

**M A S A R Y K O V A
U N I V E R Z I T A**

PRÁVNICKÁ FAKULTA

Elektronická identifikace

Diplomová práce

SEBASTIAN ŠPETA

Vedoucí práce: doc. JUDr. Radim Polčák, Ph. D.

Ústav práva a technologií
obor Právo

Brno 2019



Bibliografický záznam

Autor:	Sebastian Špeta Právnická fakulta, Masarykova univerzita Ústav práva a technologií
Název práce:	Elektronická identifikace
Studijní program:	PrF M-PPV Právo a právní věda
Studijní obor:	Právo
Vedoucí práce:	doc. JUDr. Radim Polčák, Ph. D.
Akademický rok:	2019
Počet stran:	76
Klíčová slova:	autentizace, eID, EIDAS, elektronická identita, elektronická identifikace, eSignature, identita, identifikace, OECD, služby vytvářející důvěru, UNCITRAL

Bibliografic record

Author: Sebastian Špeta
Faculty of Law, Masaryk University
Ústav práva a technologií

Title of Thesis: Electronic identification

Degree Programme: **PrF M-PPV Právo a právní věda**

Field of Study: Právo

Supervisor: doc. JUDr. Radim Polčák, Ph. D.

Academic Year: 2019

Number of Pages: 76

Keywords: authentication, eID, EIDAS, electronic identity, electronic identification, eSignature, identity, identification, trust services, OECD, UNCITRAL

Abstrakt

Tato práce se zabývá přeshraničním užitím systémů pro spolehlivou identifikaci osob ve veřejnoprávním a soukromoprávním styku. V práci je nejprve proveden výklad pojmu elektronické identifikace a analýza standardního systému elektronické identifikace. Práce se věnuje současným právním řešením se zaměřením na EIDAS a právní úpravu elektronické identifikace v České republice. Podrobný rozbor je věnován problému přeshraničního uznávání elektronických identit. Závěrečná část práce se věnuje rozboru a diskuzi aktuálních mezinárodních iniciativ pro přeshraniční elektronickou identifikaci.

Abstract

This thesis deals with cross-border use of systems for reliable identification of persons in public and private relations. At first, the concept of electronic identification and standard electronic identification system are analysed. The thesis deals with the current legal solutions focusing on EIDAS and electronic identification regulation in the Czech Republic. A detailed analysis is devoted to the problem of cross-border recognition of electronic identities. The final part is dedicated to the analysis and discussion of current international initiatives for cross-border electronic identification.

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma **Elektronická identifikace** zpracoval sám. Veškeré prameny a zdroje informací, které jsem použil k sepsání této práce, byly citovány v poznámkách pod čarou a jsou uvedeny v seznamu použitých pramenů a literatury.

V Praze 28. června 2019

.....
Sebastian Špeta

Poděkování

Na tomto místě bych chtěl poděkovat v první řadě doc. JUDr. Radimu Polčákovi, Ph.D., mému vedoucímu, za veškeré konzultace, rady a podněty, které mě dovedly ke zdárnému dokončení této práce. Mé díky patří též Martinovi za korekturu a nekonečnou trpělivost.

Obsah

Seznam pojmů a zkratk	13
1 Úvod	15
2 Elektronická identifikace – pojem a proces	17
2.1 Elektronická identita a elektronická identifikace	17
2.2 Procesy v systémech elektronické identifikace	20
2.3 Typy systémů elektronické identifikace.....	26
3 Přehled současných právních řešení	29
3.1 Evropská unie – nařízení EIDAS	29
3.2 Právní úprava na území České republiky.....	36
4 Přeshraniční spolupráce v oblasti elektronické identifikace	46
4.1 Analýza problému přeshraničního uznávání v oblasti elektronické identifikace	46
4.2 Řešení v rámci Evropské unie – povinnost vzájemného uznávání podle EIDAS	51
4.3 Přeshraniční spolupráce v České republice	56
5 Mezinárodní iniciativy v oblasti elektronické identifikace	58
5.1 OECD.....	58
5.2 UNCITRAL.....	59
6 Závěr	65
Použité zdroje	67
Monografie	67
Články	67
Internetové zdroje.....	70
Právní předpisy	73

Seznam pojmů a zkratek

AML zákon	– Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
EIDAS	– má význam uvedený v kapitole 3 této práce;
eSignature směrnice	má význam uvedený v kapitole 3 této práce;
KYC	– Know Your Customer
NIA	– Národní identitní autorita
OECD	– Organisation for Economic Co-operation and Development
UNCITRAL	– United Nations Commission on International Trade Law
ZOEI	– Zákon o elektronické identifikaci.

1 Úvod

Ve světě, který čím dál více závisí na elektronických transakcích a datech, přestávají být historické způsoby prokázání totožnosti (založené na papírových dokladech a interakci z očí do očí) zdaleka dostačující. Za tímto účelem došlo v internetovém prostředí k vytvoření řady systémů, které svým uživatelům umožňují s různou mírou jistoty identifikovat se elektronicky. Absence vzájemné komunikace a důvěry mezi těmito systémy však ve svém důsledku vedla ke vzniku nespočetného množství izolovaných systémů, jejichž vzájemná nekompatibilita nutí jejich uživatele zpravidla identifikovat se u každé služby, kterou chtějí využívat a fakticky si tak vytvářet stále nové elektronické identity.

Oblast elektronické identifikace zůstala po dlouhou dobu neupravena tradičním právem, převážně závislejícím na papírovém prostředí. Pionýrem v této oblasti se stalo Finsko, které v roce 1999 jako první země na světě zavedlo elektronické občanské průkazy.¹ Ty (a ostatní důvěryhodné systémy elektronické identifikace) umožňují jednoznačnou identifikaci osob nejen pro vzdálený přístup ke službám poskytovaným státem (eGovernment), ale mohou být přijímány a uznávány i ostatními subjekty veřejného i soukromého sektoru.

Protože v současné době existuje velké množství systémů pro elektronickou identifikaci, a to jak poskytovaných státy svým občanům, tak soukromoprávními poskytovateli, zaměřím se v této práci především na jejich přeshraniční použití, přičemž cílem této práce by mělo být právě zhodnocení současných řešení uznávání elektronických identit.

¹ RISSANEN, Teemu. Electronic identity in Finland: ID cards vs. bank IDs. Identity in the Information Society [online] Springer Netherlands, 2010, no. 3, no.1, p. 175-194. [cit. 2019-05-28] p. 176-177

Za tím účelem nejprve provedu výklad pojmu elektronické identifikace a analýzu standardního systému elektronické identifikace. Následně se budu zabývat současnou právní úpravou elektronické identifikace, přičemž primárně se budu věnovat právnímu řešení na území Evropské unie a České republiky. Než se zaměřím na současné přeshraniční způsoby elektronické identifikace na tomto území, provedu též analýzu problému přeshraničního uznávání elektronických identit. Protože řešení přeshraničního uznávání nelze dosáhnout na úrovni jednotlivých států, obzvláště v kulturně a ekonomicky nesourodém prostředí, provedu rozbor současných mezinárodních iniciativ věnujících se této oblasti, ve které hraje hlavní roli organizace UNCITRAL.

Vzhledem k partikulární úpravě elektronické identifikace na území jednotlivých států a do nedávné doby i absenci právní úpravy na území České republiky budu při zpracování tohoto tématu primárně vycházet ze zahraniční odborné literatury a výzkumů a záznamů z jednání probíhajících na půdě jednotlivých mezinárodních organizací. V práci se též pokusím zohlednit mé zkušenosti s používáním dostupných důvěryhodných způsobů elektronické identifikace, a nakonec i z mé účasti na jednáních UNCITRAL.

Přestože v praxi mohou být identifikovány i jiné entity než osoby, což může být jedním z významných aspektů *internetu věcí*, budu se v této práci věnovat pouze identifikaci osob, neboť relevantní právní úprava v této oblasti podle mého vědomí zatím neexistuje. Z důvodu limitace rozsahem této práce se nebudu věnovat službám vytvářejícím důvěru a ochraně osobních údajů, avšak domnívám se, že těmto oblastem již byl v odborných kruzích věnován dostatečný prostor.

2 Elektronická identifikace – pojem a proces

V této úvodní kapitole se nejprve pokusím vysvětlit samotný pojem elektronické identifikace a procesy, které jsou s elektronickou identifikací spojené. Následně se zaměřím na analýzu systémů elektronické identifikace a souvisejících procesů, která bude spočívat zejména v popisu a diskuzi o možných úskalích jednotlivých procesů, které jsou vlastní většině systémů elektronické identifikace. V závěru poskytnu přehled nejběžnějších typů systémů elektronické identifikace.

2.1 Elektronická identita a elektronická identifikace

Pojem identita, vycházejícího z latinského *identitas*, totožnost a je jazykově značně komplexním pojmem, vnímaným rozdílně v odlišných oblastech lidského poznání. Pro účely této práce budu za identitu považovat soubor dat a informací (atributů) spojených s danou osobou, jejichž kombinace umožňuje tuto osobu v daném kontextu dostatečně identifikovat a odlišit od jiných osob.² Identita osoby je ze své podstaty jedna, může však mít neomezené množství identifikačních prostředků. Elektronická identita je pak elektronickým vyjádřením analogové identity, a může být vytvořena kombinací analogových a elektronických

² Srov. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.150 - Legal issues related to identity management and trust services – Terms and concepts relevant to identity management and trust services* [online]. New York: United Nations, 2018. Distributed 6.2.2018 [cit. 30.10.2018]. s.5.

atributů.³ Světové ekonomické fórum elektronickou identitu popsalo jako:

„soubor jednotlivých atributů, které popisují entitu a určují, jakých transakcí se může účastnit.“⁴

Byť definicí elektronické identity existuje mnoho, tato podle mého názoru nejlépe napovídá o možnostech jejího využití. Elektronická identita totiž umožňuje osobám zúčastňovat se transakcí, během kterých je protistranám třeba prokázat, že jsou nositeli určitých atributů pro takovou transakci nezbytných.

Za účelem identifikace slouží v elektronickém prostředí namísto analogových dokladů takzvané prostředky elektronické identifikace. Zatímco analogové doklady slouží k identifikaci fyzicky přítomné entity, prostředek elektronické identifikace umožňuje její identifikaci vzdáleně.

Lze tedy shrnout, že v obecné rovině lze za elektronickou identifikaci považovat proces používání takových atributů v elektronické podobě, které určitou osobu v daném kontextu dostatečně identifikují, tedy – prokázání totožnosti s využitím elektronických prostředků.⁵

³ Srov. OECD. The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers. OECD Digital Economy Papers [online]. OECD Publishing, Paris, 2009. [cit. 30.11.2018] s. 6.

⁴ Srov. World Economic Forum. A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity [online]. World Economic Forum, 2016, [cit. 27.5.2019]. s. 41.

⁵ Článek 3 odstavec 1 EIDAS.

Z důvodu technického řešení těchto prostředků nebude v případě elektronické identifikace tím, kdo identifikaci provádí, fyzická osoba, ale spíše počítač nebo obdobný systém.⁶

Systém, na jehož základě jsou osobám vydávány prostředky pro elektronickou identifikaci, je označován jako systém elektronické identifikace. Ten má však více funkcí, neboť, jak shrnuje například UNCITRAL, je jím rozuměn:

„soubor pravidel, postupů a technologických řešení, jejichž základním smyslem je vytváření důvěryhodného prostředí pro vytváření a ověřování identit zúčastněných entit.“⁷

Systém elektronické identifikace tak zahrnuje i proces autentizace, který umožňuje elektronickou identifikaci potvrdit (ověřit).⁸ Přesto, že pro systémy elektronické identifikace neexistuje žádné standardizované řešení, lze shrnout, že na procesech elektronické identifikace a autentizace jsou závislé všechny.⁹

Míra důvěry v procesy elektronické identifikace a autentizace je vyjádřena takzvanými úrovněmi záruky. Ty označují míru důvěry v proces, který byl použit za účelem zjištění identity osoby, které byl

⁶ Srov. DE ANDRADE, Norberto Nuno Gomes et al. *Electronic identity*. New York: Springer, 2014, s. 4.

⁷ In: United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.120 – Overview of identity management – Background paper submitted by the Identity Management Legal Task Force of the American Bar Association* [online]. Vienna: United Nations, 2012. [cit. 30.10.2018]. s. 2-6.

⁸ Srov. článek 3 odstavec 5 EIDAS.

⁹ In: SULLIVAN, Clare. Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review* [online]. 2018, vol. 34, issue 4, s. 723-731 [cit. 2019-02-28]. s. 724.

vydán prostředek elektronické identifikace a míru důvěry, že osoba, která se prostředkem elektronické identifikace prokazuje, je osoba, které byl tento prostředek vydán.¹⁰ Úrovně záruky jsou v praxi označovány čísly nebo slovními označeními (úroveň záruky nízká, značná, vysoká¹¹), přičemž vyšší úroveň záruky by měla přinést i vyšší míru jistoty, že elektronická identita s daným prostředkem spojená nebyla upravena nebo pozměněna.¹²

2.2 Procesy v systémech elektronické identifikace

Účast osoby v systému elektronické identifikace může být shrnuta následovně.

Počátečním krokem je její identifikace v systému. Během tohoto procesu dojde ke sběru atributů o identifikované osobě (případně i jejich ověření) a vydání prostředku elektronické identifikace. Pokud chce následně osoba pomocí tohoto prostředku prokázat svou totožnost, dojde k ověření, že osoba, která tento prostředek předkládá (a tedy tvrdí, že je osobou, které byl tento prostředek vydán) je skutečně tato osoba.

