Univerzita Karlova

Filozofická fakulta

Ústav informačních studií a knihovnictví

Bakalářská práce

David Černý

Rozdíl mezi standardy elektronických podpisů před a po zavedení eIDAS

Difference between electronic signature standards before and after the introduction of eIDAS

Praha 2023

Vedoucí práce: Ing. Jitka Novotná, Ph.D.

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, že jsem řádně citoval všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 5. 12. 2023

David Černý

Poděkování

Poděkování patří vedoucí práce Ing. Jitce Novotné, Ph.D., za odborné vedení a pomoc při tvorbě práce. Dále bych chtěl poděkovat respondentům za spolupráci.

Abstrakt

Práce porovnává fungování českého elektronického podpisu před a po implementaci nařízení Evropského parlamentu a Rady, který zavedl evropský standard pro elektronickou komunikaci eIDAS (electronic IDentification, Authentication and trust Services). Teoretická část práce na základě rešerše z dostupných zdrojů popisuje legislativní úpravu obou systémů, způsoby jejich fungování a příklady použití. Praktická část obsahuje kvalitativní šetření v oblasti elektronických podpisů a popis průběhu implementace nařízení eIDAS v České republice včetně případových studií.

Klíčová slova

Elektronický podpis – elektronická komunikace – informační architektura – eGovernment

Abstract

The work compares the differences in the use of the Czech electronic signature before and after the implementation of the regulation of the European Parliament and Council, which introduced the European standard for electronic communication eIDAS (electronic IDentification, Authentication and trust Services). Based on the research from available sources, the theoretical part of the work describes the legislative regulation of both systems, their ways of functioning and examples of use. The practical part contains a qualitative study in the field of electronic signatures and a description of the implementation of the eIDAS regulation in the Czech Republic, including case studies.

Keywords

Electronic signature – electronic communication – information architecture – eGovernment

OBSAH

SEZNAM POUŽITÝCH ZKRATEK

EDI	elektronická výměna dat
eIDAS	evropský standard pro elektronickou komunikaci
ETSI	Evropský ústav pro telekomunikační normy
FIPS	Federal Information Processing Standard
I. CA	První certifikační autorita
IČO	identifikační číslo organizace
IT	informační technologie
MV ČR	Ministerstvo vnitra České republiky
NAKIT	Národní agentura pro komunikační a informační technologie
OSN	Organizace spojených národů
PKI	Infrastruktura veřejných klíčů
PSP	Poslanecká sněmovna Parlamentu České republiky
SPIS	Sdružení pro informační společnost
TDKIV	Terminologická databáze knihoven a informační vědy
ÚOOU	Úřad pro ochranu osobních údajů
USB	Universal Serial Bus

1. ÚVOD

Elektronický podpis byl zaveden koncem 90. let a oproti vlastnoručnímu podpisu je zde několik rozdílů. Za podepisujícího ho vytváří speciální software a namísto slov je složen pouze z číslic. Téma této práce jsem si vybral, protože mě tato problematika velice zajímá a elektronické podpisy považuji za velmi užitečný nástroj v životě v 21. století.

Teoretická část se zabývá legislativními předpisy upravujícími elektronický podpis a samotnou definicí tohoto pojmu. Charakterizuje jeho typy a způsoby používání.

Praktická část se soustředí na představení výsledků výzkumu provedeného mezi certifikačními agenturami v České republice. Dále popisuje hlavní rozdíly mezi starou a novou právní úpravou elektronických podpisů.

V seznamu odborných zdrojů převažují legislativní dokumenty, literatura a online zdroje. Prostudovány byly zdroje domácí i zahraniční. K citování zdrojů byl zvolen styl ČSN ISO 690.

2. TEORETICKÁ ČÁST

2.1 Zákon o elektronickém podpisu

2.1.1 Důvody vytvoření právního předpisu

Podnětem k úvahám o tvorbě zákona o elektronickém podpisu bylo stále rostoucí užívání moderních telekomunikačních prostředků jako elektronické pošty, faxů nebo elektronické výměny dat (EDI). Tyto technologie se využívají zejména v provádění obchodních transakcí. Nicméně vzhledem k neexistenci právní regulace elektronických transakcí bylo rizikové tyto vymoženosti využívat, jelikož elektronicky podepsaný dokument nemusela druhá strana vůbec přijmout, a pokud by nastal soudní spor, neměl by takový dokument důkazní hodnotu. Taková situace komplikovala také přístup na mezinárodní trh, kde se elektronická komunikace využívala stále více.

