb mají v důsledku přijetí ZoBI přístup do základních registrů a systémů státu, konkrétně se jedná o základní registr obyvatel, informační systém evidence obyvatel, informační systém cizinců, informační systém evidence občanských

průkazů a informační systém evidence cestovních dokladů, na jehož základě mají plnit povinnosti výše uvedené. Vedle zřízení přístupu pro banky a poskytovatele identifikačních služeb také došlo ke zřízení ekvivalentního přístupu pro pojišťovny (podrobněji v části 2.4.4 této práce).

2.4.2 Dopad do AML zákona

Přijetím ZoBI došlo k rozšíření možností způsobu identifikace pro povinné osoby podle AML zákona. Toto doplnění spočívá ve vložení nového § 8a, který vytváří paritní možnost k prvotní identifikaci osob podle § 8 odst. 1 a 2 písm. a) AML zákona, tedy identifikaci osoby za její fyzické přítomnosti a za podmínek zaznamenání údajů z průkazu totožnosti.

AML zákon zná ještě dvě alternativy k identifikaci osoby podle svého § 8 odst. 1 a 2 písm. a). První je identifikace pomocí tzv. korunové platby (podrobněji v části 4.2 této práce), která je zakotvena v § 11 odst. 7 AML zákona, a druhá za užití postupu podle § 11 odst. 8 AML zákona spočívajícího ve využití identifikace osoby u kvalifikovaného poskytovatele služeb vytvářejících důvěru ve smyslu nařízení eIDAS, přesněji se jedná o využití elektronického podpisu. Tyto metody lze ale pro účely elektronické identifikace použít pouze v případě že povinná osoba, tedy v našem případě banka, nemá žádnou pochybnost o totožnosti svého klienta. Z toho důvodu lze ty klienty, u nichž neproběhla identifikace za fyzické přítomnosti, vyloučit z využitelné identifikace, a tedy jim nelze vystavit prostředek pro elektronickou identifikaci.

Při spuštění Bankovní identity nebyl těmto osobám prostředek pro elektronickou identifikaci automaticky zřízen a v případě, že by o něj daná osoba požádala, musela by proběhnout identifikace podle § 8 odst. 1 písm. a) AML zákona za její fyzické přítomnosti na jedné z poboček banky.

Tento nově zavedený způsob identifikace na dálku je podmíněn hned několika požadavky, které je třeba využitím elektronické identifikace splnit.

Podmínky podle § 8a odst. 1 písm. a) AML zákona jsou kumulativně: prostředek pro elektronickou identifikaci musí být vydán a používán v rámci kvalifikovaného systému, tj. státního systému elektronické identifikace (pod tuto podmínku lze zařadit i ty prostředky elektronické identifikace vystavené systémy elektronické identifikace jiných členských států) a splnění technických specifik, norem a postupů pro vysokou úroveň záruky podle prováděcího aktu MTS.

V případě § 8a odst. 1 písm. b) AML zákona se jedná o podmínky, za nichž lze využít prostředek pro elektronickou identifikaci při prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti mimo rámec kvalifikovaného systému, tj. prostředek pro elektronickou identifikaci vydaný bankou nebo poskytovatelem identifikačních služeb.

2.4.3 Okolnosti přijetí ZoBI a jeho některé praktické důsledky

Do přijetí ZoBI bylo využití elektronické identifikace, systémů elektronické identifikace či jejich nástrojů spíše záležitostí jednotlivců, fanoušků a obeznámených osob. Tento stav souvisí i s faktem, že do té doby byl nejpoužívanějším prostředkem pro elektronickou identifikaci občanský průkaz obsahující čip. To byl postup, který postrádal nejzásadnější výhodu elektronické identifikace, a to možnost identifikace na dálku, například z domova. I když občan disponoval potřebným občanským průkazem, musel taktéž disponovat potřebným hardwarem, který uměl rozpoznat a přečíst čip v občanském průkazu. To znamenalo, že většina tehdejších uživatelů elektronické identifikace musela fyzicky dojít na některý z úřadů, který tento hardware měl, nebo si ho občan musel koupit – řečí ekonomie, jednalo se o vstupní překážku či bariéru takovou, že drtivou většinu potenciálních uživatelů odradila.

Dalším podstatným důvodem minimálního využití elektronické identifikace byl samotný ZoEI, který dále neupravoval možné využití elektronické identifikace v soukromoprávních vztazích, ač takovou možnost nařízení eIDAS předpokládalo.

Přijetím ZoBI došlo k podstatné změně v „dostupnosti“ služby elektronické identifikace občanům, respektive klientům bank. Namísto zajišťování nových občanek a zvláštního hardwaru dostal prakticky každý klient bank přes noc přístup do systému elektronické identifikace své banky, která byla napojená na státem provozovaný systém. Tedy přístup do služeb poskytovaných státem jako například Portál občana, portál Moje daně online, Portál Pražana a další. Zlepšení dostupnosti mělo velice rychlou odezvu a již v prvních třech měsících provozu došlo k růstu počtu aktivních uživatelů v řádu stovek tisíc.^{64, 65}

Přijetím také došlo k faktickému rozšíření elektronické identifikace do soukromoprávního sektoru, který do přijetí ZoBI neměl příliš mnoho opor, a snížení vstupních nákladů pro společnost, která by chtěla systém elektronické identifikace vytvořit tzv. na zelené louce. Novela ZoB umožnila vytvoření služby Bankovní identity za pomoci bank, kterým do přijetí

⁶⁴ SOVOVÁ E. Průlom: o digitální občanku je velký zájem, šetří čas a ulehčuje život [online]. iDnes.cz, 19.04.2021 [cit. 27.07.2023]. Dostupné z: https://www.idnes.cz/finance/financni-radce/bankovni-identita-banky-digitalni-obcanka-overovani.A210416_084442_viteze_sov

⁶⁵ SKALKOVÁ O. Bankovní identita znamená průlom v on-line ověřování totožnosti [online]. Hospodářské noviny, 14.04.2021 [cit. 27.07.2023]. Dostupné z: <https://archiv.hn.cz/c1-66903310-bankovni-identita-znamená-prulom-v-on-line-overovani-totoznosti>

ZoBI takovou činnost právě ZoB znemožňoval (viz v části 2.4.1.1 této práce).

Banky pro zřízení tohoto přístupu musely získat souhlas svých klientů, který si zajistily formou předčasné změny všeobecných obchodních podmínek a systémem *opt-out*, čímž prakticky každý klient získal svůj vlastní bankovní prostředek elektronické identifikace.

K tomuto masovému rozšíření na klienty bank však vedl komplikovaný proces zahrnující zástupce bank, Českou bankovní asociaci, Českou národní banku (dále jako „ČNB“), Ministerstvo financí, Ministerstvo vnitra, Finanční analytický úřad (dále jako „FAÚ“) a Správu základních registrů.⁶⁶

2.4.4 Proces přijetí ZoBI

ZoBI byl v legislativním procesu Parlamentem České republiky navržen jako novela zákona o bankách označená jako sněmovní tisk č. 554.⁶⁷ Přes zásadní důsledky pro fungování státu a jeho komunikaci s občany nebyl navrhovatelem některý z ústředních správních orgánů, ale skupina poslanců. Součástí této skupiny byl i tehdejší předseda vlády Andrej Babiš a někteří tehdejší ministři jako například Klára Dostálová, ale i opoziční poslanci za ODS, Piráty, TOP 09, KDU-ČSL či SPD.⁶⁸

Opodstatnění takového kroku lze pouze odhadovat, ve veřejných záznamech Poslanecké sněmovny důvod není uveden. Lze se ale domnívat, že tím došlo k urychlení a zjednodušení celého procesu, jelikož díky použití cesty poslaneckého návrhu byl zcela vypuštěn postup, který se uplatňuje u vládního návrhu zákona, tedy zejména meziresortní připomínkové řízení, které mnohdy trvá několik týdnů či měsíců a kvůli své komplexnosti a preciznosti mnohdy donutí předkladatele upravit značné části navrhovaného legislativního textu.

Samotná rychlost projednání v Poslanecké sněmovně byla rovněž nezvyklá, poslancům byl sněmovní tisk rozeslán 30. 7. 2019 a 3. čtení bylo dokončeno již 4. 12. 2019. Podpisu prezidenta se zákon dočkal již 12. 2. 2020, zhruba 7 měsíců od prvního předložení skupinou poslanců. To je vzhledem k 30denní lhůtě pro vyjádření vlády, 60denní lhůtě k projednání výbory a 30denní lhůtě pro projednání Senátem úctyhodný výsledek svědčící o dostatečném předjednání návrhu všemi zainteresovanými stranami. Pro porovnání, deklarovaná průměrná doba přijetí zákona je

⁶⁶ KORBEL F., KOVÁŘ D. Právní úprava tzv. bankovní identity [online]. Advokátní deník online, 09.05.2021 [cit. 27.07.2023]. Dostupné z: <https://advokatnidenik.cz/2021/05/09/pravni-uprava-tzv-bankovni-identity-2/>

⁶⁷ Sněmovní tisk 554 [online]. Poslanecká sněmovna, 12.07.2019 [cit. 27.07.2023]. Dostupné z: <https://www.psp.cz/sqw/historie.sqw?o=8&T=554>

⁶⁸ Tamtéž.

v České republice cca 12 měsíců.⁶⁹

Vláda ve svém vyjádření se k návrhu zákony vytkla mimo jiné následující body:⁷⁰

- návrh neupravuje příslušnost vykonavatele veřejné správy k výkonu dozoru nad bankami, pobočkami zahraničních bank nebo poskytovateli identifikačních služeb ani nezakládá dozorovou pravomoc ČNB nebo FAÚ podle AML zákona;
- existuje riziko spojené s prakticky nekontrolovaným přístupem do řady informačních systémů a základních registrů státu ze stran bank, zahraničních bank a poskytovatelů identifikačních služeb, zároveň vláda upozorňuje na absenci ochrany údajů o konkrétních osobách, které mají vztah ke zpravodajské službě;
- návrh nezaručuje bezplatný přístup organizačních složek státu a dalších státních organizací k elektronické identifikaci pomocí prostředku pro elektronickou identifikaci, který neprošel národním bodem pro identifikaci a autentizaci;
- v neposlední řadě vláda návrhu vytkla možné řetězení prostředků elektronické identifikace, kdy banka vydá prostředek elektronické osobě, která se jí v minulosti identifikovala pomocí jiného uznaného prostředku (např. tzv. „penny transfer“), a tedy nebyla možná kontrola s údaji v centrálních registrech státu (podrobněji k této problematice v části 4.2 této práce).