V návaznosti na poskytnutých odpovědích a jejich důvěryhodnosti se spoléhající se druhá strana může rozhodnout zda, případně jak bude v jednání pokračovat – jaká oprávnění k jejím zdrojům osobě přidělí, zda s ní uzavře smlouvu a podobně. Tento proces se označuje jako

¹⁰ Srov. Telecommunication standardization sector of ITU. *Recommendation ITU-T X.1252 - Baseline identity management terms and definition* [online]. Geneva: International Telecommunication Union, 2010. [cit. 12.2.2019]. s. 3-4.

¹¹ Srov. například článek 8 EIDAS.

¹² Srov. DUMORTIER, Jos. Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation). SSRN Electronic Journal [online]. Elsevier, 2016 [cit. 11. 12. 2018] s. 8.

autorizace. Jakmile entita již není spojována se systémem elektronické identifikace, příslušný prostředek elektronické identifikace může být zrušen.

2.2.1 Identifikace a vydávání prostředků elektronické identifikace

První krok každé osoby v systému elektronické identifikace je její identifikace v tomto systému¹³ (osoba, která se takto identifikuje, je také označována jako uživatel, nebo subjekt elektronické identifikace). Identifikace je zpravidla jednorázový proces, účelem kterého je poskytnout odpověď na otázku „Kdo jsi?“¹⁴. V průběhu identifikace dochází ke shromažďování a případnému ověřování atributů určité osoby tak, aby ji bylo dostatečně možné v daném kontextu definovat, tedy vytvořit její elektronickou identitu.¹⁵

Shromažďování a ověřování atributů identifikované osoby může být prováděno zcela online, nebo může obsahovat některé offline prvky. K důvěryhodnému ověření údajů o identifikované entitě bývá většinou vyžadováno poskytnutí analogových dokladů¹⁶ (ať již vydaných vládou jako například občanský či řidičský průkaz nebo vydaných soukromými osobami – kreditní karta).¹⁷ Charakter a množství požadovaných

¹³ Proces identifikace někdy též bývá označován jako registrace a/nebo rozlišován jako dva samostatné procesy – zápis (anglicky: *enrolment*) a registrace.

¹⁴ Srov. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.120*. op. cit., s. 6.

¹⁵ Srov. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.150*. op. cit., s. 5.

¹⁶ Srov. SULLIVAN, 2018, op. cit., s. 725.

¹⁷ Například identifikace do systému mojeID provozovaného organizací CZ.NIC probíhá online, je však doplněna o ověření telefonního čísla zasláním textové

atributů nezbytných pro vytvoření identity v daném kontextu se liší podle požadavků a úrovně záruky daného systému.¹⁸

Zatímco pro některé transakce jsou úroveň záruky nebo požadované atributů upraveny právním předpisem (například EIDAS, procesy KYC¹⁹), pro většinu, zejména soukromoprávních jednání, tomu tak není. Absence pravidel pro identifikace tak často může vést k tomu, že bude vyraženo až příliš uživatelských atributů v porovnání se srovnatelným analogovým jednáním – například zatímco běžná hotovostní koupě v obchodě probíhá většinou anonymně, na internetu je taková transakce bez uvedení alespoň jména, emailové adresy a adresy bydliště často nemyslitelná.²⁰ Stejně tak pro zobrazení internetové stránky s obsahem přístupným od určitého věku není třeba poskytovat veškerá data o tomto uživateli, ale atribut věku nebo data narození bude dostačující.

Registrací entity dojde slovy Thomase Myhra k:

„propojení proudu dat s touto entitou,“²¹

zprávy s PIN kódem, ověřením korespondenční adresy zasláním dopisu na tvrzenou adresu a případně i ověřením totožnosti oproti občanskému průkazu. Viz MojeID: ZALOŽENÍ NOVÉHO ÚČTU. *MojeID* [online]. Praha: CZ.NIC, z. s. p. o. 2018 [cit. 2019-02-28].

¹⁸ Srov: SULLIVAN, 2018, op. cit. s. 727.

¹⁹ K tomu více např. ARNER, Douglas W. et al. The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. *European Banking Institute Working Paper Series 2018*. [online]. European Banking Institute, 2018, no. 28.

²⁰ Srov. DE ANDRADE, 2014, op. cit., s. 19.

²¹ In: MYHR, Thomas. Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution: or I am 621216-1318, but I am also 161262-

a relevantní atributy této osoby budou vyjádřeny daty na prostředku elektronické identifikace, který bude této osobě vydán. Prostředek elektronické identifikace může mít řadu podob, a to jak hmotných, tak nehmotných.²² Lze si ho představit například jako obyčejné uživatelské jméno, certifikát uložený na flash disku či telefonu, elektronický podpis nebo čipová karta.²³

Entita, která uživatele identifikuje, vydá mu prostředek elektronické identifikace a následně může jeho totožnost autentizovat, je označována jako identifikující strana, nebo poskytovatel identity.²⁴ Pokud takto prováděné elektronické identifikaci a autentizaci důvěřují jiné entity (v pozici takzvané spoléhající se strany²⁵), je tato entita označována též jako důvěryhodná třetí osoba.^{26,27}

43774.1 Do you know who I am?. *Information Security Technical Report* [online]. Elsevier, 2008, vol. 13 issue 2, s. 77.

²² Srov. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.144 – Work in the field of electronic commerce – legal issues relating to electronic identity management and trust services – Proposal by Austria, Belgium, France, Italy, the United Kingdom and European Union* [online]. New York: United Nations, 2017. Distributed 30.1.2017. [vid. 30.10.2018]. s. 7.

²³ Srov. OECD. 2009. op. cit. s. 7.

²⁴ Srov. United Nations Commission on International Trade Law, *A/CN.9/WG.IV/WP.120*. op. cit., s. 6.

²⁵ Srov. Článek 3 odstavec 6 EIDAS.

²⁶ Srov. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.150* s. 8.

²⁷ V systémech elektronické identifikace může jedna entita často zastávat několik rolí. Poskytovatel totožnosti bude často i spoléhající se stranou (například banka při výdeji platební karty a jejím přijetí v bankomatu).

2.2.2 Autentizace

Zatímco v případě identifikace jsme si pomohli otázkou „Kdo jsi?“, smyslem autentizace²⁸ je odpovědět na otázku „Jak to můžeš dokázat?“. Pokud si osoba přeje v analogovém prostředí vykonávat oprávnění této osobě udělené, při kterém je třeba ověření její totožnosti, zpravidla za tímto účelem předloží určitý doklad (například cestovní pas při vstupu do letadla, kartu do knihovny při výpůjčce) a tvrdí, že je osobou, které byl tento doklad vydán. Aby mohla osoba, které je doklad předložen, toto tvrzení ověřit, je třeba, aby bylo něčím podloženo.²⁹ Takovým podkladům se říká autentizátory a může jimi být cokoli, co prokazuje spojení mezi předkládaným dokladem a osobou, která ho předkládá.³⁰

Autentizátory můžeme dělit do tří skupin – jsou jimi znalosti, majetek a vlastnosti. Může jimi tedy být tedy něco, co osoba ví (heslo), vlastní (čipová karta) nebo čím je (biometrické údaje).³¹ Jedním z nejtypičtějších autentizátorů analogového světa pravděpodobně bude fotografie, která je porovnávána se vzhledem předkladatele dokladu.

Účelem procesu autentizace tedy je ověření, že osoba, která doklad předkládá, je osoba, které byl tento doklad dříve vydán. V případě elektronické identifikace je proces autentizace velmi podobný tomu analogovému. Osoba, která chce prokázat svou totožnost, se za tímto

²⁸ Jak uvádí například Sullivan, pro termín autentizace (anglicky: *authentication*) je mnohdy zaměnitelně používán termín ověření (anglicky: *verification*). In: SULLIVAN, 2018, op. cit. s. 742.

²⁹ Srov. OECD. 2007. op. cit. s. 7.

³⁰ Srov. United Nations Commission on International Trade Law. A/CN.9/WG.IV/WP.150 s. 4.

³¹ Srov. OECD. 2007. op. cit. s. 7.

účelem prokáže prostředkem elektronické identifikace a toto tvrzení podloží autentizátorem (nebo několika, jsou-li systémem vyžadovány).³²

V návaznosti na požadované úrovni záruky daného systému může entita, která autentizaci provádí, oproti stávajícím záznamům (získaným při identifikaci) ověřit, zda osoba skutečně je tím, komu byl prostředek elektronické identifikace vydán. V návaznosti na výsledcích tohoto procesu se rozhodne, zda a jak bude v transakci pokračovat.

2.2.3 Autorizace

Proces navazuje na proces elektronické identifikace a autentizace, je s ním propojen, ale svou podstatou již není jeho součástí.³³ V rámci tohoto procesu spoléhající se strana posuzuje, k jakým zdrojům a právům umožní konkrétnímu subjektu přístup.

Ověření totožnosti v rámci autentizace tedy nemusí být jediným cílem tohoto procesu. Spoléhající se strana se totiž může na základě procesu autentizace rozhodnout, zda a jaká oprávnění uživateli poskytne.³⁴ Může dojít k situaci, ve které spoléhající se strana na základě provedené autentizace zjistí, že některý z uživatelských atributů není uspokojivý pro přístup k jejím zdrojům a v jednání pokračovat nebude přesto, že totožnost byla úspěšně ověřena.

³² V praxi nejčastějším příkladem bude použití uživatelského jména jako prostředku elektronické identifikace a hesla jako autentizátoru, tedy něčeho, co uživatel ví.

³³ Někdy bývá označován spíše jako součást procesu řízení přístupů (anglicky: access management) Srov. OECD. 2011. op. cit., s. 17.

³⁴ Srov. United Nations Commission on International Trade Law. A/CN.9/WG.IV/WP.120. op. cit., s. 4.

2.2.4 Zrušení

Pomyslným posledním procesem, který se může vyskytnout v rámci systému elektronické identifikace je zrušení prostředku elektronické identifikace a vymazání údajů vedených o entitě.

2.3 Typy systémů elektronické identifikace

Přesto, že procesy uvedené v předchozí kapitole a pojmenování účastníci jsou vlastní téměř všem systémům elektronické identifikace, neexistuje v současné době žádné standardizované řešení (naopak existují spíše řešení izolovaná, navzájem nekompatibilní a částečná). Kromě systémů elektronické identifikace provozovaných státy navíc existuje v elektronickém prostředí řada systémů provozovaných soukromými subjekty, které mohou být použity pro zabezpečenou komunikaci i obchodní transakce, zcela bez státního přičinění, a často mohou mít v elektronickém prostředí i větší význam než ty provozované státem.³⁵ Přes tuto roztržitost můžeme rozeznávat čtyři základní, modelové typy systémů elektronické identifikace.

Historicky nejstarší skupinu řešení tvoří takzvané izolované (anglicky: *siloes*) systémy. Tyto systémy operují odděleně a nezávisle na ostatních systémech. Data a informace jejich uživatelů jsou uloženy pouze v těchto konkrétních systémech, což na jednu stranu znamená, že v případě jejich úniku půjde tyto hůře spojit s daty a informacemi v jiném systému,³⁶ na druhou stranu musí uživatel, který využívá více systémů,

³⁵ Srov. DE ANDRADE, op. cit., s. 20.

³⁶ Anebo naopak, případný útočník může zaútočit na jeden hůře zabezpečený systém a tam získané autentizátory použít pro přístup do jiných, více zabezpečených

absolvovat identifikační proces v každém z nich zvlášť a zpřístupňovat tak své atributy (mnohdy duplicitně) několika různým subjektům (poskytovatelům identit). V případě změny uživatelských atributů je pak třeba tyto oznámit všem izolovaným systémům, ve kterých je uživatel identifikovaný. Subjekty provozující izolované systémy v těchto případech jednají jako poskytovatelé identity i jako spoléhající se strany zároveň, neboť v rámci identifikace vydávají prostředky elektronické identifikace, na základě kterých posléze provádějí autentizaci³⁷ (a případně i autorizaci). Tyto systémy jsou vhodné například pro velké organizace, kterým umožňují omezit přístup ke svým interním službám pouze omezenému, kontrolovanému počtu uživatelů.

Další významnou skupinou jsou takzvané centralizované systémy. V těch jsou veškerá data a informace o uživateli shromažďována u jednoho nezávislého subjektu, který tyto dále poskytuje jednotlivým třetím osobám v pozici spoléhající se stranám. Osoba poskytovatele identity je tak ze své podstaty od spoléhajících se stran zásadně odlišná. Tento systém je uživatelsky přívětivý, identifikace a autentizace probíhá pouze v jednom systému, stejně jako provedení změny zapsaných údajů. Případný bezpečnostní únik na straně poskytovatele identity však znamená ohrožení veškerých uživatelských dat.³⁸

Právě této bezpečnostní hrozbě mají zabránit takzvané federované systémy. Zatímco data a informace o uživateli jsou v těchto systémech

systémů, do kterých uživatel používá stejná hesla. Srov. LAURENT, Maryline; BOUZEFRANE, Samia. *Digital Identity Management*. 1 ed. London: ISTE Press Ltd, 2015. s. 34.

³⁷ Srov. United Nations Commission on International Trade Law, A/CN.9/WG.IV/WP.120. op. cit. s. 4.

³⁸ Srov. LAURENT; BOUZEFRANE. op. cit. s. 35.

uloženy u jednotlivých poskytovatelů služeb, jeden centrální *poskytovatel identifikátorů* sleduje veškerá propojení mezi jednotlivými daty a příslušnými uživateli. Uživatel se poté autentizuje u jednoho poskytovatele identifikátorů, přičemž tato autentizace je dostačující pro celou federaci.³⁹ Poskytovatel identifikátorů může díky znalosti těchto propojení jednoho uživatele zprostředkovávat sdílení informací mezi jednotlivými službami, čímž se fakticky stává důvěryhodnou třetí osobou.