Dalším důvodem bylo zajištění identifikace a autentizace podepisující osoby. Zatímco u tradičních dokumentů si lidé vystačili s vlastnoručním podpisem a připojením osobních údajů, u elektronických dokumentů je velice snadné provést digitalizaci písemného dokumentu (jako obrázku) a přitom přenést i podpis, který je na dokumentu učiněn. Komplikovanější situace nastává u dokumentů plně vytvořených počítačovou technikou, kde je ještě těžší poznat, kdo dokument podepsal.

Na začátku existovaly dvě možnosti právní úpravy. Buď vytvořit zvláštní zákon o elektronickém obchodu, nebo zakotvit elektronický podpis v právním řádu České republiky. Uvažovaný zákon o elektronickém obchodu by vznikl podle vzoru vytvořeného komisí OSN, který slouží jako inspirace pro národní legislativní orgány. Nicméně podle předkladatele by vyžadoval velké množství legislativních prací a také celou řadu v souvisejících zákonech. Proto byl upřednostněn návrh vytvořit zákon o elektronickém podpisu.

Hlavním principem nového zákona mělo být *„učinit dokumenty a podpisy na papíře a elektronické rovnoprávnými“*. To také souviselo s přáním předkladatelů, aby mohli občané vykonávat některé úřední úkony dálkovým způsobem. *„Přitom bude třeba brát v úvahu skutečnost, že k identifikaci a autentizaci se bude v budoucnosti nijak vzdálené používat i jiných prostředků, než je elektronický podpis.“*[1]

[1] Sněmovní tisk 415/0: Návrh zákona o elektronickém podpisu. *PSP* [online]. Praha: Poslanecká sněmovna Parlamentu České republiky, 1999 [cit. 2022-11-04]. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=3&CT=415&CT1=0

2.1.2 Proces vzniku a legislativní proces

Návrh zákona o elektronickém podpisu se začal připravovat v roce 1999 v tehdejším Úřadu pro státní informační systém (ÚSIS). Nicméně příprava právního předpisu nepostupovala příliš rychle a po nátlaku podnikatelské sféry se práce ujalo Sdružení pro informační společnost (SPIS), které připravilo finální návrh zákona pro poslance – předkladatele. Hlavním iniciátorem byl poslanec Vladimír Mlynář, dalšími spolupředkladateli byli Stanislav Gross, Ivan Langer a Cyril Svoboda.

První verze byla představena 23. 9. 1999. Jejím autorem byl doc. Vladimír Smejkal. Po zapracování připomínek vznikla druhá verze, která byla odeslána do Poslanecké sněmovny, a 26. 1. 2000 proběhlo první čtení. Mezi tím byla na základě dohody mezi ÚSIS a SPIS představena třetí verze, která původní návrh uvedla do souladu s *nařízením Evropského parlamentu a Rady o zásadách Společenství pro elektronické podpisy 1999/93/ES*, který byl taktéž předán do Parlamentu k projednání.

Mezi původní verzí a verzí ovlivněnou unijním právem byly ale veliké rozdíly, což způsobilo mnohé názorové střety při rozhodování zákonodárců, jakou cestou se vydat. Například se muselo rozhodnout, do jaké míry technicky konkrétní má zákon být. Evropská legislativa obsahovala přesné technologické specifikace, což ale čeští navrhovatelé nechtěli. Jeden z předkladatelů, poslanec Vladimír Mlynář, k tomu řekl toto: *„V případě, že přijdou nové techniky identifikace – identifikace lidí z DNA či očních duhovek – direktiva se jednoduše změní. Náš zákon ale nikoliv. Proto my navrhujeme zákon, který by nepočítal s ničím technicky konkrétním. Byl by přesně pro situaci v ČR a přesně by ho vymezil až Úřad pro elektronický podpis.“*