Jak plyne ze stenoáznamu 39. schůze Poslanecké sněmovny, ve 2. čtení sněmovního tisku při rozpravě o tisku 554 byly načteny dva pozměňovací návrhy.⁷¹

První byl komplexní pozměňovací návrh, který je výsledkem práce poslaneckého výboru pro veřejnou správu a který reagoval na výtky uvedené ve vládním stanovisku.

Pozměňovací návrh prakticky přepracoval znění celého návrhu zákona. V některých případech provedl kosmetické změny, jinde reformuloval některé myšlenky v návrhu a v některých případech původní návrh prakticky nahradil.

Pozměňovací návrh upravil znění návrhu zákona v problematice příslušnosti orgánu veřejné správy při dozoru nad podnikatelskou činností v oblasti elektronické identifikace tak, že celou

⁶⁹ GURČOVÁ K. 6 největších legislativních ležáků. Které zákony politici uložili k ledu, ačkoli je po nich poptávka? [online]. iRozhlas 22.05.2017 [cit. 27.07.2023]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/6-nejvetsich-legislativnich-lezaku-ktere-zakony-politici-ulozili-k-ledu-ackoli_1705220600_kno

⁷⁰ Stanovisko vlády k návrhu poslanců Barbory Kořanové, Martina Kupky, Ivana Bartoše, Pavla Jelínka, Pavla Kováčika, Jana Chvojky, Jana Bartoška, Heleny Langšádlové, Věry Kovářové a dalších na vydání zákona, 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 (sněmovní tisk č. 554) [online]. oDOK.cz 26.08.2019 [cit. 27.07.2023]. Dostupné z: <https://odok.cz/portal/veklep/material/ALBSBELH9NWU/>

⁷¹ Stenoáznam části projednávání bodu pořadu schůze z 39. schůze Poslanecké sněmovny [online]. Parlament České republiky, Poslanecká sněmovna, 26. listopadu 2019 [cit. 28.07.2023]. Dostupné z: https://www.psp.cz/eknih/2017ps/stenprot/039schuz/bqbs/b00700501.htm#_d

aktivitu elektronické identifikace zařadil pod bankovní tajemství ve smyslu § 38 ZoB, čímž byla zajištěna povinnost bank podávat zprávu o záležitostech týkajících se klienta různým subjektům veřejné správy, od soudů přes správce daně, FAÚ, zdravotní pojišťovny až po Ministerstvo financí či Policii České republiky.⁷²

Snaha o omezení nekontrolovaného přístupu bank do registrů provozovaných státem je dle mého názoru spíše kosmetickou změnou, která se v pozměňovacím návrhu projevila v podobě selekce dat, ke kterým má banka ve státních registrech přístup. Konkrétně byla oproti původnímu znění bankám odejmuta možnost zjistit doručovací adresu identifikované osoby, údaje o elektronické adrese (tj. e-mail) a telefonním čísle identifikované osoby a obrazový záznam (tj. fotka na občanském průkazu nebo cestovním dokladu) identifikované osoby. Fakticky tak sice došlo k omezení penza údajů, ke kterým se banka skrze státní registry dostane, ale jedná se o údaje, které nejsou příliš relevantní. Zajímavostí je, že v předmětném ustanovení s výčtem dat, které banka může z centrálních registrů získat, došlo k vložení nového odst. 9, který v konečném důsledku umožňuje bankám přístup ke všem údajům v centrálních registrech státu, a to po získání souhlasu identifikované osoby.⁷³ Při uvědomění si, jakým způsobem banky získaly souhlas od svých klientů k vytvoření prostředků elektronické identifikace (formou *opt-out* souhlasu), se domnívám, že výčet získatelných osobních údajů, které jsou vymezené v předmětném ustanovení ZoBI, je pouhou vějičkou a nikoli faktickou restrikcí či regulací subjektů provozujících podnikatelskou činnost v poskytování elektronické identifikace.

Otázku ohledně nemožnosti bezúplatného přístupu organizačních složek státu a územních samosprávných celků k elektronické identifikaci vyřešil pozměňovací návrh vložením § 38ad odst. 2. Ten umožnil výše zmíněným subjektům využívat prostředek elektronické identifikace vydaný bankou pro účely prokázání totožnosti v situacích, v nichž to vyžaduje právní předpis nebo výkon působnosti, avšak pouze prostřednictvím kvalifikovaného systému, tj. alespoň na úrovni záruky značné.⁷⁴

V reakci na znemožnění vydání prostředku pro elektronickou identifikaci těm osobám, které banky v minulosti identifikovali při své prvotní identifikaci pomocí tzv. penny transfer (tj. tak, že osoba nikdy nebyla fyzicky identifikována v pobočce banky) či jiným státem neuznávaným způsobem identifikace, kdy se klient v identifikoval způsobem, který nezaručuje spolehlivost

⁷² § 38 odst. 1 a 3 zákona č. 49/2020 Sb., o bankovní identitě. In: *Sbírka zákonů*. 06. 02. 2020. ISSN 1211-1244. Dostupné z:

<https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrf6mrqiyf6nbzfuya>

⁷³ Sněmovní tisk 554/5, Pozměňovací a jiné návrhy k tisku 554/0. [online]. Parlament České republiky, Poslanecká sněmovna, 26. listopadu 2019 [cit. 28.07.2023 Dostupné z: <https://www.psp.cz/sqw/text/tiskt.sqw?o=8&ct=554&ct1=5>

⁷⁴ Sněmovní tisk 554/5, Pozměňovací a jiné návrhy k tisku 554/0. [online]. Parlament České republiky, Poslanecká sněmovna, 26. listopadu 2019 [cit. 28.07.2023 Dostupné z: <https://www.psp.cz/sqw/text/tiskt.sqw?o=8&ct=554&ct1=5>

jeho identifikace, došlo ke změně v textaci návrhu zákona.⁷⁵ Změna spočívala v zavedení povinnosti, že u všech těch klientů, kterým bude vydáván prostředek pro elektronickou identifikaci, bude provedení první identifikace vždy za fyzické přítomnosti identifikovaného, s jedinou výjimkou, která spočívá v opětovné identifikaci pomocí již získaného prostředku pro elektronickou identifikaci.

Jako druhý pozměňovací návrh byl načten návrh poslankyně Barbory Kořanové (ANO 2011), který do celého systému bankovní elektronické identifikace nově zařadil pojišťovny. Jedná se o část třetí ZoBI, změna zákona č. 277/2009 Sb., o pojišťovnictví (dále jen „ZoP“), a část čtvrtou, tedy změnu zákona č. 168/1999 Sb., o pojištění odpovědnosti z provozu vozidla. Zvláštní na tomto pozměňovacím návrhu je, že pro Českou kancelář pojistitelů zřizuje přístup do základních registrů státu, konkrétně do základního registru obyvatel, informačního systému evidence obyvatel, informačního systému cizinců, informačního systému evidence občanských průkazů a informačního systému evidence cestovních dokladů, avšak neumožňuje České kanceláři pojistitelů ani pojišťovnám vykonávat podnikatelskou činnost spočívající v poskytování elektronické identifikace, autentizace nebo služeb vytvářející důvěru.

Mezi odbornou veřejností je sice tato úprava ZoP vítána a dle jejího názoru pomáhá pojišťovnám s jejich zákonnou povinností v rámci AML zákona.⁷⁶ Podle mého názoru se však fakticky jedná o přílepek ZoBI, který ve svém jádru pro pojišťovny sice zřizuje přístup do základních registrů a pravděpodobně pro správné důvody, bohužel jsou ale tyto důvody jiné než u bank a logicky nezapadají do systematiky návrhu zákona, a tak je začlenění do ZoBI neopodstatněné a nesprávné. Argumentace, že je taková změna vhodná a smysluplná, není nosná z pohledu legislativního procesu a dělby moci v České republice. V případě, že je jakákoli změna právního řádu České republiky opodstatněná, musí dojít k jejímu řádnému a samostatnému projednání, ostatně jak konzistentně judikuje Ústavní soud České republiky. Dle mého názoru svědčí i dodatečná úprava názvu regulace, která proběhla ve třetím čtení zákona a byla navržen jako legislativně technická úprava znění. Z původní novely zákona o bankách se později stala novela zákona o bankách a dalších zákonů.⁷⁷

Oba pozměňovací návrhy Poslanecké sněmovna ve svém třetím čtení prakticky jednohlasně přijala.