Konečně poslední skupinu tvoří takzvané uživatelsky orientované systémy, které jsou navrženy za účelem poskytnutí větší kontroly uživatelům nad zpřístupňováním jejich údajů. Uživatelé v těchto systémech neposkytují žádné své údaje poskytovatelům služeb přímo, namísto toho si mohou vybrat poskytovatele identity od poskytovatele služeb odlišného. Poskytovatelé identity uchovávají data a informace uživatelů a též provádí proces autentizace (jako důvěryhodné třetí osoby), zatímco poskytovatelé služeb výsledek tohoto procesu přijímají (jako spoléhající se osoby) a pokračují v samotné autorizaci. Na rozdíl od federovaných systémů nejsou poskytovatelé totožnosti součástí federace, v rámci které autentizace probíhá.⁴⁰ Uživatel může využívat několik vzájemně oddělených poskytovatelů elektronické identifikace, aby nebyly veškeré jeho osobní údaje uloženy na jednom místě a (byť spoléhající se strana může některé údaje přímo vyžadovat) též záleží na něm, které osobní údaje spoléhající se straně zpřístupní.⁴¹

³⁹ Srov. OECD, 2011, op. cit., s. 161.

⁴⁰ Srov. Ibid.

⁴¹ OECD, 2011, op. cit., s. 162.

3 Přehled současných právních řešení

V této kapitole se budu věnovat současným právním řešením elektronické identifikace. Výklad přitom zaměřím na nařízení EIDAS,⁴² které se oblasti elektronické identifikace z velké části věnuje. Následně se v budu zabývat výhradně českou úpravou elektronické identifikace v České republice. Přesto, že přeshraničním aspektům elektronické identifikace se budou věnovat až následující kapitoly, nelze se tomuto tématu, vzhledem k charakteru a účelu úpravy EIDAS, vyhnout úplně.

3.1 Evropská unie – nařízení EIDAS

EIDAS, nařízení přímo použitelné od 1. července 2016, přináší právní rámec pro systémy elektronické identifikace a služby vytvářející důvěru na úrovni Evropské unie. Za cíl si klade

„vytvoření systému pro bezpečnou elektronickou komunikaci v Evropské unii, prohloubení důvěry v elektronické transakce a zvýšení efektivnosti veřejných a soukromých online služeb a elektronického obchodu.“⁴³

EIDAS ke dni své účinnosti ruší takzvanou eSignature směrnici⁴⁴, jejíž oblast úpravy převzal, nově však upravuje nejen elektronické

⁴² Celým názvem Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

⁴³ In: Bezpečnější transakce na internetu. *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 11. 12. 2018].

⁴⁴ Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

podpisy, ale i spektrum dalších služeb vytvářejících důvěru (jako například elektronická časová razítka), čímž dochází k rozšíření *acquis communautaire*.⁴⁵

Záměrem eSignature směrnice bylo oslovit trh elektronických identit v jeho počátcích a nabídnout právní základ pro elektronické podpisy a kvalifikované certifikáty, nicméně přesto, že online trh exponenciálně rostl, implementace eSignature směrnice k tomu podle některých názorů nikterak nepřispěla, když sice probíhala, ovšem většinou se zaměřovala pouze na oblast eGovernmentu.⁴⁶

Směrnice taktéž vůbec neřešila otázku elektronické identifikace. Zatímco pomocí elektronického podpisu mohou podepisující osoby uvést, že jsou autory daného dokumentu, a že s určitým dokumentem nebylo manipulováno, eSignature směrnice neumožňovala odpovědět na základní otázky elektronické identifikace v širším slova smyslu.⁴⁷ Směrnice totiž ve svém důsledku nanejvýše stanovila, že takzvané zaručené elektronické podpisy založené na kvalifikovaných certifikátech jsou ekvivalentem vlastnoručních podpisů a ostatním elektronickým podpisům nesmí být odepírány jejich právní účinky.⁴⁸ Jinými slovy, eSignature směrnice neobsahovala žádná ustanovení, která by měla jakýkoli význam z hlediska autentizace. Postavení na roveň vlastnoručnímu podpisu nemá samo o sobě ve vztahu k autentizaci

⁴⁵ Za absenci úpravy ostatních služeb vytvářejících důvěru byla eSignature směrnice též kritizována. Srov. CUIJPERS, Colette; SCHROERS, Jessica. eIDAS as guideline for the development of a pan European eID framework in FutureID. In: HÜNHLEIN, D. (eds.). *GI-Edition Lecture Notes in Informatics* [online]. 2014, [cit. 11. 12. 2018] s. 6.

⁴⁶ Srov. DE ANDRADE. op. cit. s. 13-15.

⁴⁷ Tedy „Kdo jsi?“ a „Jak to můžeš dokázat?“.

⁴⁸ Článek 5 eSignature směrnice.

žádnou relevanci, když vlastnoruční podpis nelze bez dalšího kontextu považovat za dostatečný k prokázání totožnosti.⁴⁹

Některé členské státy již před použitelností EIDAS svým občanům národní řešení elektronické identifikace umožňovaly. Ta byla většinou založena na kombinaci analogových dokladů, jejich ochranných prvků a různých technických prostředků.^{50,51} Tato národní řešení mezi sebou ovšem nekomunikovala a byla navzájem neslučitelná, což bylo dáno především jejich odděleným vývojem, řízeným příslušnými národními předpisy.⁵²

Konkrétním problémem, který tímto postupem vznikl a který má EIDAS v oblasti elektronické identifikace odstranit, je nemožnost využití již existujících prostředků elektronické identifikace pro přístup ke službám poskytovaným jinými členskými státy než těmi, kterými byly tyto prostředky vydány.⁵³ To je problematické zejména pro ty online služby, pro jejichž užití je vyžadována vyšší úroveň zabezpečení a důvěryhodnost identifikace, jako je případ přeshraničního poskytování

⁴⁹ Srov. GRAUX, Hans; MAJAVA, Jarkko; MEYVIS, Eric. *Study on eID Interoperability for PEGS: Update of Country Profiles. Analysis & assessment report* [online]. European Communities: 2009, 228 [cit. 11. 12. 2018]. s. 108.

⁵⁰ Srov. DONÁT, Josef; MAISNER, Martin; PIFFL, Robert. *Nařízení eIDAS. Komentář*. 1. vyd. Praha: Nakladatelství C.H. Beck, 2017, Beckovy komentáře. s. 20.

⁵¹ Běžnou praxí je například opatření občanského průkazu elektronickým čipem, který ve spojení s patřičným technickým zařízením umožní autentizaci pro přístup k některé online službě.

⁵² Srov. SHEHU, Abubakar-sadiq; PINTO, António; CORREIA, Manuel E. On the Interoperability of European National Identity Cards. In: *Novaes P. et al. Ambient Intelligence – Software and Applications – 9th International Symposium on Ambient Intelligence. Advances in Intelligent Systems and Computing*. Springer, Cham. 2018, vol. 806. [cit. 2019-2-28] s. 343-344.

⁵³ Srov. Recitál 13 EIDAS.

zdravotní péče nebo online zadávání veřejných zakázek. Konečně vyžadování použití národních prostředků a neuznávání prostředků z jiných členských států je podle některých názorů též v rozporu s principem volného pohybu osob.⁵⁴

Snahou EIDAS není zavedení jednotného systému elektronické identifikace ve veřejné sféře pro celou Evropskou unii. Vydávání takzvaných prostředků primární identifikace (například občanských průkazů) je suverénní výsadou členských států, kterou EIDAS plně respektuje. S účinností EIDAS zřizování systémů elektronické identifikace pro přístup ke službám veřejného sektoru zůstává v gesci jednotlivých členských států v souladu s jejich dosavadní tradicí⁵⁵ a EIDAS se zaměřuje pouze na přeshraniční aspekty elektronické identifikace.

EIDAS doprovází řada prováděcích aktů, které byly přijaty na základě jeho zmocňovacích ustanovení. Z těchto prováděcích aktů je pro oblast elektronické identifikace relevantní následující čtveřice:

- Prováděcí rozhodnutí Komise (EU) 2015/296, které stanovuje procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace, například proces peer – review;
- Prováděcí nařízení Komise (EU) 2015/1501, které stanovuje technický a provozní rámec pro zajištění interoperability oznámených systému elektronické identifikace;

⁵⁴ Srov. POPE, Nick; ALIN, Jonathan. *The Impact of the European eIDAS Regulation* [online]. Thales e-Security [cit. 12.2.2019]. s. 8.

⁵⁵ Srov. DONÁT, Josef; MAISNER, Martin; PIFFL, Robert. op. cit. s 20.

- Prováděcí nařízení Komise (EU) 2015/1502, které stanovuje minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci; a
- Prováděcí rozhodnutí Komise (EU) 2015/1984, které stanovuje okolnosti postupu oznamování systémů elektronické identifikace Komisi.

3.1.1 Elektronická identifikace podle EIDAS

EIDAS nezakládá povinnost členským státům systémy elektronické identifikace vytvářet a ohlašovat Komisi, ale ukládá jim povinnost uznat prostředky elektronické identifikace vydané v rámci řádně oznámených systémů elektronické identifikace ostatních členských států pro přístup ke svým službám veřejné správy. Smyslem uznávání v rámci EIDAS není uznání prostředku jako takového, ale elektronické identity na něm obsažené. EIDAS se tedy vztahuje pouze na oznámené systémy elektronické identifikace⁵⁶ a nadále může existovat řada v praxi používaných systémů, které nebudou EIDAS regulované a nebudou jim tedy ani přiznány přeshraniční účinky dle EIDAS.

Elektronicky identifikovat lze podle EIDAS fyzické a právnické osoby a fyzické osoby zastupující osoby právnické.⁵⁷ Ty lze identifikovat používáním jejich *osobních identifikačních údajů* v elektronické podobě, kterými EIDAS rozumí *soubor údajů umožňující určit totožnost osoby*.^{58,59}

⁵⁶ Článek 2 písmeno a) EIDAS.

⁵⁷ Článek 3 odstavec 1 EIDAS.

⁵⁸ Článek 3 odstavec 3 EIDAS.

⁵⁹ Minimálním souborem údajů, podle kterých lze podle EIDAS určit totožnost, je v souladu s prováděcím nařízením Komise (EU) 2015/1501 v případě fyzické osoby: její (i) současné příjmení, (ii) současné jméno, (iii) datum narození, a (iv) jedinečný, pokud možno následně neměnný identifikátor.

3.1.2 Úrovně záruky

Jedním z problémů vzájemného uznávání je různá úroveň zabezpečení systémů elektronické identifikace v jednotlivých státech, tedy jejich úroveň záruky. EIDAS pro prostředky elektronické identifikace vydané v rámci oznámeného systému elektronické identifikace rozlišuje úrovně záruky tři, a to úroveň nízkou, značnou a vysokou.⁶⁰ Protože jednotný standard pro úrovně záruky neexistuje, byly za účelem zajištění shody a mapování stávajících systémů stanoveny minimální technické specifikace a postupy pro jednotlivé úrovně záruky prováděcím nařízením.⁶¹

Samotná úroveň záruky prostředků pro elektronickou identifikaci je vyhodnocována na základě naplnění podmínek rozdělených do čtyř kategorií, kterými jsou (i) přihlášení, (ii) správa prostředků pro elektronickou identifikaci, (iii) autentizace a (iv) řízení a organizace. Úrovně záruky prostředků pro elektronickou identifikaci oznamuje členský stát Komisi spolu s popisem oznamovaného systému.⁶²

3.1.3 Odpovědnost za škodu

Odpovědnost za škodu upravuje EIDAS odděleně pro elektronickou identifikaci a služby vytvářející důvěru. V případě služeb vytvářejících důvěru je dána odpovědnost za škodu způsobenou neplněním

⁶⁰ Článek 8 EIDAS.

⁶¹ Nařízení (EU) 2015/1502, které konceptuálně vychází a přejímá definice z pilotního projektu STORK a z mezinárodního standardu ISO/IEC 29115 tj. základní normy dostupné v oblasti úrovně záruky prostředků pro elektronickou identifikaci.

⁶² Článek 9 odstavec 1 písmeno a) EIDAS.

povinností podle EIDAS jak kvalifikovaným tak nekvalifikovaným poskytovatelům služeb vytvářejících důvěru.⁶³

V případě elektronické identifikace se však odpovědnost týká vyjma strany vydávající prostředky pro elektronickou identifikaci a strany provozující postup autentizace i přímo oznamujícího státu.⁶⁴ Odpovědnost je dána za škodu způsobenou nesplněním povinností podle EIDAS subjektivní i objektivní, a to za škodu způsobenou fyzickým i právnickým osobám, nicméně pouze v přeshraničních transakcích. Oznamující stát pak odpovídá v případě, že nezajistí dostupnost online autentizace nebo nezajistí, že osobní identifikační údaje budou jedinečně identifikovat danou osobu.

EIDAS tedy na jednu stranu podporuje zapojení soukromého sektoru, když se v odstavci 13 recitálu vyjadřuje, že:

„členské státy by měly mít možnost používat nebo zavést prostředky pro účely elektronické identifikace pro přístup k online službám. Měly by mít rovněž možnost rozhodnout, zda do poskytování těchto prostředků zapojí soukromý sektor,“⁶⁵

zároveň by však tento přístup k odpovědnosti mohl členské státy od oznámení některých systémů odrazovat. Oznámení systémů elektronické identifikace je čistě v gesci členských států, ke zmírnění jejich rizik spojených s oznámením se nabízí také možnost zavést kroky v podobě pravidelných auditů, fondů, nebo, jak navrhuji někteří autoři, veřejných dražeb, jako je tomu běžné v případě telekomunikačních

⁶³ Článek 13 EIDAS.