Další rozdíly existovaly v terminologii. „Unijní“ verze například používá termíny jako „podepisující osoba“ (resp. „podepsaná osoba“), „certifikát“ či „certifikační autorita“. Oproti tomu předchozí verze používaly ke stejnému účelu termíny „oprávněná osoba“, „osvědčení“ a „ověřovatel informací“. Největší rozkol lze spatřovat v ustanovení, komu elektronický podpis vlastně patří. Unijní pravidla stanovují, že podpis patří tomu, kdo vlastní speciální software k vytvoření podpisu. Česká verze se přiklání k názoru, že podpis je toho, kdo vyvolá akci vedoucí k podepsání dokumentu (např. stisk tlačítka na klávesnici).[2]

Nakonec se poslanci shodli na verzi, která je v souladu s nařízením Evropské unie, a tu poslali do druhého i třetího čtení. Závěrečné hlasování proběhlo 24. 5. 2000. Senát Parlamentu České

[2] PETERKA, Jiří. Česká cesta k elektronickému podpisu? *IT-NET*. Praha: Vogel Publishing, 2000, **1**(6), s. 28.

republiky návrh zákona schválil 29. 6. a prezident republiky přijatý zákon podepsal 12. 7., čímž byl legislativní proces dokončen. Dne 29. 7. 2000 byl zákon publikován ve Sbírce zákonů pod číslem 227/2000 Sb. a účinnost zákon nabyl 1. 10. 2000.

Během jeho platnosti prošel třemi novelami, v letech 2004, 2010 a 2012. Zákon o elektronických podpisech byl zrušen 19. 9. 2016.[3]

2.1.3 Hlavní principy a struktura zákona

Zákon o elektronickém podpisu stanovoval pojmy, postupy a subjekty, které jsou součástí procesu vytváření, používání a ověřování prostých i zaručených elektronických podpisů, jež mají řádně sloužit k verifikaci elektronických dokumentů.[4]

Právní předpis se v době přijetí dělil na devět částí, v nichž bylo celkem 28 paragrafů.

Nejdůležitější je první část. Jde o samotnou úpravu problematiky elektronických podpisů. Nejprve jsou definovány základní pojmy jako elektronický podpis a jeho druhy, rozdělení podepisujících osob, druhy poskytovatelů certifikačních služeb, druhy poskytovaných certifikátů a kategorie prostředků pro vytváření a ověřování elektronických podpisů. Dále zákon stanoví povinnosti všech aktérů procesu, určuje odpovědnost za škodu a také podmínky pro udělení akreditace k poskytování certifikačních služeb. Předpis také obsahuje formální náležitosti jednotlivých certifikátů a podmínky k uznávání zahraničních kvalifikovaných certifikátů. Závěr první části je věnován určení sankcí, které hrozí fyzickým či právnickým osobám za porušení zákona. Posledním paragrafem je zmocňovací ustanovení, které ministerstvu dává právo vydat prováděcí předpisy k některým částem zákona. Zbylých osm částí obsahuje změny dalších zákonů, které musely být v souladu se zákonem o elektronických podpisech, aby mohl být plně funkční. Musely se změnit například správní řád, občanský soudní řád nebo zákon o správě daní. Často to bylo kvůli přidání možnosti podávat elektronicky podepsaný dokument vedle tištěné podoby. Devátá část stanovuje účinnost, a to první den třetího kalendářního měsíce, který následuje po dni vyhlášení.[5]

[3] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).
[4] Sněmovní tisk 415/0: Návrh zákona o elektronickém podpisu. *PSP* [online]. Praha: Poslanecká sněmovna Parlamentu České republiky, 1999 [cit. 2022-11-04]. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=3&CT=415&CT1=0
[5] *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů,* s. 13–30.

2.1.4 Související právní předpisy

Jelikož některá zákonná ustanovení vyžadují zpřesnění či stanovení dalších podmínek, které se mohou v průběhu času měnit, vydaly některé státní orgány k zákonu prováděcí předpisy.