⁷⁵ Srov. původní návrh § 11a odst. 6 AML zákona a pozměňovací návrh § 38ac odst. 1 písm. b) body 1. a 2.

⁷⁶ KORBEL F., KOVÁŘ D. Právní úprava tzv. bankovní identity [online]. Advokátní deník online, 09.05.2021 [cit. 27.07.2023]. Dostupné z: <https://advokatnidenik.cz/2021/05/09/pravni-uprava-tzv-bankovni-identity-2/>

⁷⁷ Stenozáznam části projednávání bodu pořadu 39. schůze Poslanecké sněmovny. [online]. Parlament České republiky, 4. prosince 2019 [cit. 30.07.2023]. Dostupné z: <https://www.psp.cz/eknih/2017ps/stenprot/039schuz/bqbs/b19221001.htm>

Zajímavostí je neúspěšná snaha poslance Patrika Nachera, který se nejprve snažil vsadit do samotné novely úpravu možnosti identifikace osoby, tak aby bylo možné vystavit prostředek elektronické identifikace i těm klientům bank, jejichž identifikace neproběhla za jejich fyzické přítomnosti, ale formou tzv. korunové platby (v angl. *penny transfer*; podrobněji v části 4.2 této práce) což bylo v přímém rozporu s výhradami vlády (viz výše). Po negativním přijetí návrhu úpravy zákona na půdě Poslanecké sněmovny se poslanec Nacher úspěšně domohl zaúkolování veřejné správy prověřením možností a případným legislativním návrhem, jak tyto osoby identifikované pomocí tzv. korunové platby zapojit.⁷⁸

Navazující proces přijetí zákona v Senátu prošel prakticky bez problémů. Ačkoli návrh zákona Ústavně-právní výbor doporučil Senátu zamítnout, došlo k uplatnění pravidla podle čl. 46 odst. 3 Ústavy České republiky, tedy že se Senátem neprojednaný návrh ve lhůtě 30 dní se považuje jako přijatý.

Prezident návrh zákona podepsal 12. února 2020 a zákon byl ve sbírce zákonů publikován 19. února 2020.⁷⁹

2.5 Bankovní identita, a.s.

Na základě procesu, který začal sdělením Evropské komise ve své „Digitální agendě pro Evropu“ z 26. srpna 2010 a dovršil jej podpisem ZoBI prezident České republiky dne 12. února 2020, došlo ke vzniku podnikatelské oblasti v elektronické identifikaci, v níž mohou banky v České republice realizovat svůj podnikatelský záměr.

Prakticky obratem po přijetí ZoBI učinily jednotlivé banky první kroky ve vývoji a následném spuštění služeb v oblasti elektronické identifikace, např. Československá obchodní banka se svou ČSOB Identitou⁸⁰, která je dle záznamu v seznamu kvalifikovaných správců uváděna ve dvou úrovních záruky, a to nízké a zaručené.⁸¹

Nejzásadnějším je ale vznik společnosti Bankovní identita, a.s., IČO: 095 13 817, se sídlem Smrčkova 2485/4, Libeň, 180 00 Praha 8 (dále jako „**Bankovní společnost**“), která byla do rejstříku zapsána dne 15. září 2020 a jejíž první akcionáři jsou Česká spořitelna, a.s., Československá obchodní banka, a.s., a Komerční banka, a.s.⁸²

⁷⁸ Tamtéž.

⁷⁹ Legislativní proces přijetí ZoBI. [online]. Parlament České republiky, 19. února 2020 [cit. 29.07.2023] Dostupné z: <https://www.psp.cz/sqw/historie.sqw?o=8&T=554>

⁸⁰ ČSOB Identita [online]. Československá obchodní banka [cit. 29.07.2023] Dostupné z: <https://www.csob.cz/portal/csob/csob-identita>

⁸¹ Kvalifikovaní správci [online]. Identita občana [cit. 29.07.2023] Dostupné z: <https://info.identitaobcana.cz/KvalifikovaniSpravci.aspx>

⁸² Výpis z obchodního rejstříku Bankovní společnosti [online]. Obchodní rejstřík [cit. 29.07.2023] Dostupné z: <https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=1095744&typ=PLATNY>

Cílem Bankovní společnosti bylo a stále je agregovat jednotlivé prostředky elektronické identifikace svých akcionářů, tedy bank, a nabízet tento agregát ke komerčním účelům. Služba, kterou Bankovní společnost nabízí nese komerční název BankID, tvoří jeden společný bod pro napojení na systémy kvalifikované identifikace jednotlivých bank v České republice. Bankovní společnost je tak v obdobné pozici jako Národní identitní autorita, která plní funkci národního bodu, resp. uzlu.

Postupem času se do Bankovní společnosti zapojily další bankovní domy, a původní tři akcionáře tak k dnešnímu dni doplnily Air Bank a.s., Fio banka, a.s., mBank S.A., organizační složka, MONETA Money Bank, a.s., Raiffeisenbank a.s. a UniCredit Bank Czech Republic and Slovakia, a.s.⁸³

Dle veřejných prohlášení stávajícího výkonného ředitele Bankovní společnosti Marka Růžičky bylo jejími akcionáři vydáno již více než 9 milionů prostředků elektronické identifikace s tím, že unikátních uživatelů, tj. fyzických osob, je kolem 5,5 milionu. Potenciál v České republice je kolem 6 milionů unikátních uživatelů.⁸⁴

Avšak i přes nebývale rozsáhlou síť uživatelů je společnost dle zveřejněných účetních závěrek stále ve ztrátě a nebyla schopna svůj obchodní záměr a potenciál digitální společnosti v České republice proměnit v zisku schopný vehikl. Účetní závěrka za rok 2022 a ostatní uveřejněné dokumenty ve sbírce listin Bankovní společnosti uvádějí ztrátu 84 269 749,42 Kč.⁸⁵ Ohledně způsobu úhrady ztráty, jejího odůvodnění a řešení vedou stávající akcionáři spor.⁸⁶

Bankovní společnost aktuálně poskytuje službu elektronické identifikace subjektům v soukromém sektoru, a to většinou tam, kde k tomu je zákonný požadavek ať už pro zpřístupnění samotné služby, prodej zboží či jen pro identifikaci konkrétní osoby při přihlašování do prostředí té které služby. Služby Bankovní společnosti tak lze využít při online nákupu či komunikaci nebo při konzumaci služeb provozovatele sázkových her, dodavatele energií, poskytovatele úvěrů, provozovatele telekomunikačních služeb, zdravotní pojišťovny, poskytovatele zdravotních služeb nebo dokonce při využívání služeb notáře v České republice či organizace pro zajišťování hlídání dětí nebo při nákupu v bezobslužných prodejnách

⁸³ Seznam akcionářů Bankovní společnosti dle webu Bankovní společnosti. BankID [cit. 29.07.2023] Dostupné z: <https://www.bankid.cz/onas>

⁸⁴ 03_Bank ID a ověřování identity, autentizace, Marek Růžička. Youtube [online]. 14.10.2022 [cit. 29.07.2023]. Dostupné z: <https://www.youtube.com/watch?v=PXYQj-FiNM&t=579s>

⁸⁵ Zápis z jednání valné hromady Bankovní společnosti ze dne 22. června 2023. Obchodní rejstřík [online]. 28.07.2023 [cit. 29.07.2023]. Dostupné z: <https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=77681541&subjektId=1095744&spis=1229161>

⁸⁶ ZATLOUKAL J. Velké a malé banky se prou o dluhy i zisk z Bankovní identity. Seznam zprávy [online]. 03.02.2023 [cit. 29.07.2023]. Dostupné z: <https://www.seznamzpravy.cz/clanek/ekonomika-firmy-velke-a-male-banky-se-prou-o-dluhy-i-zisk-z-bankovni-identity-225068>

potravin.⁸⁷

Z dostupných statistik Bankovní společnosti je 75 % veškerých online přihlášení k veřejnoprávním službám státu pomocí prostředku elektronické identifikace vydaného bankou.⁸⁸

Bankovní společnost připravuje a postupně spouští také další služby, které vychází z nařízení eIDAS. Zejména se jedná o BankID Sign – elektronický podpis na úrovni zaručeného podpisu, BankID+, prokázání věku (např. při nákupu alkoholu online), ale také plnou digitalizaci hypoték či přípravu na eIDAS 2.0 / EU Digital ID Wallet.⁸⁹

⁸⁷ 03_Bank ID a ověřování identity, autentizace, Marek Růžička. Youtube [online]. 14.10.2022 [cit. 29.07.2023]. Dostupné z: <https://www.youtube.com/watch?v=PxYPQj-FiNM&t=579s>

⁸⁸ Tamtéž.

⁸⁹ Tamtéž.