⁶⁴ Článek 11 EIDAS.

⁶⁵ Recitál 13 EIDAS.

operátorů.⁶⁶ Na druhou stranu, přímá odpovědnost státu by mohla v případě hrozícího ohrožení systémů nacházejících se na území některého státu vynutit jeho rychlou reakci k řešení takového problému.

EIDAS nicméně v plném rozsahu odkazuje na vnitrostátní pravidla upravující odpovědnost za škodu, včetně otázek vymezení škod nebo důkazního břemene.⁶⁷ V českém právním prostředí tak bude stát v pozici oznamovatele systému elektronické identifikace pravděpodobně odpovídat podle ustanovení § 2910 občanského zákoníku za porušení mimosmluvní povinnosti, přičemž právním základem odpovědnosti za škodu je EIDAS, který je jako předpis vyšší právní síly občanskému zákoníku nadřazen. Závazný výklad může ovšem přinést až následná rozhodovací praxe soudů.

3.2 Právní úprava na území České republiky

Do 1. července 2018 v České republice nebyl právně upraven institut elektronické identifikace a způsoby prokázání totožnosti na dálku byly upraveny partikulárně pro konkrétní účely. Změnu přinesl zákon č. 250/2017 Sb., o elektronické identifikaci (**ZOEI**), který je adaptačním zákonem k nařízení EIDAS (respektive k jeho části elektronické identifikace⁶⁸) a který je účinný ke dni jeho přímé použitelnosti. ZOEI je obecným předpisem, který stanovuje obecný právní rámec pro prokazování totožnosti prostřednictvím elektronické identifikace –

⁶⁶ Srov: DONÁT, Josef; MAISNER, Martin; PIFFL, Robert. op. cit. s. 49.

⁶⁷ Článek 11 odstavec 4 EIDAS ve spojení s recitálem 18 EIDAS.

⁶⁸ Adaptační část věnující se službám vytvářejícím důvěru, která byla použitelná dříve, byla provedena zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

nevyklučuje tak, aby jiné zákony zvolily odlišnou úpravu pro konkrétní služby veřejného sektoru, například aby ověření totožnosti prostřednictvím elektronické identifikace vyloučily.⁶⁹ Měl by přinést sjednocení způsobů ověřování totožnosti pro přístup k online službám poskytovaným jednotlivými orgány veřejné správy. Také by měl umožnit, aby uživatelé veřejných služeb při komunikaci s jejich poskytovateli využívali své prostředky elektronické identifikace, které byly vydány subjekty soukromého práva.

3.2.1 Zákon o elektronické identifikaci

Klíčovým ustanovením ZoEI je jeho § 2, stanovující obecné pravidlo pro prokázání totožnosti pomocí elektronické identifikace:

„Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace (dále jen „kvalifikovaný systém“).“⁷⁰

Hypotézou tohoto ustanovení je požadavek prokázání totožnosti, a to buď obsažený v právním předpise nebo vyžadovaný okolnostmi uplatňování veřejné moci. Přesto, že k naplnění této hypotézy bude docházet primárně ve veřejnoprávních vztazích, budou tomuto režimu podřízeny i některé soukromoprávní subjekty, a to v případě, že ověření totožnosti bude stanoveno jako povinnost (například AML zákon stanovuje povinnost „identifikace klienta“ celé škále soukromoprávních

⁶⁹ Srov. Důvodová zpráva k zákonu č. 250/2017 Sb. o elektronické identifikaci, č. 250/2017. Dz. In: ASPI [právní informační systém]. Wolters Kluwer ČR. s. 8.

⁷⁰ § 2 ZO EI.

osob⁷¹). Druhou částí hypotézy je umožnění ověření totožnosti s využitím elektronické identifikace. ZOEl takovou povinnost nijak neukládá, tato možnost musí být dána ze strany entity oprávněné k ověření totožnosti. Pokud není zákonem stanoveno jinak, je na rozhodnutí daného subjektu, zda ověření totožnosti s využitím elektronické identifikace umožní. Pokud dojde k naplnění hypotézy, je dána povinnost v takovém případě prokázání totožnosti s využitím elektronické identifikace využívat pouze takzvaný kvalifikovaný systém elektronické identifikace. ZOEl stanovuje dvouleté přechodné období (do července 2020), během kterého nemusí být prokázání totožnosti s využitím elektronické identifikace použito kvalifikovaného systému,⁷² což poskytuje domovským poskytovatelům prostor pro uvedení svých dosavadních systémů do souladu s novými požadavky tohoto zákona.

Vzhledem k přímé použitelnosti EIDAS neobsahuje ZOEl definice v EIDAS již obsažené (tedy včetně samotného pojmu elektronické identifikace), zavádí však některé nové pojmy a instituty, kterým se budou věnovat následující podkapitoly.

3.2.2 Kvalifikovaný poskytovatel

Podle ZOEl lze totožnost pomocí elektronické identifikace prokázat v rámci online služby nebo jiné činnosti.⁷³ Osoba, která prokázání totožnosti ve vztahu k těmto aktivitám umožňuje, je zákonem označována jako *kvalifikovaný poskytovatel*, a je tak v postavení spoléhající se strany.

⁷¹ Srov. zejm. § 2 a § 7 AML zákona.

⁷² § 27 odstavec 2 ZOEl.

⁷³ § 18 ZOEl.

Kvalifikovaný poskytovatel má povinnost vyrozumět správce národního bodu (viz níže) o skutečnosti, že je kvalifikovaným poskytovatelem, společně s uvedením služeb, při kterých prokázání totožnosti s využitím elektronické identifikace umožňuje, a o požadované úrovni záruky prostředku pro elektronickou identifikaci. Které entity se mohou stát kvalifikovaným poskytovatelem, zákon nevymezuje – vyjma fyzických a právnických osob to tedy mohou být i jiná právní uspořádání, například organizační složky státu.⁷⁴

3.2.3 Kvalifikovaný systém

Aby mohl být systém elektronické identifikace označen jako kvalifikovaný, musí naplnit podmínky stanovené v § 3 ZOEL. V první řadě musí tento systém spravovat takzvaný kvalifikovaný správce systému elektronické identifikace. Systém musí dále naplňovat požadavky alespoň pro jednu z úrovní záruk stanovených přímo použitelným předpisem upravujícím požadavky pro úrovně záruky prostředků pro elektronickou identifikaci.⁷⁵ Dalším požadavkem je, aby systém umožňoval poskytnutí služby národního bodu, tedy musí být s národním bodem kompatibilní. Konečně zákon požaduje, aby v rámci kvalifikovaného systému byly v souladu s požadavky pro příslušnou úroveň záruky stanovenými příslušným předpisem EU⁷⁶ (i) osobní identifikační údaje jedinečně identifikující osobu v okamžiku vydání

⁷⁴ Na seznamu kvalifikovaných poskytovatelů zveřejňovaném Správou základních registrů se vyskytuje například Město Pelhřimov, Generální finanční ředitelství nebo Státní ústav pro kontrolu léčiv.

⁷⁵ Tedy prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015.

⁷⁶ Tyto požadavky jsou přejímány z článku 7 písmen d) a e) eIDAS. Příslušným předpisem je opět prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015.

prostředku pro elektronickou identifikaci spojeny s danou osobou a (ii) vydávány a používány pouze prostředky pro elektronickou identifikaci, které jsou spojeny s osobou, kterou identifikují.⁷⁷

Za kvalifikovaný systém jsou považovány ty systémy elektronické identifikace oznámené podle EIDAS, v rámci kterých je vydáván prostředek elektronické identifikace s úrovní záruky alespoň značnou.⁷⁸

3.2.4 Kvalifikovaný správce

Každý kvalifikovaný systém musí spravovat kvalifikovaný správce. Tím může být státní orgán, nebo, v případě nestátních subjektů⁷⁹, osoba, které byla udělena akreditace pro správu kvalifikovaného systému.⁸⁰ Státním kvalifikovaným správcem je například ministerstvo vnitra, které se v souladu s § 4 odst. 8 zákona o občanských průkazech považuje za vydavatele občanského průkazu se strojově čitelnými údaji a s kontaktním elektronickým čipem. Seznam kvalifikovaných správců (spolu s jimi vydanými prostředky pro elektronickou identifikaci) vede Správa základních registrů.

Nestátním kvalifikovaným správcům uděluje akreditaci ministerstvo vnitra, a to na základě písemné žádosti ve smyslu správního řádu. Žadatel o akreditaci musí splnit a v rámci žádosti doložit splnění řady podmínek. Předně musí jím spravovaný systém elektronické identifikace a vydávaný prostředek pro elektronickou identifikaci splňovat požadavky na jednu z úrovní záruk dle EIDAS. Žadatel dále musí

⁷⁷ § 3 odstavec 1 písmena d) a e) ZOEl.

⁷⁸ § 3 odstavec 2 ZOEl.

⁷⁹ Nestátní kvalifikovaný správce je při zachování vlivu oznamujícího státu předvídan i ve článku 7 písmene a) EIDAS.

⁸⁰ §4 ZOEl.

být bezúhonný a mít uzavřené pojištění odpovědnosti za škody, které případně způsobí při správě kvalifikovaného systému⁸¹ a musí mít zpracovaný plán ukončení činnosti. Systém žadatele musí umožnit poskytnutí služeb národního bodu⁸² a konečně žadatel o akreditaci musí být pro správu systému způsobilý z hlediska veřejného pořádku, bezpečnosti a práv třetích osob.

O žádosti je ministerstvo vnitra povinno rozhodnout do tří měsíců (tedy odchylně od správního řádu, což důvodová zpráva zdůvodňuje náročností a odborností takového posouzení). Z konstrukce zákona vyplývá, že udělení akreditace by mělo být nárokové (*„Splňuje-li žadatel o akreditaci podmínky pro udělení akreditace, ministerstvo akreditaci udělí“*⁸³). Možnou komplikaci zde spatřuji v pravomoci ministerstva vyžádat si informace od Policie České republiky nebo zpravodajské služby za účelem zjištění způsobilosti z hlediska bezpečnosti a veřejného pořádku. Žadatel (respektive fyzická osoba zajišťující činnost kvalifikovaného správce) by tak podle mého názoru měl být analogicky bezpečnostně způsobilý podle zákona o ochraně utajovaných informací, tedy splňovat podmínky pro vydání dokladu o bezpečnostní způsobilosti.⁸⁴ Domnívám se, že například požadavek na spolehlivost do procesu akreditace vnáší vyšší stupeň správního uvážení a snižuje tak jeho předvídatelnost. Přestože tento požadavek je, s ohledem na možné důsledky nedůvěryhodných správců, pochopitelný, mohly by v praxi

⁸¹ Jehož minimální výše není stanovena a v současné době je ponechána na uvážení každého žadatele.

⁸² Povinnost poskytnutí služeb národního bodu je dána i povinností kvalifikovaného správce ověřit totožnost držitele prostřednictvím národního bodu ve smyslu § 16 odstavce 1 písmena c) ZoIE.

⁸³ § 5 odstavec 6 ZOIE.

⁸⁴ § 80 a následující zákona č. 412/2005 Sb.

nastávat situace, kdy akreditace udělena nebude, a vzhledem k možnému utajení postupů zpravodajských služeb nebude mít žadatel možnost dozvědět se o charakteru své nezpůsobilosti, respektive jak ji napravit.

Státní i nestátní kvalifikovaní správci musí dále dodržovat povinnosti, které jim ukládá ZOEL. Musí tak například zajišťovat dostupnost jimi spravovaných kvalifikovaných systémů nebo vést evidenci jimi vydaných prostředků pro elektronickou identifikaci. Oba typy správců jsou povinni dále zpracovat a pravidelně aktualizovat plán ukončení činnosti. Součástí tohoto plánu je i plánovaný postup pro informování správce národního bodu a držitelů prostředků pro elektronickou identifikaci o ukončení činnosti kvalifikovaného správce. V případě ukončení činnosti musí kvalifikovaní správci též předat evidenci vydaných prostředků pro elektronickou identifikaci ministerstvu vnitra a jimi vydané prostředky pro elektronickou identifikaci zneplatnit.⁸⁵ ZOEL však neobsahuje žádný speciální postup pro provádění kontroly nad kvalifikovanými správci, vyjma uložení obecné kontrolní funkce, kterou provádí ministerstvo vnitra podle kontrolního řádu⁸⁶ a proces odejmutí akreditace, avšak pouze na základě výzvy.⁸⁷

Další pravidla, která se uplatní během případného narušení bezpečnosti systému elektronické identifikace upravuje, jako přímo použitelný předpis, EIDAS. Ten předpokládá zavedení opatření k pozastavení platnosti nebo zrušení již oznámených systémů

⁸⁵ § 16 ZOEL.

⁸⁶ § 19 odstavec 1 písmeno c) ZOEL.

⁸⁷ V souladu s § 7 ZOEL.

elektronické identifikace, případně jejich vyškrtnutí ze seznamu elektronické identifikace⁸⁸ a též stanovuje povinnost pozastavit přeshraniční autentizaci v případě narušení bezpečnosti oznámeného systému elektronické identifikace.⁸⁹ Tyto pravidla se však uplatní pouze na oznámené systémy elektronické identifikace.

3.2.5 Národní identitní autorita

Národní identitní autorita (**NIA**) je národní bod pro identifikaci a autentizaci ve smyslu § 20 ZOEI, informační systém veřejné správy ve smyslu zákona o informačních systémech veřejné správy,⁹⁰ a tvoří klíčový prvek v procesu elektronické identifikace. Národní bod zprostředkovává komunikaci mezi uživateli, kvalifikovanými poskytovateli a kvalifikovanými správci navzájem a mezi těmito účastníky a základními registry.