Níže jsou uvedeny dvě nejzásadnější normy:

- Jednou z prvních bylo *nařízení vlády č. 304/2001 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).* Předpis nařizuje orgánům veřejné moci povinnost zřídit si elektronickou podatelnu, pokud se jich týká povinnost přijímat podání učiněná v elektronické podobě, podepsaná elektronicky nebo ony samy mohou činit právní úkony elektronickým způsobem. Dále musí pověřit zaměstnance vytvářením a ověřováním zaručených elektronických podpisů, vybavit je k tomu potřebnými prostředky a kvalifikovaným certifikátem vydaným akreditovaným poskytovatelem certifikačních služeb.[6]
- Dalším podzákonným předpisem je *vyhláška č. 366/2001 Sb. Úřadu pro ochranu osobních údajů, o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu*. Úřad v ní stanovuje, jaké dokumenty musí předložit certifikační autorita, aby splnila své zákonné povinnosti. Firma musí předložit plán své certifikační politiky, bezpečnostní směrnici nebo plán pro zvládání krizových situací. *„Vyhláška také stanoví požadavky na bezpečnost informačního systému nebo požadavky na bezpečnost postupu při vydávání kvalifikovaných certifikátů a provozování seznamu kvalifikovaných certifikátů, které byly zneplatněny.“*[7]

Tyto právní normy byly vlivem novel zákona o elektronickém podpisu postupem času měněny a byly vydány i předpisy nové reagující na potřeby doby.

2.1.5 Novely zákona o elektronickém podpisu

Zákon o elektronickém podpisu byl celkem třikrát novelizován, v letech 2004, 2010 a 2012.

V roce 2004 Česká republika vstoupila do Evropské unie. Svázání s evropskou legislativou tak muselo být mnohem těsnější, než bylo doposud. Toto měla zařídit novela zákona

[6] *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů*, s. 41–42.
[7] Výroční zpráva 2001. *ÚOOU* [online]. Praha: Úřad pro ochranu osobních údajů, 2002 [cit. 2022-11-12]. Dostupné z: https://www.uoou.cz/files/vz_2001.pdf

č. 440/2004 Sb. Nově zavedla pojem „elektronické časové razítko“, jež mělo zajistit zjištění změny u e-dokumentů tak, že k nim přiřadilo aktuální časový údaj. Další nový pojem, „elektronická značka“, byla obdobou zaručeného elektronického podpisu, který mohou využívat právnické osoby i organizační složky státu. Tyto změny požadovala Evropská komise.

Novela č. 101/2010 Sb. reaguje na rozhodnutí Evropské komise 2009/767/ES a *„stanovuje povinnost vést seznam důvěryhodných certifikačních služeb a uznávat kvalifikované certifikáty vydané v jiných členských státech EU“*. Toto ale v praxi příliš nefungovalo.

Poslední změna je z roku 2012 a stanoví pojmy „uznávaný elektronický podpis“ a „uznávaná elektronická značka“. Tyto typy elektronického podpisu musí nově používat každý, kdo činí právní úkon elektronickým způsobem vůči orgánům veřejné správy.[8]

2.2 Elektronický podpis

2.2.1 Definice

Existují různé definice pojmu „elektronický podpis“ a často je představován poněkud jinak.

Například Česká terminologická databáze knihovnictví a informační vědy (TDKIV) elektronický podpis uvádí pouze jako ekvivalent jiného termínu, a to digitálního podpisu. Definice zní: *„Technologie, která představuje elektronickou analogii vlastnoručního podpisu na tištěném dokumentu. Digitální podpis využívá autorizace dat na základě asymetrického šifrování. Podepisující uživatel zašifruje informaci svým soukromým klíčem a příjemce ji dešifruje uživatelovým veřejným klíčem, jehož pravost potvrzuje digitální certifikát. Digitální podpis zajišťuje autenticitu, integritu, nepopiratelnost a ukotvení v čase.“*[9]

Digitální podpis je zde synonymem, nicméně Jiří Peterka, autor knihy Báječný svět elektronického podpisu, ho chápe jako nadstavbu elektronického podpisu, který je oproti němu založen na certifikátu a infrastruktuře veřejného klíče, je tedy bezpečnější.

[8] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).
[9] SKLENÁK, Vilém. Digitální podpis. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR, 2003 [cit. 2022-11-20]. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000000597&local_base=KTD

Jiří Peterka také nedefinuje elektronický podpis samotný, zabývá se až jeho druhy, jako jsou zaručený nebo uznávaný elektronický podpis. Podle něho je takový podpis „bez přívlastků“ slabý a má jen malou vypovídací hodnotu.[10]

Zákon o elektronickém podpisu říká, že *„elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“*. Tato definice je převzata z evropské směrnice 1999/93/ES.[11]

Všechny tyto definice se shodují na tom, že samotný elektronický podpis není příliš využitelný, nemá žádné požadavky na zabezpečení ani identifikaci dané osoby. Může mít podobu podpisu pod emailem nebo jména autora v záhlaví článku.[12]

Nicméně je to hlavní základní rámec pro jeho odvozené typy, které tyto uvedené požadavky splňují, a o nich pojednává následující podkapitola.