3 Elektronická identifikace a bankovní identita

Jak bylo popsáno výše, elektronická identifikace podle nařízení eIDAS byla včleněna do českého právního řádu převážně pomocí dvou legislativních počinů, ZoEI a následně ZoBI. To umožnilo vzniknout dvěma paralelně na sobě existujícím systémům elektronické identifikace, jeden nazýváme státní systém e-ID (dále jako „**státní e-ID**“) a druhý bankovní systém e-ID (dále jako „**bankovní e-ID**“). Nic přitom nevylučuje vznik dalších systémů elektronické identifikace, které budou buďto uzavřené vůči celoevropskému systému podle nařízení eIDAS, nebo na něj budou napojeny.

Systémy státní e-ID a bankovní e-ID mohou fungovat samostatně, ale i propojeně, a také lze využít systém bankovní e-ID pro elektronickou identifikaci pro službu poskytovanou mimo území České republiky (viz části 3.1.1, 3.2, 1 a 3.3 této práce).

3.1 Vymezení způsobu fungování systémů

Pro snazší pochopnutí fungování obou systémů e-ID níže uvádím tři praktické příklady využití elektronické identifikace, resp. bankovní identity.

3.1.1 Státní e-ID

Systém státního e-ID je systémem, který funguje v rozsahu ZoEI, resp. nařízení eIDAS. Dle zákona je státní e-ID kvalifikovaným systémem,⁹⁰ pro nějž platí, že:

1. je spravován identity providerem, resp. kvalifikovaným správcem;
2. splňuje technické specifikace, normy a postupy alespoň pro jednu z úrovní záruky stanovených prováděcím nařízením k nařízení eIDAS o úrovni záruky;
3. umožňuje poskytnutí propojení s NIA a je tak připojen na národní bod pro identifikaci a autentizaci;
4. v jeho rámci jsou osobní identifikační údaje jedinečně identifikující osobu v okamžiku vydání prostředku elektronické identifikace spojeny s danou osobou v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými prováděcím nařízením k nařízení eIDAS o úrovních záruk prostředků elektronické identifikace;
5. v jeho rámci je vydáván a používán pouze prostředek elektronické identifikace, který je spojen s osobou, kterou identifikuje v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými nařízením eIDAS.

⁹⁰ Srov. ustanovení § 3 odst. 1 ZoEI.

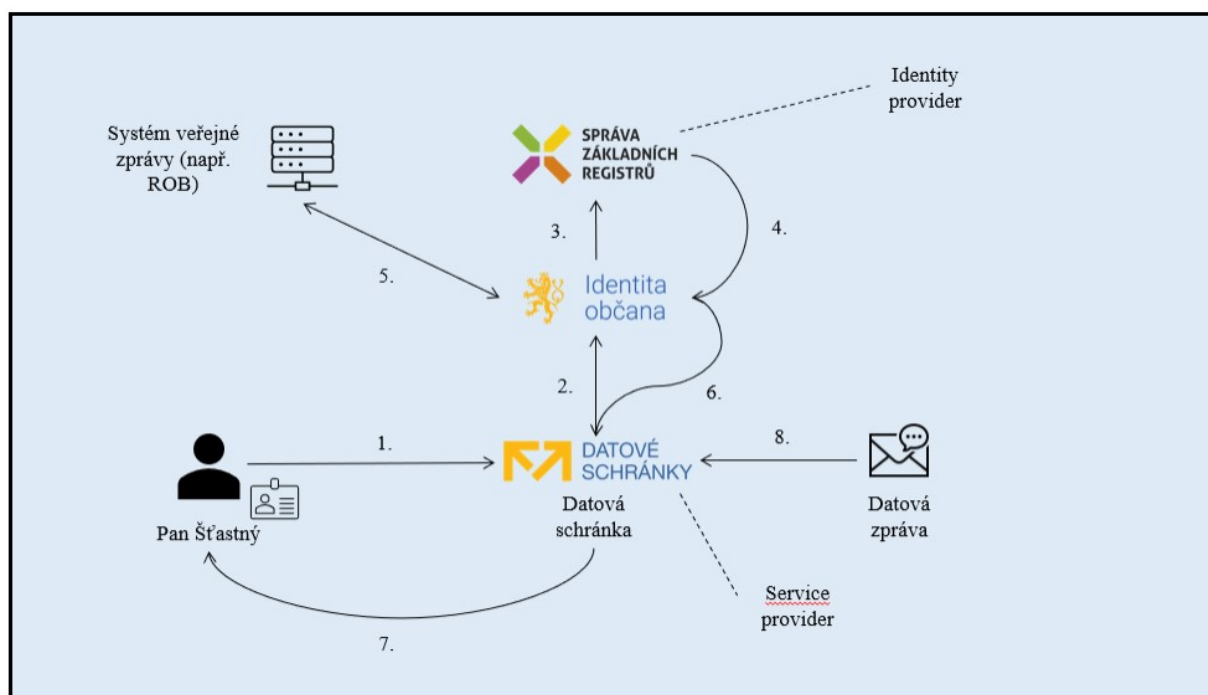
Ve státním systému e-ID je hned několik identity providerů. K uzavření rukopisu práce se jedná o Digitální a informační agenturu se svým prostředkem Mobilní klíč eGovernmentu a NIA ID, dále Ministerstvo vnitra České republiky se svou eObčankou (občanský průkaz s čipem⁹¹), První certifikační autoritu, a.s. se svou čipovou kartou STARCOS a CZ.NIC, z.s.p.o., s MojeID⁹².

Mezi service providery lze v státním systému zařadit celou škálu subjektů, které poskytují různé on-line služby, pro něž je zcela zásadní elektronická identifikace, od státní správy přes různé obce až po státní podniky jako Česká pošta, anebo i Notářskou komoru České republiky.⁹³

Mezi identity providery a service providery ve státním e-ID se řadí Národní identitní autorita (dále jako „NIA“) jako organizace provádějící autentizaci procesu elektronické identifikace.

3.1.1.1 Příklad elektronické identifikace ve státním e-ID

Pro snazší pochopení procesu elektronické identifikace uvnitř systému státní e-ID poslouží příklad pana Šťastného, který se chce přihlásit do své datové schránky za účelem získání přijaté datové zprávy:



Příklad začíná panem Šťastným, který do své osobní schránky obdrží e-mail informující ho o nové datové zprávě v jeho osobní datové schránce. Tu si pan Šťastný chce převzít.

⁹¹ Všechny občanské průkazy vydané po 1. 1. 2018 v sobě mají čip obsahující informace potřebné pro elektronickou identifikaci.

⁹² Aktuální seznam identity providerů ve státním e-ID. 25.06.2021. Dostupné na: <https://info.identitaobcana.cz/KvalifikovaniSpravci.aspx>

⁹³ Aktuální seznam service providerů ve státním e-ID. 25.06.2023. Dostupné na: <https://info.identitaobcana.cz/sep/>

1. Za tímto účelem pan Šťastný navštíví webovou stránku Datové schránky⁹⁴, kde si pro přihlášení vybere možnost Identitu občana.
2. Po vybrání způsobu identifikace je pan Šťastný k přesměrován na portál NIA. Na portálu NIA si pan Šťastný z nabízených možností vybere eObčanku od Ministerstva vnitra a je přesměrován k identity providerovi, který jeho prostředek elektronické identifikace vydal, v našem případě případech Správě základních registrů.
3. Poté se musí pan Šťastný u svého identity providera prokázat vložení své eObčanky do čtečky.
4. Správa základních registrů předá NIA potřebné údaje o panu Šťastném, pomocí nichž je NIA schopna dohledat ho v systému veřejné správy a ověřit jeho totožnost.
5. NIA na základě dat získaných od identity providera a dat předložených panem Šťastným autentizuje přihlášení pana Šťastného s údaji v databázi veřejné správy.
6. Výsledek svého zjištění (identifikace se shoduje/neshoduje) NIA předá Informačnímu systému datových schránek, tj. service providerovi.
7. Service provider následně informuje pana Šťastného o jeho úspěšném přihlášení (v případě správných údajů – jinak přihlášení zamítne) a vpustí pana Šťastného do rozhraní systému datových schránek.
8. Pan Šťastný se po úspěšném přihlášení může dostat ke své doručené datové zprávě.