Národní bod je též provozovatelem uzlu EIDAS, který umožňuje propojení vnitrostátních infrastruktur jednotlivých členských států. Národní bod vytváří národní část uzlu EIDAS a udržuje vazbu mezi záznamy v Registru obyvatel a záznamy u kvalifikovaných systémů elektronické identifikace.

3.2.6 Současný stav

Přihlášení do NIA je v současné době umožněno prostřednictvím elektronického občanského průkazu a prostřednictvím identifikačního prostředku „Jméno, heslo a SMS“ provozovaného Správou základních

⁸⁸ Článek 9 EIDAS.

⁸⁹ Článek 10 EIDAS.

⁹⁰ § 2 zákona č. 365/2000 Sb.

registru,⁹¹ tedy prostřednictvím prostředků vydávaných kvalifikovaný systémy provozovanými státními kvalifikovanými správci. NIA v současné době podporuje též přihlášení prostřednictvím německého notifikovaného systému. Podle dostupných zdrojů v současné době požádal o udělení akreditace pouze jeden subjekt.⁹²

Možný průlom v této oblasti slibuje takzvaný projekt SONIA, tedy plán České bankovní asociace, cílem kterého je vytvoření systému BankID, které by existovalo vedle NIA. Elektronickou identitu by v tomto případě vytvářely jednotlivé licencované banky působící v České republice, které by držely veškerá data a informace jednotlivých uživatelů – BankID by v takovém případě, stejně jako NIA, bylo pouhým zprostředkovatelem.⁹³

Výhodou takového systému může být relativně jednoduchá zátěž pro uživatele, kteří by si nemuseli vytvářet další prostředek pro přihlášení k online službám a mohli by využít stávajících údajů, které používají například pro přístup k internetovému bankovníctví. Stát naopak získá až miliony nových uživatelů eGovernmentu, a to bez jakýchkoli nákladů (výjimkou může být dohled, který by mohla jako orgán dohledu nad bankami vykonávat ČNB). Požadavky na solventnost bank by navíc mohly poskytovat důvěru, že příslušná banka bude mít

⁹¹ Úroveň záruky tohoto systému je střední. Pokud nemá registrovaná osoba zřízenou datovou schránku nebo nevlastní občanský průkaz s čimep, je pro dokončení registrace návštěva CzechPointu. Jako druhý faktor autentizace se používá kód doručený prostřednictvím SMS.

⁹² KUCHAR, Petr; Elektronická identifikace v ČR, NIA, eOP. In: konference eIDENTITA 2019 [online]. Praha: Ministerstvo vnitra České republiky, 2019 [cit. 2019-5-28] pp. 6.

⁹³ ŠTĚPÁNEK, Pavel; DONÁT, Josef. *Projekt SONIA: příspěvek bank k rozvoji digitálního Česka. Konference ISSS Hradec Králové* [online]. Hradec Králové: Česká bankovní asociace, 2019 [cit. 2019-5-28] pp. 18

v případě bezpečnostního úniku dostatečný kapitál na náhradu způsobených škod.

Tomuto plánu však v současné době stojí v cestě několik především legislativních překážek. Současná bankovní licence neumožňuje bankám vytvářet elektronickou identitu a značně omezuje nakládání s osobními údaji. V této souvislosti je vhodné též uvést, že AML zákon neumožňuje identifikaci pomocí elektronické identifikace(!). Povinná osoba podle AML zákona může klienta identifikovat toliko u kvalifikovaného poskytovatele služeb vytvářejících důvěru.⁹⁴ Formálně tedy podle AML zákona nelze prokazovat totožnost ani za pomocí elektronického občanského průkazu s čipem.

S dalším vývojem projektu nicméně již počítá i vládní koncepce „Digitální Česko.“⁹⁵ Projekt SONIA má totiž jednu výhodu v tom, že systém elektronické identifikace provozovaný bankami není žádnou novinkou. Již v roce 2003 byl ve Švédsku vydán první prostředek elektronické identifikace v systému BankID, který v současné době využívá již 8 milionů uživatelů.⁹⁶

⁹⁴ § 11 odstavec 8 zákona o AML.

⁹⁵ digitální;ČESKO. Vládní program digitalizace České republiky 2018+. Shrnutí implementačních plánů pro 2019. In: *Digitální Česko* [online] Praha: Úřad vlády České republiky, 2019 [cit. 2019-5-28] s. 5.

⁹⁶ This is BankID. *BankID* [online]. Finansiell ID-Teknik BID AB, 2019 [cit. 2019-5-28].

4 Přeshraniční spolupráce v oblasti elektronické identifikace

V této kapitole věnované samotné přeshraniční spoluprací v oblasti elektronické identifikace se zaměřím na samotný problém přeshraničního uznávání elektronických identit. Nejprve provedu obecnou analýzu problému přeshraničního uznávání a následně se budu věnovat způsobu, jakým se tento problém snaží vyřešit EIDAS.

4.1 Analýza problému přeshraničního uznávání v oblasti elektronické identifikace

Téměř agnostický vztah internetu k identitě jeho uživatelů⁹⁷ trefně shrnují například autoři Bílé knihy výzkumu PRIME (Privacy and Identity Management for Europe):⁹⁸

„Internet účelově postrádá jednotné nástroje pro identifikaci toho, kdo komunikuje s kým; postrádá dobře navrženou identifikační infrastrukturu.“⁹⁹

Anonymita internetu je v západní společnosti stěží považována za problém, naopak je mnohými chápána jako prostředek pro vyjádření názorů a přesvědčení bez obav z možného stíhání či jiných následků.

⁹⁷ K tomu více např.: KYNCL, Libor. IP adresa identifikuje místo připojení, nikoli osobu. *Revue pro právo a technologie*. [Online]. 2011, č. 3, s. s. 5-6. [cit. 2019-02-28].

⁹⁸ Anebo jak proslule, byť poněkud stručněji a s nadsázkou ilustroval americký New Yorker již v roce 1993: „Na internetu nikdo neví, že jsi pes.“

⁹⁹ LEENES, Ronald; SCHALLABÖCK, Jan; HANSEN, Marit. *PRIME White paper v2* [online]. PRIME, 2007. Published 27.6.2007. [vid. 12.2.2019]. s. 1.

Problém však může nastat, když je člověk ve virtuálním prostředí, slovy Františka Kasla:

*„zdánlivě zbaven některých společenských či morálních mantinelů,
a je mu umožněno realizovat temnější stránky své osobnosti bez
zjevného následku či trestu.“¹⁰⁰*

Zatímco doba úplné anonymity internetu pominula,¹⁰¹ častěji se vyskytují situace, které stejně jako v analogovém světě vyžadují ověření totožnosti. Za tímto účelem, jak pokračují autoři Bílé knihy výzkumu PRIME:

*„(...) si organizace, vlády a jednotlivci postupně vyvinuli změť
izolovaných, navzájem nekompatibilních a částečných řešení pro
potřeby jejich komunikace a transakcí. Konečný výsledek tohoto
neřízeného vývoje je ten, že organizace a vlády mají problém
identifikovat své partnery na jiných úrovních.“¹⁰²*

Výzkum provedený Cybersecurity Ventures předpokládá, že v roce 2020 bude průměrný uživatel pro přístup k online službám využívat 25 různých hesel, což znamená 25 různých poskytovatelů totožnosti.¹⁰³

¹⁰⁰ POLČÁK, R. a kol. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer ČR, 2018, s. 393.

¹⁰¹ Digitální identita se nevytváří pouze dobrovolně a vědomě, prostřednictvím identifikace u jednotlivých poskytovatelů služeb či sdílením informací na sociálních sítích, ale též nevědomě a neúmyslně, díky takzvané pasivní digitální stopě, tedy souboru informací, který vzniká při interakci s digitálním prostředím (například cookies).

¹⁰² LEENES, Ronald; SCHALLABÖCK, Jan; HANSEN, Marit. op. cit., s. 1.

¹⁰³ Pochopitelně, pro přístup k tomuto výzkumu bylo třeba se u Cybersecurity Ventures identifikovat. Má identifikace jako afghánská společnost Pes a.s. proběhla úspěšně a úroveň záruky tohoto systému jsem tak vyhodnotil jako neexistující. In: MORGAN, Steven C. CARSON, Joseph. *The World Will Need to Protect 300 Billion Passwords*

Státem zaručené systémy elektronické identifikace jsou provozovány bez ohledu na hospodářskou situaci a v Evropské unii neexistuje jediný stát, který by systém elektronické identifikace svým občanům neposkytoval (nebo takový systém nevyvíjel).¹⁰⁴ Vytvoření jediné celosvětové elektronické identity se v současné době nejeví jako uskutečnitelné a není ani žádoucí. Z toho důvodu je pro rozvoj přeshraničního eGovernmentu a elektronického obchodu nezbytné, aby některé systémy byly interoperabilní, zejména aby uznávaly prostředky elektronické identifikace vydané v rámci jiných systémů, respektive elektronické identity na nich obsažené. Interoperabilita těchto systémů však naráží na několik bariér, především právních a technických, které ve svém důsledku vedou ke vzájemné nedůvěře mezi těmito systémy.

Díky nekoordinovanému vývoji a rozdílné právní tradici jsou systémy pro elektronickou identifikaci řízeny rozdílnou právní úpravou, která zvyšuje problém přeshraničního uznávání úměrně s úrovní jistoty pro elektronickou identifikaci v konkrétním případě vyžadované. Pokud pak elektronická identifikace nesplňuje právní požadavky obou stran, je její využití v přeshraničním styku vyloučené.

Plnohodnotné uznání spatřuji v naplnění tři kritérií. V první řadě by použití prostředku cizího státu mělo mít stejný právní efekt jako použití prostředku vnitrostátního. Zúčastněným zahraničním a vnitrostátním

By 2020. *Cybersecurity Ventures* [online]. Cybersecurity Ventures: 2013 [cit. 2019-02-28] p. 2.

¹⁰⁴ Srov. SHEHU; PINTO; CORREIA. op. cit. 341.

osobám by měly být ukládány stejné povinnosti a konečně by měly nést stejnou odpovědnost za jejich porušení.¹⁰⁵

Problémem stojícím v cestě prvnímu kritériu může být například skutečnost, že státy vyžadují jiné sady identifikačních údajů pro určení totožnosti, či pro funkcionalitu systémů vyžadují specifická softwarová nebo hardwarová řešení.^{106,107}

Kritickou roli v určení povinností mohou hrát úrovně záruky, pokud na jejich parametrech existuje shoda. V zájmu států, jejichž prostředky elektronické identifikace poskytují vyšší úroveň záruky pak zpravidla není uznání prostředků s úrovní záruky nižší.¹⁰⁸

Nezanedbatelná je pak otázka výkonu dohledu a odpovědnosti. Ta by mohla vyžadovat například vytvoření nové mezinárodní organizace, nebo rozšíření působnosti a pravomoci organizace již existující.

Svá vlastní specifika pak přináší soukromoprávní oblast, neboť účastníci soukromoprávních vztahů požívají vysokou míru autonomie vůle a autoritativní určení alespoň minimálních standardů nebo jiných pravidel může být pro praxi odrazující. Autoritativní stanovení alespoň základních pravidel by však mohlo předejít zneužívání osobních údajů uživatelů. Domnívám se, že užití přeshraniční elektronické identifikace v praxi nalezne využití spíše v oblasti SME (například u eshopů), kde

¹⁰⁵ Srov. United Nations Commission on International Trade Law. *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods* [online]. Vienna: United Nations Publications, 2019 [cit. 30.10.2018]. s. 80.

¹⁰⁶ DUMORTIER. op. cit. s. 10.

¹⁰⁷ Překonání technologické bariéry není předmětem této práce, nicméně právní úprava by měla být technologicky neutrální.

¹⁰⁸ Dá se však shrnout, že k dispozici by měly být prostředky s více úrovněmi záruk. Větší míra důvěry bude bezpochyby potřeba při podání daňového přiznání než při přístupu ke studijním materiálům.

náklady na identifikaci mohou představovat znatelnou část celkové hodnoty transakce, které využití důvěryhodného ověřování totožnosti může minimalizovat.

Lze tak shrnout, že problematika přeshraniční elektronické identifikace je značně komplexní, a pro řádné fungování by vyžadovala harmonizaci vnitrostátních úprav (nebo přijetí normy vyšší právní síly). Toho však nelze dosáhnout bez vzájemné dohody a mezistátní spolupráce.

Domnívám se však, že nedůvěra v zahraniční prostředky elektronické identifikace bude v brzké budoucnosti překonána, neboť její kořeny vycházejí z faktu, že oblast elektronické identifikace (a zejména pak v oblasti mezinárodní spolupráce) byla dlouho tradičním právem, založeném na papírovém prostředí, přehlížena, zatímco v dnešní době je nutnost přeshraničního uznávání elektronické identity čím dál šířeji přijímána. Nakonec je však třeba přijmout skutečnost, že ani na úrovni Evropské unie před použitelností EIDAS významná mezinárodní spolupráce v oblasti přeshraničního uznávání elektronické identifikace neprobíhala, a spolupráce byla členskými státy v podstatě *nařízena*.