2.2.2 Vymezení základních pojmů

Aby bylo možné pochopit problematiku elektronických podpisů, je třeba znát základní pojmy uvedené v zákoně.

Zákon z roku 2000 znal dva typy elektronických podpisů, tedy **„prostý“ elektronický podpis**, který byl definován v předchozí podkapitole, a **zaručený elektronický podpis**, který je mnohem sofistikovanější. *„Je jednoznačně spojen s podepisující osobou, umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, byl vytvořen pomocí prostředků, které může osoba udržet pod svou výhradní kontrolou, a je připojen tak, že je možno zjistit jakoukoliv následnou změnu dat.“*[13]

Novela zákona z roku 2012 zavádí další verzi, a to **uznávaný elektronický podpis**. Kromě požadavků, které musí splňovat zaručený elektronický podpis, musí být tento založen na kvalifikovaném certifikátu, který je vydán akreditovaným poskytovatelem certifikačních služeb. Pokud chce někdo komunikovat s orgány veřejné moci, musí od roku 2012 používat právě tento typ.

[10] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8, s. 28.
[11] *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů*, s. 103.
[12] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8, s. 28.
[13] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

Pro fyzickou osobu, která držitelem prostředku pro vytváření elektronických podpisů a může ho používat, zákon užívá pojem **podepisující osoba.** Elektronický dokument, který je opatřen elektronickým podpisem, se nazývá **datová zpráva**. Jedná se o *„elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na technických nosičích dat, používaných při zpracování a přenosu dat elektronickou formou, jakož i data uložená na technických nosičích ve formě datového souboru“*.[14]

Novela z roku 2004 zavádí **elektronickou značku** a **časové razítko**, jež jsou založeny na stejné technologii jako elektronické podpisy. Elektronické značky mají podobnou funkci, ale nemusí je vytvářet jen fyzická osoba, nýbrž i právnická osoba nebo organizační složka státu. Značky generuje automatizovaný systém, a to i bez přímého vědomí a zásahu **označující osoby**. Značka musí být založena na systémovém certifikátu, který není vázán na konkrétní osobu.[15]

Časové razítko zaručuje, že uvedená data v elektronické podobě existovala v určitý časový okamžik v dané podobě. Může existovat vedle elektronického podpisu a využívá se jako jeho doplněk, není určeno k nahrazení. Je tedy zajištěna autenticita dokumentu a jakákoliv změna, která nastala po stvrzení razítkem, je zjistitelná. Stejně jako u podpisů jsou značky a časová razítka ve dvou verzích: „bez přívlastku“ a uznávaná.[16]

Aby bylo jasné, komu elektronický podpis, značka či razítko doopravdy patří, je jeho majitelem a má ho ve své výlučné moci, je třeba získat **certifikát**. Zákon ho definuje jako *„datovou zprávu, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost“*.[17] Certifikát je tedy potvrzením o tom, že určitý veřejný klíč (jenž je součástí certifikátu a který je používán k podpisu dokumentu) patří konkrétní osobě (její identita je popsána v certifikátu). Existují dva druhy certifikátů, komerční a kvalifikovaný. Komerční lze využít k šifrování, prokazování identity nebo k autentizaci. Mezi komerční certifikáty lze řadit emailový, kterým se podepisují emaily, nebo testovací, který slouží pro účely vývoje technologií. Neslouží ale ke komunikaci se státní správou, je tedy využitelný hlavně v soukromém sektoru. Zákon ho ani nijak nedefinuje.

[14] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).
[15] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8, s. 35.
[16] Tamtéž, s. 77.
[17] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

Kvalifikovaný certifikát musí na rozdíl od komerčního splňovat požadavky dané zákonem, je proto mnohem bezpečnější a má větší důvěryhodnost. Používá se hlavně k vytváření a ověřování uznávaných elektronických podpisů.[18] Obsahuje identifikační údaje fyzické či právnické osoby a údaje poskytovatele certifikátu, data pro ověření podpisu, jež odpovídají datům pro vytvoření podpisu, unikátní elektronickou značku poskytovatele a unikátní identifikační číslo certifikátu. Dále se musí určit začátek a konec platnosti certifikátu a rozsah použití, pro které je vydán. Může se vydávat také **kvalifikovaný systémový certifikát**, který je určen pro vytváření a ověřování elektronických značek.