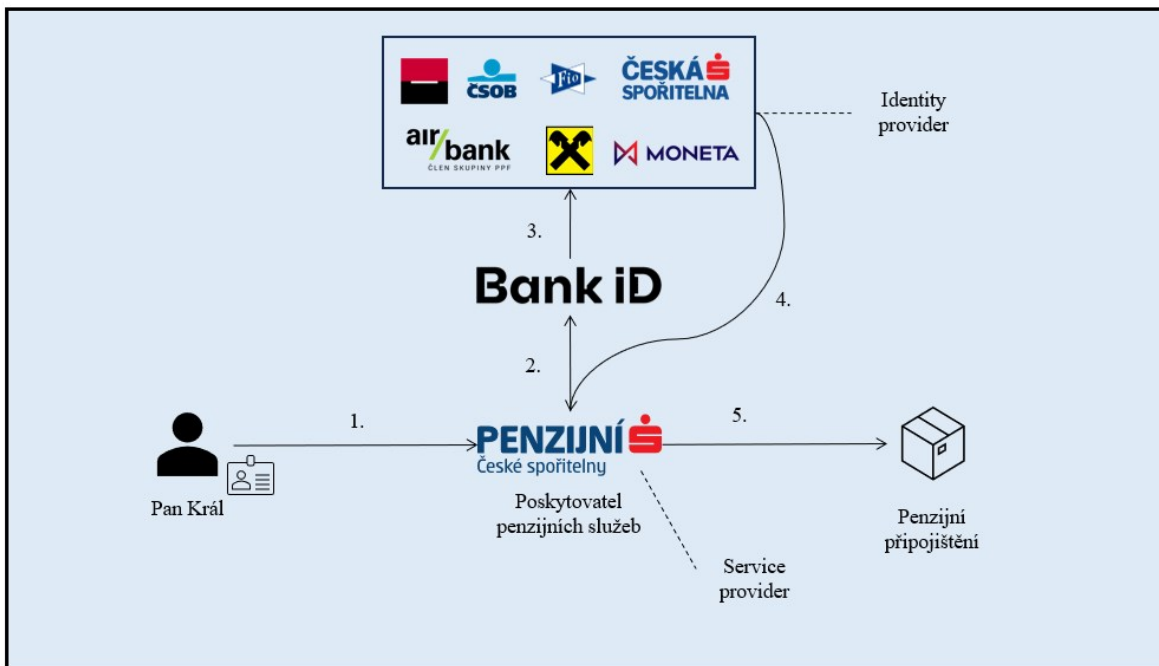
3.2 Bankovní e-ID

Bankovní identita či také Bank-ID je soukromoprávní alternativou k státnímu systému elektronické identifikace, který vznikl za účasti několik bank působících v České republice. Jeho systém je obdobný tomu státnímu s rozdílem, že identity providerů je zde hned několik, a to vždy podle toho, kde má daná osoba zřízení bankovní účet, resp. kde u dané osoby proběhla prvotní (fyzická) identifikace.

3.2.1 Příklad elektronické identifikace v Bank-ID

V tomto případě si pan Král chce sjednat penzijní připojištění u poskytovatele penzijních služeb. Sjednat si jej lze i online, ale pouze za využití Bankovní identity. K tomu dojde následujícím procesem:

⁹⁴ <https://info.mojedatovaschranka.cz/info/cs/>



1. Pán Král se rozhodne sjednat si penzijní pojištění od dceřiné společnosti České spořitelny online. Za tímto účelem navštíví její online portál.⁹⁵
2. Po úspěšném vyplnění výše spoření a zodpovězení všech ostatních finančních otázek je pan Král vyzván k identifikaci. Pan Král se rozhodne identifikovat pomocí Bank ID. Po zvolení této možnosti je mu nabídnuta volba z řady bank, které identifikaci pomocí Bank ID umožňují.
3. Pan Král si vybere svou banku, která mu následně ukáže standardní přihlašovací okno do jeho online bankovníctví.
4. Po úspěšném přihlášení do bankovníctví dojde k odeslání výsledku identifikace (identifikován/neidentifikován) do dispozice service providera.
5. Service provider výsledek zobrazí na monitoru pana Krále a v případě úspěšné identifikace dojde ke sjednání penzijního pojištění.

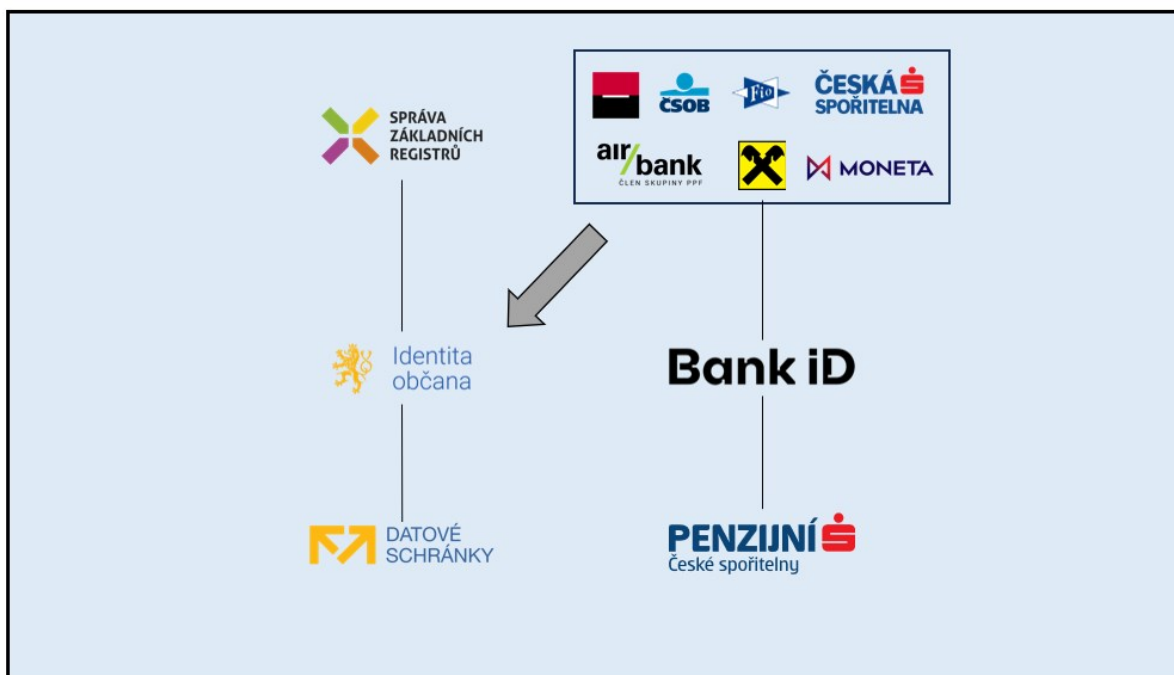
3.3 Interoperabilita státního a bankovního e-ID

Systémy státní identifikace a systému bankovní identifikace jsou sice samostatné systémy elektronické identifikace, ale lze využít jejich vzájemné kombinace, kdy se identifikující osoba může státu identifikovat skrze svou bankovní identitu. V příkladu pana Šťastného, který se chce přihlásit do své datové schránky, lze využít Bank ID.

3.3.1 Příklad využití Bank-ID při přihlašování do státem poskytovaných služeb

⁹⁵ <https://www.csps.cz/cs/penzijni-sporeni>

Rozdílem v celém procesu je, že zdrojem dat, resp. identity providerem bude přímo banka samotná a nikoli bankovní identita, která je jakýmsi agregátem pro všechny banky v případě služeb v soukromoprávním světě. To znamená, že v případě identifikace přes NIA dojde k výběru identifikace pomocí bankovní identity, která rovnou zpřístupní přihlašování bankovníctví v konkrétní bance. Ta po úspěšném přihlášení předá potřebná osobní data NIA. Poté je proces již standardní, jak je popsán výše.



4 Alternativy bankovní identity pro elektronickou identifikaci

Vedle zde uváděné elektronické identifikace, a to ať už poskytované státem, respektive státy EU, nebo soukromoprávní, jako je bankovní identita, existuje celá řada možností, které jsou pro určitou formu identifikace nebo elektronické identifikace stále užívané nebo je v minulosti bylo možné využít. Některé z nich zákon zná a připouští k určité formě identifikace, některé jsou pouze výsledkem aktuálních potřeb a vývoje trhu.

Zásadním rozdílem oproti výše popsané elektronické identifikaci je, že u většiny níže popsaných identifikací je identifikace prováděna ve dvoustranném procesu, tj. v procesu, kde vedle osoby provádějící identifikaci a osoby identifikované absentuje třetí strana kontrolující poskytovaný prostředek elektronické identifikace. U těchto dnes již alternativních způsobů identifikace také dochází k ukládání osobních dat u daného poskytovatele služeb, tedy k něčemu, čemu se Evropská komise dlouhodobě snaží zabránit. Oba tyto aspekty jsou identifikované Komisí jako problematické pro osoby poskytující identifikační prostředky a pro rozvoj poskytování služeb online obecně, jak bylo popsáno v Digitální agendě pro Evropu.⁹⁶

Níže jsou popsány a s elektronickou identifikací podle nařízení eIDAS porovnány vybrané způsoby identifikace.

4.1 Fyzická přítomnost

Identifikace za fyzické přítomnosti je, jak již bylo řečeno v úvodu práce, nejstarším a nejčastějším způsobem identifikace.

Tento způsob identifikace právní řád umožňuje v § 8 odst. 1 AML zákona, přičemž považuje identifikaci za fyzické přítomnosti identifikovaného za fakticky jediný možný způsob prvotní identifikace s ohledem na výrazně vyšší bezpečnost a zajištění naplnění smyslu a účelu identifikace jako takové. Smyslem a účelem identifikace je dle mého názoru primárně zamezit pohybu nelegálně získaného kapitálu, ostatně tomuto názoru svědčí i samotný anglický název zákona „*Anti-money laundering*“, tj. AML, a taktéž zamezit využívání určitých služeb, které zákonodárce považuje za kritické či jinak významné, osobami, jejichž totožnost nebyla jednoznačně prokázána.

Ustanovení § 8a AML zákona sice připouští nahrazení identifikace za fyzické přítomnosti identifikovaného identifikací pomocí prostředku pro elektronickou identifikaci, ale jak již bylo v této práci uvedeno, prostředek pro elektronickou identifikaci je možné získat pouze za

⁹⁶ Sdělení Evropské komise, Digitální agenda pro Evropu, 26. srpna 2010 [online] Brusel: Evropská komise, 2010 [cit. 23.06.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/cs/ALL/?uri=CELEX:52010DC0245>

předpokladu prvotní identifikace za fyzické přítomnosti. Ustanovení § 8a AML zákona tedy pouze umožňuje převzít prvotní identifikaci, která proběhla za fyzické přítomnosti identifikovaného u jiného subjektu poskytujícího služby k dalšímu subjektu, u nějž taktéž musí proběhnout identifikace.