4.2 Řešení v rámci Evropské unie – povinnost vzájemného uznávání podle EIDAS

Problém absence právní úpravy bezpečné a důvěryhodné přeshraniční elektronické identifikace na úrovni Evropské unie byl Evropskou komisí dlouhodobě adresován (například již v Akčním plánu pro elektronické podpisy a elektronickou identifikaci z listopadu 2008)¹⁰⁹ a byl označen za jednu z překážek digitálního rozvoje v Evropě.¹¹⁰

Historická zkušenost ukázala, že zajištění důvěryhodnosti přeshraničního užívání služeb pro elektronickou identifikaci v rámci Evropské unie nebylo možné uspokojivě dosáhnout na úrovni jednotlivých členských států. Naopak, vnitrostátní řešení často vytvářela pro jejich interoperabilitu překážky a státy si navzájem prostředky elektronické identifikace neuznávaly.¹¹¹ Zajištění přeshraniční interoperability těchto prostředků si klade za cíl EIDAS, a to alespoň v oblasti veřejných služeb.¹¹²

4.2.1 Povinnost vzájemného přeshraničního uznávání

¹⁰⁹ SDĚLENÍ KOMISE RADĚ, EVROPSKÉMU PARLAMENTU, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ, Akční plán pro elektronické podpisy a elektronickou identifikaci zaměřený na usnadnění poskytování přeshraničních veřejných služeb v rámci jednotného trhu ze dne 28. listopadu 2008. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 11. 12. 2018].

¹¹⁰ Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu ze dne 4. června 2012. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 11. 12. 2018].

¹¹¹ Srov. Recitál 9 EIDAS.

¹¹² Srov. Recitál 12 EIDAS.

Zajištění přeshraniční interoperability podle EIDAS je dosaženo pomocí takzvaných oznámených systémů elektronické identifikace. Státy, které za podmínek stanovených EIDAS takové systémy řádně oznámí, umožní svým občanům využití jejich prostředků pro elektronickou identifikaci v rámci celé Evropské unie.

EIDAS stanovuje povinnost přeshraničního uznávání prostředků pro elektronickou identifikaci ve svém článku 6. Dle tohoto článku povinnost uznat prostředek pro elektronickou identifikaci vydaný v jiném členském státě platí za následujících předpokladů:

- jedná se o přístup ke službě¹¹³ poskytované online;
- poskytovatelem služby je subjekt veřejného sektoru členského státu;
- pro přístup k této službě se vyžaduje elektronická identifikace s použitím prostředku pro elektronickou identifikaci a autentizaci;
a
- elektronická identifikace je vyžadována podle vnitrostátního práva nebo správní praxe.

Dále musí dojít ke splnění tří podmínek. První z podmínek stanovuje, že systém elektronické identifikace, v rámci kterého je prostředek pro elektronickou identifikaci vydán, je uveden na seznamu zveřejněném Komisí. Jinými slovy, musí dojít k jeho oznámení podle článku 9 EIDAS. Aby byl systém pro elektronickou identifikaci způsobilý pro oznámení, je třeba nejprve splnit množství podmínek stanovených

¹¹³ Přesto, že se povinnost přeshraničního uznávání vztahuje na přístup ke službám, pojem služby jako takové v rámci EIDAS definován není. Vodítko poskytuje jeho recitál 2, dle kterého se dá za online službu považovat služba poskytovaná soukromými i veřejnými poskytovateli, a to za předpokladu, že je poskytovaná pomocí prostředků elektronické komunikace.

v článku 7 EIDAS. Prostředky pro elektronickou identifikaci tak musí například být možné „*použít pro přístup k alespoň jedné službě poskytované subjektem veřejného sektoru, u níž se v oznamujícím členském státě vyžaduje elektronická identifikace,*“ či musí splňovat požadavky alespoň jedné úrovně záruky.

Počátkem procesu oznámení je poskytnutí popisu systému elektronické identifikace ostatním členským státům, a to alespoň šest měsíců před samotným oznámením (takzvaná prenotifikace). Důvodem tohoto předběžného oznámení je následné vzájemné hodnocení (*peer-review*) ze strany ostatních členských států. Vzájemné hodnocení by mělo být považováno za proces vzájemného učení, pomáhající vybudovat důvěru mezi členskými státy,¹¹⁴ a to pomocí výměny informací, zkušeností a osvědčených postupů.¹¹⁵ Z textu prováděcího nařízení upravujícího tento postup nevyplývá povinnost vzájemné hodnocení provést, když tento proces se zahajuje buď na žádost členského státu o zhodnocení jeho vlastního systému elektronické identifikace, nebo na žádost některého ze třetích států, který vyjádří zájem vzájemné hodnocení provést.¹¹⁶ Délka procesu vzájemného hodnocení by neměla přesáhnout tři měsíců.¹¹⁷

Po tomto předběžném oznámení může teprve členský stát učinit formální oznámení systému komisi. Komise poté zveřejní změny (ve formě zápisu nového systému) v seznamu systémů elektronické identifikace v Úředním věstníku Evropské unie do dvou měsíců od

¹¹⁴ Recitál 6 Prováděcího nařízení Komise č. (EU) 2015/296.

¹¹⁵ Recitál 5 Prováděcího nařízení Komise č. (EU) 2015/296.

¹¹⁶ Článek 8 Recitál 3 Prováděcího nařízení Komise č. (EU) 2015/296.

¹¹⁷ Článek 9 odstavec 2 písm. b) Prováděcího nařízení Komise č. (EU) 2015/296.

obdržení takového oznámení.¹¹⁸ Teprve od oznámení v Úředním věstníku EU začíná plynout lhůta dvanácti měsíců, po jejímž uplynutí musí ostatní státy uznávat prostředky pro elektronickou identifikaci vydané v takto oznámeném systému elektronické identifikace¹¹⁹ pro účely přeshraniční autentizace pro své online služby veřejné správy.

Druhá podmínka vyžaduje, aby úroveň záruky při přeshraniční autentizaci mezi členskými státy byla vždy stejná nebo vyšší ve srovnání s vnitrostátní autentizací.¹²⁰

Třetí podmínka vylučuje pro přeshraniční uznávání systémy s nízkou úrovní záruky. Dle této podmínky totiž příslušný subjekt veřejného sektoru musí používat v souvislosti s přístupem k online službě značnou nebo vysokou úroveň záruky.¹²¹ Výjimku umožňuje odst. 2 článku 6 EIDAS, který umožňuje subjektům veřejného sektoru pro účely přeshraniční autentizace uznání prostředku pro elektronickou identifikaci pouze s nízkou úrovní záruky, a to za předpokladu, že tento prostředek byl vydán v rámci systému elektronické identifikace uvedeného na seznamu zveřejněném komisí.¹²²

4.2.2 Zajištění interoperability podle EIDAS

Ústřední roli při propojení vnitrostátních systémů elektronické identifikace podle EIDAS hrají takzvané uzly. Uzel je

¹¹⁸ Článek 9 odstavec 3 EIDAS.

¹¹⁹ Článek 6 odstavec 1 *en fine* EIDAS.

¹²⁰ Článek 6 odstavec 1 písmeno b) EIDAS.

¹²¹ Článek 6 odstavec 1 písmeno b) EIDAS.

¹²² Článek 6 odstavec 2 EIDAS.

„místo připojení, které je součástí architektury interoperability elektronické identifikace umožňující přeshraniční autentizaci osob, která je schopna rozeznat a zpracovávat přenosy údajů nebo je předávat na jiné uzly a tím umožňuje propojení vnitrostátních infrastruktur elektronické identifikace jednotlivých členských států.“¹²³

Jsou to tedy právě uzly, mezi kterými probíhá komunikace v rámci přeshraniční elektronické identifikace mezi subjekty z jednotlivých členských států. Do procesu elektronické identifikace v tomto případě vstupuje jeho další účastník, takzvaný provozovatel uzlu, který je odpovědný za správné a spolehlivé plnění funkce místa připojení. Uzel může být provozován jak veřejnoprávními, tak soukromoprávními subjekty. EIDAS ani prováděcí nařízení nestanovuje maximální počet uzlů nacházejících se v jednom státě.

4.2.3 Oznámené systémy

EIDAS umožňuje oznámení systémů elektronické identifikace, v rámci kterých jsou prostředky pro elektronickou identifikaci vydávané jak státem, tak prostředky, které jsou vydávané z jeho pověření, ale i nezávisle na tomto státě.¹²⁴

V současné době má své oznámené systémy elektronické identifikace devět států, dalších sedm učinilo prenotifikaci.¹²⁵ Pouze ve dvou z těchto již oznámených systémů (konkrétně systémů Itálie a Spojeného království) jsou vydávány prostředky elektronické

¹²³ Bod 2 článku 2 prováděcího nařízení č. 2015/1501

¹²⁴ Článek 7 EIDAS.

¹²⁵ Overview of pre-notified and notified eID schemes under eIDAS. *CEF Digital collaboratives spaces* [online]. European Commission, 2019 [cit. 2019-5-28].

identifikace z pověření státu, v žádném případě pak ne nezávisle na oznamujícím státu.¹²⁶ Ze všech šestnácti evidovaných systémů jsou to právě tyto dva systémy, které nabízejí prostředky elektronické identifikace i nízké úrovně záruky. Takové prostředky v přeshraničních transakcích přijímané být nemusí, jejich nízká úroveň záruky totiž může potenciálně představovat hrozbu vzniku škody.

4.3 Přeshraniční spolupráce v České republice

ZOEI je účinný k 1. červenci 2018, od tohoto data tedy považuje za kvalifikované systémy i oznámené systémy elektronické identifikace dle EIDAS. Přechodné ustanovení ZOEI sice umožňuje prokázání totožnosti pomocí elektronické identifikace, při kterém se nepoužije kvalifikovaný systém, to však kvalifikované poskytovatele nezbavuje povinnosti uznávat prostředky pro elektronickou identifikaci uvedené na seznamu zveřejňovaném komisí (resp. po uplynutí dvanácti měsíců od zveřejnění tohoto seznamu¹²⁷, což v současné době splňuje pouze německý systém elektronické identifikace).

Česká republika též učinila kroky k oznámení svého systému elektronické identifikace pod názvem „Národní identifikační systém České republiky,“ v rámci kterého se jako prostředek elektronické identifikace vydává elektronický občanský průkaz,¹²⁸ kdy v současné

¹²⁶ Zjištěno na základě analýzy dostupných notifikačních dokumentů. In: *Ibid.*

¹²⁷ Článek 6 *en fine* EIDAS.

¹²⁸ National identification scheme of the Czech Republic. *NOTIFICATION FORM FOR ELECTRONIC IDENTITY SCHEME UNDER ARTICLE 9(5) OF REGULATION (EU) No 910/2014* [online]. Ministry of the interior of the Czech Republic, 2018 [cit. 27.5.2019]. s. 3.

době probíhá jeho peer-review, které započalo 1. února 2019. Podle predikcí Petra Kuchaře, hlavního architekta eGovernmentu v České republice se můžeme dočkat uznávání českého elektronického občanského průkazu pro přístup ke službám poskytovaných v jiných členských státech v srpnu, nebo září roku 2020.¹²⁹

¹²⁹ KUCHAR. op. cit. pp. 11.

5 Mezinárodní iniciativy v oblasti elektronické identifikace

5.1 OECD

Komplikace, které mohou nastat při odlišném právním vývoji národních řešení elektronické identifikace v oblasti elektronického obchodu na mezivládní úrovni, adresovala jako jedna z prvních organizace OECD, která v roce 1998 vydala „Deklaraci o autentizaci pro elektronický obchod“. Ta vyjadřuje v první řadě odhodlání signatářských států nediskriminovat elektronickou autentizaci z jiných států.¹³⁰ V následujících letech se organizace na své půdě nadále věnovala výzkumů v oblasti elektrocnikých identit, vyvrcholením kterých jsou především dvě publikace. Těmi jsou „Doporučení OECD pro elektronickou autentizaci“ z roku 2007 a publikace „Správa digitálních identit: Podpora inovací a důvěry v internetovou ekonomiku“ z roku 2011, která má sloužit především vládním normotvůrcům ke vzájemnému porozumění rolím elektronických identit a internetové ekonomiky.

Byť tyto dokumenty bezesporu mohou posloužit svému účelu a nabízí cenné shrnutí potřebnosti a vhodnosti vývoje v oblasti elektronické autentizace jako takové, právní relevanci postrádají, neboť ze své podstaty mohou sloužit pouze jako podklady pro další normotvorbu. Pro přeshraniční spolupráci nanejvýše proklamují, že státy by neměly vytvářet diskriminační prostředí a měly by *ideálně*

¹³⁰ OECD. *Ministral Declaration on Authentication for Electronic Commerce* [online]. OECD, 2019 [cit. 30.11.2018]. s.4.

uznávat služby elektronické autentizace jiných států, pokud tyto splňují vnitrostátní požadavky, nebo jejich ekvivalent.¹³¹

5.2 UNCITRAL

Komise UNCITRAL je klíčovým právním orgánem Spojených národů v oblasti mezinárodního obchodního práva a její mandát spočívá v podpoře harmonizace a modernizace mezinárodního obchodního práva. To obnáší především přípravu a propagaci právních a neprávních instrumentů v klíčových oblastech mezinárodního obchodního práva. Díky procesu přípravy těchto instrumentů, na kterém spolupracují kromě členských států komise i jiné mezivládní a soukromé subjekty, jsou výsledné texty široce uznávány, neboť zohledňují odlišné právní tradice a stupně hospodářského vývoje.¹³² Tyto instrumenty jsou právně nezávazné (jedním z nejvýznamnějších instrumentů jsou tzv. modelové zákony), avšak v návaznosti na práci komise mohou jednotlivé státy provést revize své národní právní úpravy.

Zatímco zpočátku¹³³ se komise scházela jako celek, nyní působí prostřednictvím svých šesti takzvaných pracovních skupin. Zaměření těchto skupin se v průběhu let měnilo, a Pracovní skupina IV, která se ve svém počátku věnovala mezinárodním obchodovatelným nástrojům, se od roku 1996 zabývá elektronickým obchodem. Od té doby byly na její půdě vypracovány například modelové zákony k elektronickému

¹³¹ OECD. 2007. op. cit. s. 25.