Ten, kdo certifikáty vydává a vytváří je, se nazývá **poskytovatel certifikačních služeb,** laicky ho lze nazvat také jako certifikační autoritu. Pokud vydává kvalifikované certifikáty nebo kvalifikovaná časová razítka, jedná se o **kvalifikovaného poskytovatele certifikačních služeb.**

K vydávání kvalifikovaných produktů nicméně musí získat **akreditaci** od Ministerstva vnitra České republiky. V žádosti musí poskytovatel uvést své identifikační údaje, doložit oprávnění k výkonu podnikatelské činnosti a přiložit výpis z obchodního rejstříku. Musí prokázat věcné, personální a organizační předpoklady pro vydávání kvalifikovaných produktů. Žadatel také uvede, jaké služby bude chtít poskytovat. V případě udělení akreditace ministerstvo průběžně kontroluje plnění povinností, a pokud zjistí závažná porušení, akreditaci může odejmout. Mezi povinnosti patří například dodržování zákonných náležitostí kvalifikovaného certifikátu, dostatečné identifikování klienta před vydáním certifikátu, zajištění vydání seznamu platných i neplatných certifikátů nebo přijetí bezpečnostních opatření proti zneužití a padělání certifikátů. Musí také dodržovat zásady ochrany osobních údajů. V případě porušení povinností je také odpovědný za škodu, kterou způsobil, a to podle občanského zákoníku.

Závěrem je třeba zmínit **prostředky pro bezpečné vytváření a ověřování elektronických podpisů.** Podle zákona mají zajistit, že data pro vytváření e-podpisů mají být unikátní, nemohou se měnit a jejich utajení je náležitě zajištěno. Musejí také chránit podpis proti padělání a zneužití třetí osobou. K tomu poskytovatel využívá své programové a technické znalosti. Vydání těchto prostředků se má dít bezpečným postupem, který zaručí, že jsou vydávány oprávněným osobám.[19] Z právního předpisu vyplývá, že nemohou být čistě

[18] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8, s. 37.
[19] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

softwarovými prostředky, ale musejí to být hardwarová zařízení se zabudovaným firmwarem.[20]

2.2.3 Využití elektronického podpisu

Elektronický podpis jako právoplatná alternativa k vlastnoručnímu podpisu je široce využitelný jak v soukromém, tak i ve veřejném sektoru. Stát se snaží digitalizovat své procesy a usnadnit tak občanům vyřizování úředních záležitostí. Hlavním cílem by mělo být, aby vše bylo zpřístupněno „z pohodlí domova“. Elektronický podpis se proto může užívat hlavně k ověření identity občana a jako jistota integrity dokumentu, tedy že po podepsání nebyl měněn. Občan tak může podávat daňová přiznání, žádat o sociální dávky, přihlašovat se k nemocenskému pojištění, žádat o poskytnutí informace podle zákona č. 106/1999 Sb. a využívat ho i k dalším úkonům, pokud je to umožněno. To znamená, že co by se jindy řešilo osobní návštěvou nebo písemnou žádostí s úředně ověřeným podpisem, se dá realizovat elektronickou cestou. Lze jej také využít pro přihlášení do datové schránky.[21]

V soukromém sektoru jej lze využít k obchodním transakcím a k posílání veřejných listin.

2.2.4 Princip podepisování dokumentů

Pokud má být odeslána elektronicky podepsaná zpráva, je třeba ji nejdříve zašifrovat. Využívá se tzv. asymetrické kryptografie, kdy se pro šifrování a dešifrování používá klíč, respektive jeho dvě části, soukromá a veřejná. Ty jsou vždy spojené v páru, ale nelze z veřejného klíče vytvořit odpovídající soukromý klíč. Zabrání se tak zneužití elektronického podpisu.[22]

Z obsahu zprávy a konkrétního soukromého klíče se vypočítá autentizační kód, tzv. hash, který je mnohem kratší než samotná zpráva, ale jednoznačně vypovídá o jeho obsahu. Pokud se něco jakkoliv změní, změní se i hash. Je-li zpráva autentická, musí být hash na straně příjemce shodný s tím, který zaslal odesílateli.[23]