Zásadním nedostatkem tohoto způsobu identifikace je jeho místní a časové omezení s ohledem na neustálé propojování celosvětového obchodního prostoru a jeho přechodu do online prostředí. Jak ve vztahu B2B, tak B2C je pro účely dalšího rozvoje nutné umožnit identifikaci osob i jiným způsobem, než je identifikace osoby za její fyzické přítomnosti identifikovaného.

4.2 Zprostředkovaná identifikace

Zprostředkovanou identifikací je podle § 10 AML zákona míněna situace, kdy identifikaci osoby provede nikoli osoba povinná provést identifikaci, ale jiná osoba k tomu zákonem oprávněná, která o takové identifikaci může vydat veřejnou listinu. Mezi tyto zmocněné osoby můžeme řadíme notáře (včetně zahraničních) a vybrané orgány veřejné správy, v právním řádu se pro tyto pojmy využívá pojem *kontaktní místo veřejné správy*⁹⁷. V obecné mluvě je takové místo označované mnohdy jako CzechPOINT.

Zprostředkovaná identifikace tak je pouze přenesením běžné identifikace za fyzické přítomnosti na další, zákonem předem taxativně vymezené osoby.

Vedle náležitostí uvedených v § 10 odst. 2 AML zákona musí veřejná listina obsahovat údaj o tom, pro koho byla zprostředkovaná identifikace provedena, např. pro konkrétního advokáta apod. Z toho lze soudit poměrně výrazné omezení využití takové identifikace, kdy pro každou jednotlivou identifikaci musí identifikovaná osoba provést vymezení využití takové identifikace. Dle mého názoru se jedná o rozumné a pochopitelné opatření ze strany zákonodárce, avšak tento aspekt působí značně restriktivně a omezuje praktické využití. Lze se domnívat, že nejde o nejčastěji používanou metodu.

Výsledkem je sice praktické usnadnění identifikace navýšením počtu míst, kde lze identifikaci osoby provést, ale stále se jedná o nedostatečnou odpověď na proměnu způsobu fungování trhu.

4.3 Převzatá identifikace

Oproti zprostředkované identifikaci je postup podle § 11 AML zákona, tzv. převzatá identifikace, spojena s postoupením jednou již učiněné identifikace mezi povinnými osobami provádějícími identifikaci. K takovému procesu je nutný souhlas identifikované osoby

⁹⁷ Srov. např. ustanovení § 4 písm. a) ZoB.

a přijímající povinná osoba musí být takovou identifikaci ochotna přijmout. Přejímající povinná osoba má navíc zachovanou plnou odpovědnost za správnost a kompletnost provedené identifikace.

Tento proces je v odborných publikacích či různých článcích někdy označován jako *řetězení*.

Faktickým rozdílem mezi identifikací převzatou a zprostředkovanou je absence vzniku zvláštní veřejné listiny pro účely jednotlivé identifikace. Dochází k předání identifikace samotné (to v praktické rovině může být kopie osobních dokladů, podpisu a jiných osobních dat identifikované osoby) mezi povinnými osobami.

Jistým omezením možností převzetí identifikace je, že převzít lze pouze identifikaci provedenou za fyzické přítomnosti identifikované osoby anebo elektronickou identifikaci. Zákon pak ještě stanoví speciální režim pro advokáty a notáře. Tyto povinné osoby mohou identifikaci převzít pouze od povinné osoby stejného typu (tedy od jiných advokátů nebo notářů, a to včetně zahraničních).

Převzatá identifikace tak již nakročuje vstříc dnešní realitě, ale stále ztělesňuje značné nedostatky v podobě nemožnosti volného využití identifikace u jakéhokoli dodavatele služeb/produktů. Převzít identifikaci lze pouze mezi osobami veřejného práva, resp. kontaktními místy veřejné správy.

4.4 Penny Transfer

Penny transfer, či v českém jazyce taktéž někdy označován jako korunová nebo alternativně haléřová platba, je jednou z dalších způsobů dálkové identifikace, který pro méně rizikové situace připouští AML zákon.⁹⁸

Jedná se o postup identifikace, kde nedochází k samotné identifikaci identifikované osoby, ale k prokázání existence platebního účtu vedeného na jeho jméno u úvěrové instituce působící na území členského státu Evropské unie nebo v Evropském hospodářském prostoru.

Identifikovaná osoba prokáže existenci takového účtu prostou platbou, typicky platbou té nejmenší možné hodnoty (v českém prostředí jedné koruny či jednoho haléře, v anglosaských zemích se bude jednat o jedno penny; od toho je odvozen název tohoto způsobu identifikace).

Tento způsob identifikace je vzhledem k rychlosti a jednoduchosti plateb online jedním z nejrychlejších způsobů identifikace, avšak je nutné přiznat, že se jedná o způsob, který je

⁹⁸ Srov. ustanovení § 11 odst. 7 písm e) AML zákona.

zcela nevhodný pro faktické prokázání totožnosti. Samotný proces přijímající straně totiž pouze prokáže existenci účtu, nikoli však existenci a identifikaci platící osoby.

4.5 Bring-your-own-identity

Bring-your-own-identity, či také BYOI, je jedna z možností, kterou dnešní český právní řád nezná, ale jedná se o prvek, který je značně rozšířen a masově používán v dnešní online komunikaci a běžném online fungování. Jeho vysoká četnost je pravděpodobně zapříčiněna značným ulehčením a potřebou znalosti pouze jednoho přihlášení, díky kterému je možné získat škálu služeb a produktů.

Postup předpokládá, že v procesu identifikace a autentizace u poskytovatele služeb nebo produktů identifikovaná osoba použije „vlastní“ systém identifikace pomocí externí služby, která již kvazi identifikaci provedla. Bude se jednat například o poskytnutí identifikace pomocí zřizovatele e-mailové schránky (např. Google) nebo zřizovatele sociální sítě (např. Facebook).

Fakticky proces vypadá následovně:

- i. osoba chce zakoupit určitou službu nebo produkt, pro něž je nutné se identifikovat (např. zřídit si online účet u zahraničního poskytovatele hazardních her),
- ii. pro svou identifikaci si osoba vybere některou z nabízených služeb, např. přihlášení do služby G-mail od společnosti Google,
- iii. po přihlášení a odsouhlasení předá Google vybrané informace poskytovateli, který data převezme bez dalšího ověření, a v případě domnělého splnění kritérií (věk) umožní identifikované osobě danou službu nebo produkt koupit.

Jak je patrné tento proces má hned několik vážných nedostatků. Patrně nejzásadnější je, že v drtivě většině subjekt, který předává data o identifikované osobě, nemá tato data dostatečně ověřená a v mnoha situacích je ověřit ani nemůže, protože se jedná o subjekt soukromého práva bez přístupu k potřebným registrům. Tento proces ve svém postupu tvoří kopie dat, které předává do rukou dalších subjektů, jež s daty dále pracují a spoléhají se na ně. Dochází tak k ohrožení bezpečnosti citlivých dat identifikované osoby. Taktéž může být osoba, která předává osobní data, usídlena mimo některý z členských států Evropské unie nebo Evropského hospodářského prostoru, a fakticky nebude podléhat její regulaci ani sankcím nebo možné kontrole.

Běžným uživatelům internetu je zcela jasné, že tento postup taktéž umožňuje falšovat vstupní data, kdy většina provozovatelů e-mailů či sociálních sítí nikde neověřuje věk, jméno či

jakýkoli jiný údaj identifikované osoby. Je tak poměrně snadné vytvořit účet pod cizím jménem a s ním tak zcela smyšlenou identitu.

Jak bylo popsáno, je tento způsob identifikace sice vysoce flexibilní a umožňuje výrazné zjednodušené celého procesu identifikace, avšak zjednodušen je až v takové míře, že dochází k ohnutí základního smyslu a účelu identifikace, a to nezpochybnitelného ztotožnění konkrétní osoby.

4.6 Video/fotografie

Jednou z poměrně často rozšířených metod je použití videa či aktuální fotografie identifikované osoby. Fakticky se ale nejedná o samostatný proces identifikace, ale doprovodnou metodu jednoho z dalších způsobů vzdálené identifikace podle § 11 odst. 7 písm. a) AML zákona, kdy dochází ke kontrole identifikace. Identifikovaná osoba zašle kopie dvou svých dokladů a poskytovatel služby či produktu si taktéž vyžádá fotografii či několikavteřinové video identifikované osoby jako podklad pro identifikaci a předejití možného zneužití dokladů totožnosti.

Jako praktický příklad využití této metody lze uvést společnost www.scio.cz, s.r.o., IČO 271 561 25, která je poskytovatelem služby přijímacích zkoušek pro střední a vysoké školy. V době pandemie covidu-19 umožňovala zkoušejícím provést zkoušku z domova, a to za předpokladu spuštění videokamery v průběhu zkoušky a zpřístupnění osobního dokladu, pomocí nichž došlo k identifikaci zkoušející osoby.