¹³² United Nations Commission on International Trade Law. A Guide to UNCITRAL: Basic facts about the United Nations Commission on International Trade Law [online]. Vienna: United Nations, 2013 [cit. 2016-11-20]. s. 1.

¹³³ Od svého založení 17. prosince 1966 rezolucí Valného shromáždění Organizace spojených národů 2205 (XXI).

obchodu, k elektronickému podpisu a k převoditelným elektronickým instrumentům nebo Úmluva OSN k užití elektronické komunikace v mezinárodních transakcích. Čtvrtá pracovní skupina se schází dvakrát ročně na schůzích v délce jednoho týdne, na kterých dochází k debatám a přijímání dílčích rozhodnutí mezi zúčastněnými stranami. V mezičase se pak připravují podkladové materiály.

Na půdě komise započala v roce 2015 diskuze o právních aspektech správy identit. Čtvrtá pracovní skupina se tomuto tématu začala věnovat po dokončení své práce na Modelovém zákoně k převoditelným elektronickým instrumentům v roce 2017 a její práce má směřovat k přípravě právního rámce elektronické identifikace včetně ustanovení umožňujících její přeshraniční interoperabilitu.¹³⁴

5.2.1 Návrh ustanovení o přeshraničním uznávání elektronické identifikace a služeb vytvářejících důvěru

Sekretariát UNCITRAL zpřístupnil pracovní papíry (anglicky: *working papers*) obsahující návrh ustanovení o přeshraničním uznávání elektronické identifikace a služeb vytvářejících důvěru, společně s komentářem k tomuto návrhu. Jako základní problém je identifikován nedostatek důvěry, k odstranění kterého by měla vést podpora vzájemné interoperability mezi systémy elektronické identifikace, a to veřejnými i soukromými.

Jak vyplývá ze zápisů z jednání pracovní skupiny, mnoho otázek, včetně těch nejzásadnějších, je stále předmětem intenzivních politických

¹³⁴ United Nations Commission on International Trade Law. *A/CN.9/854 - Possible future work in the area of electronic commerce — legal issues related to identity management and trust services. Proposal by Austria, Belgium, France, Italy and Poland* [online]. Vienna: United Nations, 2015, 8 s. [vid. 30.10.2018]. s. 6.

debat mezi jejími jednotlivými členy. V současné době tak ani nebylo rozhodnuto o tom, jaká konkrétní forma instrumentu bude pro regulaci zvolena. Návrh je koncipován tak, aby obsahoval základ jak pro modelový zákon, který mohou jednotlivé státy převzít do své legislativy, tak pro mezinárodní smlouvu¹³⁵. Návrh tak často pro jednotlivé články nabízí více řešení s různým rozsahem, přístupem a pojmoslovím, přičemž tato se budou v průběhu dalších jednání upravovat.

Návrh článků stojí na čtyřech základních zásadách, které jsou již v řadě instrumentů UNCITRAL uplatňovány a jsou považovány za základní prvky moderního práva elektronického obchodu. Těmito zásadami jsou: (i) zásada zákazu diskriminace elektronických prostředků, která zakazuje odmítnutí právních účinků, platnosti či důkazní přípustnosti určitého prostředku jen proto, že existuje v elektronické podobě, (ii) zásada autonomie stran, (iii) zásada technologické neutrality, která stanoví, že přijatá ustanovení musí být neutrální ve vztahu k použitým technologiím a (iv) zásada funkční rovnocennosti, podle které mají být elektronickému jednání přiznávány stejné právní účinky, pokud je schopné plnit stejnou funkci jako jednání neelektronické.

V současné době počítá návrh článků jak s identifikací osob, tak i věcí, neboť ty mohou být subjektem obchodu. Věci však budou muset

¹³⁵ United Nations Commission on International Trade Law. A/CN.9/WG.IV/WP.158 *Explanatory Remarks on the Draft Provisions on the Cross-border Recognition of Identity Management and Trust Services* [online]. New York: United Nations, 2019, 11 s [cit. 12.2.2019]. s. 3.

fungovat v jiném právním režimu, neboť nemají právní osobnost a nemohou tak nést odpovědnost.¹³⁶

Základním ustanovením pro správu identit je zásada funkční rovnocennosti. Elektronický způsob identifikace by měl být považovaný za rovnocenný tomu analogovému v případě, kdy:

„spolehlivá metoda je použita k ověření významných atributů subjektu v souladu se stejnou mírou jistoty“¹³⁷

Požadavky na spolehlivou metodu jsou zatím určeny značně neurčitě. V úvahu by měly být brány zejména dohody mezi stranami, dohled nad příslušným systémem nebo jeho certifikace a úroveň záruky s ním spojená. Z konstrukce návrhu a poznámek v něm uvedených dále vyplývá, že další debaty čtvrté pracovní skupiny by mohly vést například ke stanovení alespoň minimálních konkrétních požadavků na systémy, jako například požadavky na audit, pojištění, nebo akreditaci.

Návrh zatím neuvádí ani základní určení nebo popis úrovně záruky, byť na ně ve svém textu odkazuje. Vzhledem k probíhající debatě mezi stranami není možné odhadnout, zda budou ve finálním textu obsaženy.¹³⁸

¹³⁶ United Nations Commission on International Trade Law. A/CN.9/WG.IV/WP.158 *Explanatory Remarks on the Draft Provisions on the Cross-border Recognition of Identity Management and Trust Services* [online]. New York: United Nations, 2019 [cit. 12.2.2019]. s. 3.

¹³⁷ United Nations Commission on International Trade Law. A/CN.9/WG.IV/WP.157 *Draft Provisions on the Cross-border Recognition of IdM and Trust Services* [online]. New York: United Nations, 2019 [cit. 12.2.2019]. s. 6.

¹³⁸ United Nations Commission on International Trade Law. A/CN.9/965 *Report of Working Group IV (Electronic Commerce) on the work of its fifty-seventh session*

Návrh upravuje v současné podobě režim odpovědnosti pouze pro provozovatele systému elektronické identifikace¹³⁹ (ať již soukromoprávní nebo veřejnoprávní). Ti jsou podle návrhu odpovědní za škodu způsobenou neposkytováním služby v souladu se smlouvou nebo zákonnými požadavky. Návrh, stejně jako EIDAS, požaduje především řádnou identifikaci a zajištění dostupnosti procesů elektronické identifikace. Návrh umožňuje tuto odpovědnost limitovat nastavením omezení pro použití těchto služeb za předpokladu, že je takové omezení dostatečně známé. Pevně určená není ani forma zavinění.

V oblasti odpovědnosti nejsou v současné době stanovena pravidla pro určení, řádem kterého státu se bude režim odpovědnosti řídit. Vzhledem k problematice této otázky je dokonce zvažována nutnost vytvoření specifické mezinárodní úpravy. Variantou je také použití vnitrostátního režimu odpovědnosti pro systémy elektronické identifikace zahraničních států.

Samotnému přeshraničnímu aspektu elektronické identifikace se věnují závěrečné dva články návrhu. Návrh v zásadě stanovuje nediskriminační pravidlo, podle kterého mají zahraniční prostředky stejný právní účinek jako ty vnitrostátní, a to v případě, že poskytují stejnou úroveň spolehlivosti.¹⁴⁰

(Vienna, 19–23 November 2018) [online]. Vienna: United Nations, 2018 [cit. 12.2.2019]. s. 9.

¹³⁹ Na rozdíl od Modelového zákona pro elektronické podpisy, který upravoval odpovědnost i spoléhajících se stran.

¹⁴⁰ United Nations Commission on International Trade Law. A/CN.9/WG.IV/WP.157. op. cit. 11.

Závěrečný článek pak vyžaduje, aby určené orgány a osoby, veřejné i soukromé, v oblasti elektronické identifikace a služeb vytvářejících důvěru spolupracovaly se svými zahraničními protějšky, a to zejména v oblastech certifikace, definice úrovně záruky nebo diskuzí o nedávném vývoji.

5.2.2 Předpokládaný další vývoj

Návrh článků v současné době svou neurčitostí odráží nekoherentnost kulturního a ekonomického prostředí, která je dána odlišným stupněm rozvoje a rozdíly kvality právních úprav zúčastněných států. Návrh je tak zatím pouze jakousi základní kostrou, jejíž výslednou podobu lze zatím stěží odhadovat, neboť dosáhnout mezi členy shody i na základních otázkách se zdá být velice obtížné. O tom jsem měl možnost se přesvědčit osobně během 57. schůze skupiny konající se ve dnech 19-23. listopadu 2018, které jsem měl tu čest se zúčastnit jako delegát Ústavu práva a technologií Masarykovy univerzity. Zatímco některé příspěvky byly přínosné a zdá se, že vývoj řídí skupina několika zainteresovaných členů, jiné příspěvky naopak postup vyloženě tlačí zpět. Tento stav je podle mého dán i relativně malou frekvencí schůzí a nezanedbatelnou roli hrají i orgány UNCITRALU připravující podkladové materiály, jak jsem zjistil při porovnání mého zápisu z jednání se zněním oficiálního shrnutí schůze.

Návrh je navíc v současné době připravován již s vědomím úpravy EIDAS, se kterým jsou jeho jednotlivé body srovnávány a uvažuje se tak i o sjednocení pojmosloví. Z tohoto důvodu ani není vhodné stanovovat adresátům úpravy zásadně odlišné nebo přísnější podmínky a domnívám se proto, že cesta minimální úpravy se nabízí jako nejvhodnější řešení.

6 Závěr

Záměrem první části této práce bylo analyzovat standardní systém elektronické identifikace. Než jsem začal tuto práci psát, jsem si neuvědomoval, jak všudypřítomným každodenním fenoménem elektronická identifikace ve skutečnosti je, kolik má forem a kolik elektronických identit je běžně používáno. Domnívám se však, že díky analýze dostupné odborné literatury (pro přístup ke které jsem se často musel elektronicky identifikovat) se mi podařilo nejen provést výklad pojmu elektronické identifikace, ale také analyzovat základní procesy, které v systémech elektronické identifikace probíhají. Přesto, že jedno standardní řešení těchto systémů neexistuje, uvedl jsem i přehled jejich základních typů a upozornil jsem na nedostatky a možné komplikace, které jsou vlastní jak jednotlivým typům systémů, tak elektronické identifikaci jako takové.

Zatímco pro přístup k odborným článkům nebo například pro nákup v eshopu není vyžadována vysoká míra důvěry v elektronickou identifikaci, vyskytují se v elektronickém prostředí případy, ve kterých je důvěryhodné ověření totožnosti nezbytné, a to zejména v oblasti přístupu ke službám poskytovaným státy svým občanům. Za tímto účelem většina vyspělých států, včetně České republiky, v dnešní době již pro své občany zřídila systémy, které důvěryhodnou elektronickou identifikaci umožňují.

Při analýze české právní úpravy jsem pak upozornil na některá její úskalí. Domnívám se, že elektronická identifikace má v České republice potenciál. Tomu, aby mohl být naplno využit, však stále brání některé, převážně legislativní překážky.

Dospěl jsem k závěru, že vývoj systémů důvěryhodné identifikace probíhal mezi státy nekoordinovaně a v současné době je téměř nemožné využít elektronické identity vydané v jednom státě pro přístup ke službám poskytovaným jiným státem. Zaměřil jsem se tedy na konkrétní problémy, které přeshraničnímu uznávání elektronických identit brání a pokusil jsem se najít jejich možné řešení.

Problematiku neuznávání elektronických identit adresuje v Evropské unii v oblasti veřejných služeb EIDAS, a to zavedením povinnosti pro členské státy umožnit přístup ke svým službám pomocí prostředků elektronické identifikace vydaných v jiném členském státě, pokud takové systémy splňují podmínky EIDAS a jsou řádně oznámeny. Z toho důvodu jsem analyzoval a popsal elektronickou identifikaci podle EIDAS a dále způsob, jakým je interoperabilita zajištěna. Závěrem lze shrnout, že EIDAS je v současné době jediným řešením, které právně upravuje přeshraniční uznávání elektronických identit mezi státy.

Obdobné ambice má v současné době pouze UNCITRAL, jehož čtvrtá pracovní skupina si dala za cíl vytvořit právní instrument pro přeshraniční uznávání elektronických identit, a to primárně pro oblast mezinárodního obchodu. Oproti mému očekávání však musím konstatovat, že v současné době jsou přípravy budoucího instrumentu ve velmi rané fázi, a samotný instrument dostává konkrétní obrysy velmi pomalu.

Použité zdroje

Monografie

1. DE ANDRADE, Norberto Nuno Gomes et al. *Electronic identity*. New York: Springer, 2014, 90 s. ISBN 978-1-4471-6448-7.
2. DONÁT, Josef; MAISNER, Martin; PIFFL, Robert. *Nařízení eIDAS. Komentář*. 1. vyd. Praha: Nakladatelství C.H. Beck, 2017, Beckovy komentáře, 300 s. ISBN 978-80-7400-633-3.
3. LAURENT, Maryline; BOUZEFRANE, Samia. *Digital Identity Management*. 1 ed. London: ISTE Press Ltd, 2015, s. 272. ISBN 978-1-78548-004-1.
4. POLČÁK, R. a kol. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer ČR, 2018, 656 s. ISBN 978-80-7598-045-8.
5. United Nations Commission on International Trade Law. *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods* [online]. Vienna: United Nations Publications, 2019, 114 p. [cit. 30.10.2018]. ISBN 978-92-1-133663-4 Available from: https://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf.