Soukromý klíč je třeba k vytvoření elektronického podpisu, takže je nutné, aby jedince jednoznačně identifikoval. Proto musí být zabezpečený, aby nedošlo k situaci, že se za jedince podepíše někdo jiný.[24]

---

[20] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8, s. 130.
[21] Elektronický podpis. *Jak na internet* [online]. CZ.NIC, 2023 [cit. 2023-01-15]. Dostupné z: https://www.jaknainternet.cz/page/1249/elektronicky-podpis/
[22] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8, s. 36.
[23] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-7169-479-7, s. 219.
[24] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8, s. 36.

Je-li podepsaný dokument odeslán, příjemce dostane odesílatelův veřejný klíč, který slouží k vyhodnocení platnosti elektronického podpisu a k ověření integrity zprávy. K tomu, aby si příjemce ověřil, že klíč patří skutečně odesílateli, se užívají certifikáty vydávané certifikačními autoritami.[25]

2.3 Nařízení eIDAS

2.3.1 Důvody vytvoření právního předpisu

Evropská komise tento návrh vytvořila v rámci dlouhodobé strategie s názvem Digitální agenda pro Evropu, která má za cíl odstranit stávající překážky digitálního rozvoje v Evropě. *Nařízením o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu* chtěla vytvořit právní rámec, který zabrání roztříštěnosti systémů elektronické identifikace, vybudovat mezi nimi interoperabilitu a zlepšit fungování elektronických služeb, které mohou využívat občané, podniky a orgány veřejné správy, ať už jsou z kteréhokoliv členského státu. Nařízení mělo také vytvořit ochranná opatření proti kyberkriminalitě.[26]

Zároveň byla tato opatření důležitá k uskutečnění jednotného digitálního trhu, který je jedním z výstupů Digitální agendy pro Evropu. Ten zahrnuje digitální marketing, elektronické obchodování a telekomunikace. Je základem evropské spolupráce podobně jako Evropský hospodářský prostor a umožňuje volné přeshraniční užívání elektronických produktů a vzájemnou komunikaci mezi fyzickými i právnickými osobami a státními orgány.[27]

Nařízení tak mělo posílit jistotu, že právní akt vytvořený v jednom státě bude mít stejnou platnost i ve druhém. Pokud se subjekt práva dostatečně identifikuje u kvalifikované důvěryhodné služby, která je vázána evropskými podmínkami, může obchodovat či se jinak smluvně vázat v kterémkoliv členském státě Evropské unie. Studenti se pak mohou bez problému hlásit na zahraniční univerzity, lidé mohou podávat daňová přiznání jinému státu nebo pacienti se mohou dostat ke zdravotní dokumentaci, pokud budou ošetřováni v zahraniční nemocnici. To vše mohou díky jednoznačné identifikaci, kterou zajistí

[25] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8, s. 37.
[26] Evropská unie. Dokument 52012PC0238: Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 4. 6. 2012 [cit. 2022-12-01]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:52012PC0238
[27] Jednotný digitální trh. *Jak na internet* [online]. CZ.NIC, 2019 [cit. 2022-12-01]. Dostupné z: https://www.jaknainternet.cz/page/3052/jednotny-digitalni-trh/

certifikační autorita, a díky procesu autentizace, který ověří, jestli daný subjekt může službu využít. Nařízení se tak mělo týkat všech druhů elektronických kontaktů.

Návrh vychází z čl. 114 Smlouvy o fungování Evropské unie, který vyzývá k přijímání pravidel, jež mají odstranit překážky ve fungování jednotného trhu. Jako nejvhodnější právní předpis Komise zvolila formu nařízení, které má přímý účinek ve vnitrostátním právu a státy si nemohou některá jeho ustanovení upravit, jak je tomu třeba u směrnice. Podle Komise tak bude zaručena právní jednotnost dohodnutých pravidel.

Komise musela prokázat, že návrh respektuje zásadu subsidiarity. Ta stanoví, že *„Evropská unie je oprávněna jednat jen tehdy, nelze-li daného cíle dosáhnout efektivněji na jiné, nižší, úrovni“*. To znamená, že unie nemůže rozhodovat ve věcech, které nejsou výlučně v její působnosti a které mohou upravovat mnohem efektivněji národní, regionální či místní orgány. Toto opatření má chránit kulturní rozmanitost Evropy a suverenitu členských států[28].