5 Možné využití elektronické a bankovní identifikace v budoucnosti a očekávaný vývoj legislativy

5.1 eDIAS 2.0

Vedle různých vesměs drobných legislativních počinů českého zákonodárce, který více či méně zpřesňuje dosavadní legislativu upravující elektronickou identifikaci a bankovní identifikaci, např. novelizačního zákona č. 261/2021 Sb. či zákona č. 471/2022 Sb., nedochází na úrovni České republiky k žádnému významnému posunu v této oblasti. Bohužel k posunu nedochází ani na úrovni odborných diskusí, politických proklamací či jiných aktivit. Lze se tak domnívat, že Česká republika včetně své odborné veřejnosti zcela ponechala tuto disciplínu v rukách Evropské komise a jejích orgánů a bude pouze přejímat politiku a rozhodnutí, které bude celoevropským řešením.

Na druhé straně se Evropská komise již několik let připravuje na aktualizaci nařízení eIDAS,

tzv. eIDAS 2.0, které má za cíl podstatné rozšíření využití elektronické identifikace a jemu přidružených nástrojů do každodenní činnosti občanů EU, a to nejenom při komunikaci se státem nebo bankami (v případě využívání veřejnoprávních služeb), ale také při registraci či komunikaci u ryze soukromoprávních poskytovatelů služeb.

Jak bylo zmíněno výše, dne 3. června 2021 publikovala Evropská komise Zprávu o hodnocení nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, kterou měla povinnost sestavit a publikovat podle čl. 49 nařízení eIDAS (dále jako „Zpráva“).⁹⁹

Zpráva uvádí, že základem nařízení je čl. 114 SFEU, na jehož základě si Evropské komise pro nařízení eIDAS vymezila 4 základní cíle:

- rozvoj jednotného trhu,
- rozvoj klíčových přeshraničních veřejných služeb,
- posílení hospodářské soutěže na jednotném trhu,
- maximalizaci uživatelské přívětivosti (pro občan a podniky).

Dle Zprávy se nařízení eIDAS podařilo cílů v mnohém dosáhnout nebo se jim alespoň výrazně přiblížit, avšak identifikuje nedostatky, které se stávají základem pro revizi nařízení eIDAS v podobě nařízení eIDAS 2.0. Tyto identifikované nedostatky jsou:

- absence povinnosti oznamovat vnitrostátní režimy elektronické identifikace,
- omezená sada osobních údajů (a s tím spojené omezení využití elektronické identifikace),
- omezení se pouze na veřejné subjekty a nedostatečné provázání se soukromoprávním sektorem,
- nedostatečné sjednocení úrovně záruk v jednotlivých členských státech EU.

Zpráva připouští, že od roku 2014, kdy bylo nařízení eIDAS přijato, došlo k podstatným změnám ve společnosti, a to jak z pohledu politických očekávání v oblasti ochrany osobních údajů ze stran států, tak ve způsobu chování společnosti v online prostředí. Díky neustále rostoucímu trhu v online prostoru (e-commerce) dochází k soustavnému zvyšování rizik při fungování online. Nařízení eIDAS je svou koncepcí založeno na jednotlivých a samostatných systémech elektronické identifikace uvnitř jednotlivých členských států, které jsou vzájemně

⁹⁹ Úřední věstník Evropské unie [online] Brusel 2021 [cit. 24.06.2023]. Dostupné z: https://eur-lex.europa.eu/search.html?lang=cs&SUBDOM_INIT=ALL_ALL&DTS_DOM=ALL&type=advanced&DTS_SUBDOM=ALL_ALL&qid=1687642490244&LB=32014R0910&SELECT=LB_DISPLAY&sortOne=LEGAL_RELEVANCE_SORT&sortOneOrder=desc&page=2

propojené skrze jednotící evropskou linku. Bohužel jsou tyto samostatné jednotky řízeny různými normami, které jsou v mnohém rozdílné, a dochází k tak nejednotnosti s ohledem na úroveň záruk elektronických systémů, ale také palety možných služeb, které občan daného členského státu může skrze elektronickou identifikaci využít. Počet oznámených systémů elektronické identifikace o neuspokojivém stavu taktéž svědčí. K datu publikace Zprávy bylo dosud oznámeno pouze 14 členskými státy alespoň jeden režim elektronické identifikace, celkový počet oznámených systémů se rovná 19.

Zpráva taktéž připouští stále nevhodný způsob nakládání s daty, kdy identifikovaná osoba při identifikaci odevzdává celý balíček svých osobních dat, aniž by měla možnost omezit se pouze na ty údaje, které poslouží k dostatečné identifikaci, či vůbec mít možnost poskytnout pouze některá data.

V budoucnu lze očekávat požadavek vysoké míry bezpečnosti veškeré online činnosti ze strany občanů EU a podniků v EU, a to nejenom v podobě elektronické identifikace nebo služeb vytvářející důvěru, ale taktéž při podávání daňových přiznání, přihlašování se na vysoké školy, online založení bankovního účtu či žádostí o úvěry. K takovému stavu je zapotřebí podstatné rozšíření těchto služeb, aby rozdíl mezi fyzickým získáním služby a online získáním služby byl z pohledu bezpečnosti nerozeznatelný.

Zhruba v tomto duchu je tvořen dosavadní legislativní počín nařízení eIDAS 2.0.

Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, číslo jednací COM/2021/281 final (dále jako „**návrh eIDAS 2.0**“), taktéž někdy označováno jen jako revize nařízení eIDAS, přináší celou řadu významných změn.¹⁰⁰ Návrh eIDAS 2.0 je ke dni uzavření rukopisu této práce ve fázi trialogu mezi Evropským parlamentem, Evropskou komisí a zástupci Rady EU před prvním čtením v Parlamentu. Lze tak očekávat, že nařízení nebude přijato v dohledné době.

Obsah návrhu eIDAS 2.0. lze shrnout do následujících vět. Zásadní změnou oproti původnímu nařízení je jeho výrazné rozšíření, a to jak v paletě regulovaných služeb, tak v míře zásahu do každodenního života občanů EU. Dle mého názoru je největší změnou příchod tzv. evropské peněženky digitální identity, která by měla mít formu aplikace v mobilních zařízeních a byla

¹⁰⁰ Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, 3. června 2021 [online] Brusel: Evropská komise, 2021 [cit. 01.10.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281>

by univerzálně použitelná ve všech členských státech jako forma identifikace agregovaná na evropské úrovni, nikoli jako dosud na úrovni národní. Návrh také umožňuje zřízení elektronické identity pro osoby s trvalým pobytem v Unii či zřízení identity pro právnické osoby. Zde je nutné podotknout, že zahrnutí právnických osob již obsahovalo i nařízení eIDAS, ale k jeho realizaci z velké části nedošlo, například český právní řád takovou možnost vůbec nepřipouští. Je tak otázkou, zda se Evropské komisi podaří prosadit tento záměr do praxe.

Evropská peněženka nebude jen prostorem pro uložení elektronické identifikace, ale též řídičského průkazu, vysokoškolského diplomu, rodného listu i lékařských záznamů apod. Uživatel pak sám rozhodne, jaké údaje poskytne třetí straně, ale také jaké údaje do peněženky nahraje. Takto zanesené údaje mají mít univerzální platnost skrze celou EU. Aspekt volnosti nakládání s údaji na straně uživatele je také označován jako „decentralizovaná identita“.¹⁰¹

Univerzálností evropské peněženky by tak mělo v dlouhodobém horizontu omezit vzniku „bring-your-own-identity“ a s tím spojené problémy (viz 4.5 této práce). Dojde tak k výraznému posílení postavení jednotlivce při nakládání s osobními údaji při pohybování se v online prostředí.

Z návrhu eIDAS 2.0 lze také vyčíst, že žádný ze zúčastněných subjektů na identifikaci nebude moci obdržet jakékoli informace o četnosti nebo způsobu využití informací v dané peněžence, tj. půjde údaje jakkoli dále využít, např. pro cílené marketingové služby.

Jak je už patrné z výše uvedeného, peněženka bude mít univerzální použití, bude ji možné použít při registraci či získávání služeb u soukromoprávních poskytovatelů služeb. Synergickým efektem je bezplatnost a dobrovolnost peněženky, lze tak předpokládat, že nedojde k žádnému drastickému omezení již existujících možností.¹⁰²

V České republice již dochází k postupné realizaci příprav na přijetí návrhu eIDAS 2.0 v podobě projektu eDokladovka, která by měla být jistou přípravou na onu elektronickou peněženku podle návrhu eIDAS 2.0 a do níž by se postupně implementovaly technické požadavky schváleného nařízení. Podle dostupných zpráv by tato česká varianta měla mít

¹⁰¹ KOVÁŘ D., AMLER P., Už jste slyšeli o nařízení eIDAS 2.0? epravo.cz [online]. 22.01.2022 [cit. 01.10.2023]. Dostupné z: <https://www.epravo.cz/top/clanky/uz-jste-slyseli-o-narizeni-eidas-20-113866.html>

¹⁰² eIDAS 2.0 – velký krok pro digitalizaci? Sedlakova legal [online]. 04.08.2022 [cit. 01.10.2023]. Dostupné z: <https://www.sedlakovalegal.cz/cs/eidas2>

prozatím možnost uchovat občanský a řidičský průkaz s možností postupného rozšiřování.^{103,104}

¹⁰³ Blíží se eDokladovka. Česko za rok spustí digitální peněženku. iDnes [online]. 12.12.2022 [cit. 01.10.2023]. Dostupné z:

https://www.idnes.cz/ekonomika/domaci/edokladovka-digitalni-penezenka-bartos-egovernment.A221212_153202_ekonomika_akp

¹⁰⁴ Občanka v mobilu: Obavy nejsou na místě. Kdyby nás stát chtěl sledovat, může to dělat už teď, říká Koubský. iRozhlas [online]. 27.05.2023 [cit. 01.10.2023]. Dostupné z: https://www.irozhlas.cz/veda-technologie/technologie/obcanka-v-mobilu-edokladovka-e-doklady_2305271343_pj

6 Závěr

Ze všeho zde uvedeného se domnívám, že nařízení eIDAS bylo velkým krokem směrem k digitalizaci Evropské unie a digitalizace mnohých států. Cíle tohoto nařízení se sice nepodařilo za skoro jednu dekádu zcela naplnit, ale podařilo se k nim významně posunout. Díky nařízení eIDAS existuje evropský rámec pro společnou identifikaci a také došlo k umožnění přenesení identifikace do podnikatelského prostředí, což se v případě České republiky ukázalo jako klíčové pro popularizaci tohoto nástroje.