Články

6. ANDRAŠKO, Josef. MUTUAL RECOGNITION OF ELECTRONIC IDENTIFICATION MEANS UNDER THE EIDAS REGULATION AND ITS APPLICATION ISSUES. In: *AD ALTA: Journal of Interdisciplinary Research* [online]. 2017, vol. 7, no. 2, s. 9-13 [cit. 11. 12. 2018]. Available at: http://www.magnanimitas.cz/ADALTA/0702/papers/A_androsko.pdf.
7. ARNER, Douglas W. et al. The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. *European Banking Institute Working Paper Series 2018*. [online]. European Banking Institute, 2018, no. 28 [cit. 2019-02-28]. Available from: <https://www.ssrn.com/abstract=3224115>.

8. BÍLEK, Filip et al. Nařízení eIDAS (nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu). In: *Sborník konference ISSS, duben 2014* [online]. 2014, s. 4 [cit. 11. 12. 2018]. Dostupné z: https://www.cybersecurity.cz/data/MVCR_eIDAS.pdf.
9. CUIJPERS, Colette; SCHROERS, Jessica. eIDAS as guideline for the development of a pan European eID framework in FutureID. *HÜHNLEIN, D. (eds.). GI-Edition Lecture Notes in Informatics* [online]. 2014, p. 23-38 [cit. 11. 12. 2018] Available at: <http://hdl.handle.net/2066/135087>.
10. DUMORTIER, Jos. Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation). *SSRN Electronic Journal* [online]. Elsevier, 2016, 25 p. DOI: 10.2139, ISSN: 1556-5068. [cit. 2019-05-28] Available at: <https://www.ssrn.com/abstract=2855484>.
11. RISSANEN, Teemu. Electronic identity in Finland: ID cards vs. bank IDs. *Identity in the Information Society* [online] Springer Netherlands, 2010, no. 3, no.1, p. 175-194. [cit. 2019-05-28] DOI: 10.1007/s12394-010-0049-8. Available from: <http://link.springer.com/10.1007/s12394-010-0049-8>.
12. KMENT, Vojtěch. Evropské nařízení eIDAS: Impuls pro sjednocení elektronického podpisu a identifikace v EU. In: *JURISPRUDENCE* [online]. Praha: Wolters Kluwer, 2014, č. 6, s. 25-35. [cit. 28.2.2019] Dostupné z: <http://www.jurisprudence.cz/cz/casopis/evropske-narizeni-eidas-impuls-pro-sjednoceni-elektronickeho-podpisu-a-identifikace-v-eu.dm-107.pdf>.
13. KYNCL, Libor. *IP adresa identifikuje místo připojení, nikoli osobu*. *Revue pro právo a technologie*. [online]. 2011, č. 3, s. 5-6. [cit. 28.2.2019]. Dostupné z: <https://journals.muni.cz/revue/article/view/3986>.
14. LEENES, Ronald; SCHALLABÖCK, Jan; HANSEN, Marit. *PRIME White paper v2* [online]. PRIME, 2007. Published 27.6.2007. [vid. 12.2.2019]. Available from: https://www.researchgate.net/publication/248791660_PRIME_white_paper_v2.
15. MORGAN, Steven C. CARSON, Joseph. The World Will Need to Protect 300 Billion Passwords By 2020. *Cybersecurity Ventures*

- [online]. Cybersecurity Ventures: 2013, p. 5 [cit. 2019-02-28]. Available at: <https://thycotic.com/wp-content/uploads/2013/03/Cybersecurity-Ventures-Thycotic-Password-Protection.pdf>.
16. MYHR, Thomas. Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution: or I am 621216-1318, but I am also 161262-43774.1 Do you know who I am?. *Information Security Technical Report* [online]. Elsevier, 2008, vol. 13 issue 2, p. 76-82 [cit. 2019-2-28]. DOI: 10.1016/j.istr.2008.06.001. ISSN 13634127. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S1363412708000186>.
 17. POPE, Nick; ALIN, Jonathan. *The Impact of the European eIDAS Regulation* [online]. Thales e-Security, 28 p. [cit. 12.2.2019]. Available at: <http://go.thalesecurity.com/rs/480-LWA-970/images/ThalesEsecurity-European-eIDAS-Regulation-wp.pdf>.
 18. SHEHU, Abubakar-sadiq; PINTO, António; CORREIA, Manuel E. On the Interoperability of European National Identity Cards. In: *Novais P. et al. Ambient Intelligence – Software and Applications – 9th International Symposium on Ambient Intelligence. Advances in Intelligent Systems and Computing*. Springer, Cham. 2018, vol. 806. p. 338-348 [cit. 2019-2-28] DOI: 10.1007/978-3-030-01746-0_40. Available from: https://link.springer.com/chapter/10.1007/978-3-030-01746-0_40.
 19. SULLIVAN, Clare. Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review* [online]. 2018, vol. 34, issue 4, s. 723-731 [cit. 2019-02-28]. DOI: 10.1016/j.clsr.2018.05.015. ISSN 02673649. Dostupné z: <https://linkinghub.elsevier.com/retrieve/pii/S0267364918302024>.
 20. WILSON, Stephen; MOUSTAFA, Nour; SITNIKOVA, Elena. A digital identity stack to improve privacy in the IoT. In: *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. Singapore: IEEE, 2018, 2018, s. 25-29. DOI: 10.1109/WF-IoT.2018.8355199. ISBN 978-1-4673-9944-9. Dostupné z: <https://ieeexplore.ieee.org/document/8355199/>.

Internetové zdroje

1. Bezpečnější transakce na internetu. *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie, 2016 [cit. 11. 12. 2018] Dostupné z: http://publications.europa.eu/resource/cellar/7b35b005-fc14-42a3-8447-3699baf44f2d.0002.02/DOC_2.
2. digitální;ČESKO. Vládní program digitalizace České republiky 2018+. Shrnutí implementačních plánů pro 2019. In: *Digitální Česko* [online] Praha: Úřad vlády České republiky, 2019, 16 s. [cit. 2019-5-28] Dostupné z: <https://www.mvcr.cz/soubor/shrnuti-implementacnich-planu-pro-2019.aspx>.
3. KUCHAR, Petr; Elektronická identifikace v ČR, NIA, eOP. In: *konference eIDENTITA 2019* [online]. Praha: Ministerstvo vnitra České republiky, 2019, pp. 13 [cit. 2019-5-28] Available from: <https://www.egovernment.cz/soubor/elektronicka-identifikace-2019-petr-tiller-oha-mv-cr/>.
4. MojeID: ZALOŽENÍ NOVÉHO ÚČTU. *MojeID* [online]. Praha: CZ.NIC, z. s. p. o., 2018 [cit. 2019-02-28]. Dostupné z: <https://mojeid.cz/registration/>.
5. OECD. *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication* [online]. OECD, 2007. p. 35. [cit. 30.11.2018]. Available from: <http://www.oecd.org/internet/ieconomy/38921342.pdf>.
6. OECD. The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers. *OECD Digital Economy Papers* [online]. OECD Publishing, Paris, 2009. p. 20. [cit. 30.11.2018]. DOI: 10.1787/222134375767. Available from: <http://dx.doi.org/10.1787/222134375767>.
7. OECD. *DIGITAL IDENTITY MANAGEMENT: Enabling Innovation and Trust in the Internet Economy* [online]. OECD, 2011, 182 p. [cit. 30.11.2018]. Available from: <http://www.oecd.org/sti/ieconomy/49338380.pdf>.
8. OECD. *Ministral Declaration on Authentication for Electronic Commerce* [online]. OECD, 2019, 4 s [cit. 30.11.2018]. Available from: <https://legalinstruments.oecd.org/public/doc/112/112.en.pdf>.
9. Overview of pre-notified and notified eID schemes under eIDAS. *CEF Digital collaboratives spaces* [online]. European Commission,

- 2019 [cit. 2019-5-28]. Available at: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS>.
10. SDĚLENÍ KOMISE RADĚ, EVROPSKÉMU PARLAMENTU, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ, Akční plán pro elektronické podpisy a elektronickou identifikaci zaměřený na usnadnění poskytování přeshraničních veřejných služeb v rámci jednotného trhu ze dne 28. listopadu 2008. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 11. 12. 2018].
11. ŠTĚPÁNEK, Pavel; DONÁT, Josef. *Projekt SONIA: příspěvek bank k rozvoji digitálního Česka. Konference ISSS Hradec Králové* [online]. Hradec Králové: Česká bankovní asociace, 2019, pp. 20 [cit. 2019-5-28] Dostupné z: https://www.issc.cz/archiv/2019/download/prezentace/cba_dolejsi.pdf.
12. Telecommunication standardization sector of ITU. *Recommendation ITU-T X.1252 - Baseline identity management terms and definition* [online]. Geneva: International Telecommunication Union, 2010. Published 27.7.2010, 24 p. [cit. 12.2.2019]. Available from: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1252-201004-I!!PDF-E&type=items.
13. GRAUX, Hans; MAJAVA, Jarkko; MEYVIS, Eric. *Study on eID Interoperability for PEGS: Update of Country Profiles. Analysis & assessment report* [online]. European Communities: 2009, 228 s., [cit. 11. 12. 2018]. Available from: <http://ec.europa.eu/idabc/servlets/Doc2ba1.pdf?id=32521>.
14. This is BankID. *BankID* [online]. Finansiell ID-Teknik BID AB, 2019 [cit. 2019-5-28] Dostupné z: <https://www.bankid.com/en/om-bankid/detta-ar-bankid>.
15. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.120 - Overview of identity management - Background paper submitted by the Identity Management Legal Task Force of the American Bar Association* [online]. Vienna: United Nations, 2012. [vid. 30.10.2018]. Available from: <https://undocs.org/A/CN.9/WG.IV/WP.120>.
16. United Nations Commission on International Trade Law. *A Guide to UNCITRAL: Basic facts about the United Nations Commission on*

- International Trade Law* [online]. Vienna: United Nations, 2013, 66 s. [cit. 2016-11-20]. Available at: <https://www.uncitral.org/pdf/english/texts/general/12-57491-Guide-to-UNCITRAL-e.pdf>.
17. United Nations Commission on International Trade Law. *A/CN.9/854 - Possible future work in the area of electronic commerce — legal issues related to identity management and trust services. Proposal by Austria, Belgium, France, Italy and Poland* [online]. Vienna: United Nations, 2015, 8 s. [vid. 30.10.2018]. Available from: <https://undocs.org/en/A/CN.9/854>.
 18. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.144 – Work in the field of electronic commerce – legal issues relating to electronic identity management and trust services – Proposal by Austria, Belgium, France, Italy, the United Kingdom and European Union* [online]. New York: United Nations, 2017. Distributed 30.1.2017. [vid. 30.10.2018]. Available from: <https://undocs.org/A/CN.9/WG.IV/WP.144>.
 19. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.150 - Legal issues related to identity management and trust services – Terms and concepts relevant to identity management and trust services* [online]. New York: United Nations, 2018. Distributed 6.2.2018 [vid. 30.10.2018]. Available from: <https://undocs.org/en/A/CN.9/WG.IV/WP.150>.
 20. United Nations Commission on International Trade Law. *A/CN.9/965 Report of Working Group IV (Electronic Commerce) on the work of its fifty-seventh session (Vienna, 19–23 November 2018)* [online]. Vienna: United Nations, 2018, 18 s [cit. 12.2.2019]. Available at: <https://undocs.org/A/CN.9/965>.
 21. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.157 Draft Provisions on the Cross-border Recognition of IdM and Trust Services* [online]. New York: United Nations, 2019, 11 s [cit. 12.2.2019]. Available at: <https://undocs.org/en/A/CN.9/WG.IV/WP.157>.
 22. United Nations Commission on International Trade Law. *A/CN.9/WG.IV/WP.158 Explanatory Remarks on the Draft Provisions on the Cross-border Recognition of Identity Management and Trust Services* [online]. New York: United Nations, 2019, 11 s [cit. 12.2.2019]. Available at: <https://undocs.org/en/A/CN.9/WG.IV/WP.158>.

23. World Economic Forum. *A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity* [online]. World Economic Forum, 2016, p. 108 [cit. 27.5.2019]. Available from: [http://www3.weforum.org/docs/WEF A Blueprint for Digital I dentity.pdf](http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf).

Právní předpisy

Zákony

24. Zákon č. 89/2012 Sb., občanský zákoník.
25. Zákon č. 250/2017 Sb., o elektronické identifikaci.
26. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.
27. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Právní předpisy EU

28. Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
29. PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace podle čl. 12 odst. 7 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.
30. PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2015/1501 ze dne 8. září 2015 o rámci interoperability podle čl. 12 odst. 8 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.
31. PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úroveň záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a

- Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.
32. PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2015/1984 ze dne 3. listopadu 2015, kterým se stanoví okolnosti, formáty a postupy pro oznamování podle čl. 9 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.
33. Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

Ostatní

34. Důvodová zpráva k zákonu č. 250/2017 Sb. o elektronické identifikaci, č. 250/2017 Dz. In: *ASPI* [právní informační systém]. Wolters Kluwer ČR
35. Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu ze dne 4. června 2012. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 11. 12. 2018]. Dostupný z: <https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A52012PC0238>.
36. National identification scheme of the Czech Republic. *NOTIFICATION FORM FOR ELECTRONIC IDENTITY SCHEME UNDER ARTICLE 9(5) OF REGULATION (EU) No 910/2014* [online]. Ministry of the interior of the Czech Republic, 2018, 7 s. [cit. 27.5.2019]. Available from: [https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Czech+Republic?preview=/74091909/105382087/2.CZ+eID+NOTIFICATION%20FORM+2018+11+22%20\(2\).pdf](https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Czech+Republic?preview=/74091909/105382087/2.CZ+eID+NOTIFICATION%20FORM+2018+11+22%20(2).pdf)