Česká republika, ale i členské státy obecně bohužel dlouhodobě ukazují svou rigiditu vůči neustále se proměňující společnosti, která pravděpodobně chce mít veškerou byrokracii v podobě jednoduché a přehledné aplikace, pomocí níž se za pár kliků dostane ke všem službám, které státu zajišťuje.

Elektronická identifikace tak v České republice funguje, je masivně využívána, výrazně přispěla k dosažení cíle digitálního státu a mimo jiné tak pravděpodobně výrazně ulehčila mnoha úřadům ale zejména uživatelům elektronické identifikace. Bohužel, jak již bylo řečeno v práci samotné, tohoto výsledku dosáhl soukromý sektor, kterému právní řád a zákonodárce výjimečně nepřekážel, ač je nutné přiznat, že ani takové řešení není zdaleka vhodné.

Taktéž je patrná snaha reflexe vlastních činů Evropské komise, resp. EU, která si pomocí svých zpětných mechanismů kontroly uvědomuje svou zaostalost za technologickým rozvojem a potřebami trhu. Toto uvědomění materializuje ve svém návrhu eIDAS 2.0, který se alespoň v této podobě jeví jako zcela formující prvek budoucí podoby komunikace občanů se státem a mnoha poskytovateli služeb a produktů online.

Domnívám se, že cílů, které si Evropská komise předsevzala, bude velice obtížné dosáhnout, a to už jen při uvědomění si podstaty existence práva samotného, které je reakcí na existující situaci, kterou se zákonodárce rozhodl upravit a svázat určitým souborem pravidel. V praktické rovině to tak znamená, že právo bude vždy nedostižně stíhat aktuální situaci.

7 Seznam používaných zkratk

Agentura	Digitální informační agentura
AML zákon	zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
Bankovní společnost	Bankovní identita, a.s., IČO: 095 13 817, se sídlem Smrčkova 2485/4, Libeň, 180 00 Praha 8
ČNB	Česká národní banka
FAÚ	Finanční analytický úřad
nařízení eIDAS	nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
návrh eIDAS 2.0.	Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu
NIA	Národní identitní autorita
prováděcí akt INT	Prováděcím aktu Evropské komise (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 Nařízení eIDAS
prováděcí akt MTS	Prováděcího nařízení Evropské 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 eIDAS
SFEU	Smlouva o fungování Evropské unie
směrnice ZpEP	Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy
ZoB	zákon č. 21/1992 Sb., o bankách
ZoBI	zákon č. 49/2020 Sb., o bankovní identitě
ZoEI	zákon č. 250/2017 Sb., o elektronické identifikaci
ZoP	zákon č. 277/2009 Sb., o pojišťovnictví
ZoŽp	zákon č. 455/1991 Sb., o živnostenském podnikání
Zpráva	Zpráva o hodnocení nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu

8 Seznam zdrojů

Právní předpisy

- zákon č. 29/1946 Sb., kterým se zavádějí pracovní průkazy
- zákon č. 198/1948 Sb., o občanských průkazech
- zákon č. 455/1991 Sb., o živnostenském podnikání
- zákon č. 21/1992 Sb., o bankách
- zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
- zákon č. 277/2009 Sb., o pojišťovnictví
- zákon č. 250/2017 Sb., o elektronické identifikaci
- zákon č. 49/2020 Sb., o bankovní identitě
- nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy
- Prováděcího nařízení Evropské 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 eIDAS
- Prováděcího nařízení Evropské komise (EU) 2022/960, kterým se opravuje české znění prováděcího nařízení (EU) 2015/1502, kterým se stanoví minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 Nařízení eIDAS
- Smlouva o fungování Evropské unie
- Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu

Sněmovní tisky

- Sněmovní tisk 1069 – Vládní návrh zákona o elektronické identifikaci – EU. 21.03.2017. Dostupné z: <https://www.psp.cz/sqw/historie.sqw?o=7&T=1069>
- Sněmovní tisk 554 [online]. Poslanecká sněmovna, 12.07.2019 [cit. 27.07.2023]. Dostupné z: <https://www.psp.cz/sqw/historie.sqw?o=8&T=554>

Knihy a komentáře

- MARÁZ, Karel. Sfragistika: studijní texty pro posluchače pomocných věd historických a archivnictví. Brno: Masarykova univerzita, 2014. ISBN 978-80-210-7143-8
- STRAUS Jiří a kol. Dějiny Československé kriminalistiky slovem i obrazem. Praha: POLICE HISTORY, 2003, ISBN: 80-86477-18-5.
- HLAVINOVÁ, Markéta, PILÍKOVÁ, Jaroslava, KABEŠ, Viktor. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. 3. vydání. Praha: C. H. Beck, 2022
- PERHÁČOVÁ, M., VESELSKÝ, Š. Zákon o bankovní identitě: Komentář. [Systém ASPI]. Wolters Kluwer [cit. 2023-11-29]. ASPI_ID KO49_2020CZ. Dostupné z: www.aspi.cz. ISSN 2336-517X.

Články a jiní internetové odkazy

- DLUBALOVÁ, Klára. Počet elektronických Identit občanů překonal hranici 10 milionů [online]. Web Ministerstva vnitra. [cit. 27.10.2023]. Dostupné z: <https://www.mvcr.cz/clanek/pocet-elektronickyh-identit-obcanu-prekonal-hranici-10-milionu.aspx>
- KORBEL F., KOVÁŘ D. Právní úprava tzv. bankovní identity [online]. Advokátní deník online, 09.05.2021 [cit. 27.07.2023]. Dostupné z: <https://advokatnidenik.cz/2021/05/09/pravni-uprava-tzv-bankovni-identity-2/>
- SOVOVÁ E. Průlom: o digitální občanku je velký zájem, šetří čas a ulehčuje život [online]. iDnes.cz, 19.04.2021 [cit. 27.07.2023]. Dostupné z: https://www.idnes.cz/finance/financni-radce/bankovni-identita-banky-digitalni-obcanka-overovani.A210416_084442_viteze_sov
- SKALKOVÁ O. Bankovní identita znamená průlom v on-line ověřování totožnosti [online]. Hospodářské noviny, 14.04.2021 [cit. 27.07.2023]. Dostupné z: <https://archiv.hn.cz/c1-66903310-bankovni-identita-znamena-prulom-v-on-line-overovani-totoznosti>
- GURČOVÁ K. 6 největších legislativních ležáků. Které zákony politici uložili k ledu, ačkoli je po nich poptávka? [online]. iRozhlas 22.05.2017 [cit. 27.07.2023]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/6-nejvetsich-legislativnich-lezaku-ktere-zakony-politici-ulozili-k-ledu-ackoli_1705220600_kno
- eIDAS 2.0 – velký krok pro digitalizaci? Sedlakova legal [online]. 04.08.2022 [cit. 01.10.2023]. Dostupné z: <https://www.sedlakovalegal.cz/cs/eidas2>

- KOVÁŘ D., AMLER P., Už jste slyšeli o nařízení eIDAS 2.0? epravo.cz [online]. 22.01.2022 [cit. 01.10.2023]. Dostupné z: <https://www.epravo.cz/top/clanky/uz-jste-slyseli-o-narizeni-eidas-20-113866.html>
- Blíží se eDokladovka. Česko za rok spustí digitální peněženku. iDnes [online]. 12.12.2022 [cit. 01.10.2023]. Dostupné z: https://www.idnes.cz/ekonomika/domaci/edokladovka-digitalni-penezenka-bartos-egovernment.A221212_153202_ekonomika_akp

Nelegislativní akty

- Sdělení Evropské komise, Digitální agenda pro Evropu, 26. srpna 2010 [online] Brusel: Evropská komise, 2010 [cit. 23.06.2023]. Dostupné z: <https://eur-lex.europa.eu/legal-content/cs/ALL/?uri=CELEX:52010DC0245>
- Zpráva o hodnocení nařízení (EU) č. 910/2014 o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu

Video

- 03_ Bank ID a ověřování identity, autentizace, Marek Růžička. Youtube [online]. 14.10.2022 [cit. 29.07.2023]. Dostupné z: <https://www.youtube.com/watch?v=PxYPQj-FiNM&t=579s>