Podle Komise vnitrostátní úprava e-identifikace, autentizace a elektronických podpisů nestačí k plnění cílů strategie Digitální agendy pro Evropu, a naopak vytváří překážky pro interoperabilitu v Evropě. Státy si navzájem neuznávají prostředky pro elektronickou identifikaci, a je proto nutné stanovit společný rámec pro přeshraniční identifikaci. Dále Komise připomíná, že zatím nebylo dosaženo cílů na základě dobrovolné spolupráce členských států a nejspíš k tomu nedojde ani v budoucnu. Proto přistoupila k tomuto kroku.[29]

2.3.2 Legislativní proces

Před začátkem procesu probíhaly četné konzultace mezi Evropskou komisí, Evropským parlamentem, členskými státy a Evropským inspektorem ochrany údajů. Všichni účastníci mohli návrh připomínkovat a vytvářet zpětnou vazbu. Také probíhal internetový konzultační panel malých a středních podniků s cílem zjistit jejich názory a potřeby.

Evropská komise návrh schválila 4. 6. 2012 a tentýž den ho odeslala Evropskému parlamentu a Radě Evropské Unie. Návrh schválila Rada Evropské unie 20. 12. 2012 bez pozměňovacích návrhů. Evropský parlament návrh schválil 3. 4. 2014, nicméně navrhl několik změn, takže se návrh vrátil k projednání do Evropské komise. Ta tisk 9. 7. 2014 schválila i s navrženými

[28] SVÁROVSKÝ, Martin. Co je to subsidiarita? Módní zaklínadlo, nebo základ evropanství? In: *Forum 24* [online]. Praha: FORUM 24, 4. 2. 2021 [cit. 2022-12-01]. Dostupné z: https://www.forum24.cz/co-je-to-subsidiarita-modni-zaklinadlo-nebo-zaklad-evropanstvi/

[29] Evropská unie. Dokument 52012PC0238: Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu. In*: EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 4. 6. 2012 [cit. 2022-12-01]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:52012PC0238

změnami, tudíž mohlo být 28.8 nařízení uveřejněno v Úředním věstníku. Dne 17. 9. nastala jeho platnost.[30]

2.3.3 Hlavní principy a struktura nařízení

Nařízení se skládá z preambule, z šesti kapitol a čtyř příloh. Kapitoly se dělí na články, pouze třetí kapitola se dělí na 8 oddílů a až pak na články.

Preambule nejprve shrnuje důvody, proč byl tento právní předpis vydán a proč se přistoupilo k celounijnímu řešení. Připomíná usnesení evropských institucí, která Evropskou komisi dlouhodobě vyzývají k odstranění překážek na digitálním trhu. Vysvětluje hlavní principy, jako jsou nutnost uznávání elektronického identifikačního prostředku jiným členským státem, bezpečnost celého autentizačního procesu a nutnost udržovat vysokou úroveň důvěry pro elektronické prostředky. Dále uvádí, co má nařízení regulovat, jde například o fungování služeb vytvářejících důvěru (certifikačních autorit), pravidla dohledu nad dodržováním nařízení. Nové povinnosti se budou týkat pouze veřejného sektoru, soukromý sektor se může zapojit, pokud to bude pro něj výhodné. Nařízení by mělo být také co nejvíce technologicky neutrální, aby právo nebránilo inovacím a rozvoji digitálních technologií.

První kapitola obsahuje obecná ustanovení, vymezuje předmět a působnost zařízení, definuje pojmy uvedené v předpisu a stanoví zásady vnitřního trhu.

Druhá kapitola se věnuje elektronické identifikaci, a to tak, že zajišťuje vzájemné uznávání a přijímání prostředků pro elektronickou identifikaci za stanovených společných podmínek. *„Nařízení neukládá členským státům povinnost zavést nebo oznámit systémy elektronické identifikace, nýbrž uznávat a přijímat oznámené elektronické identifikace u těch internetových služeb, u nichž se k získání přístupu na vnitrostátní úrovni vyžaduje elektronická identifikace.“* Dále členský stát musí zajistit jednoznačné spojení mezi daty pro elektronickou identifikaci a dotčenou osobou. Kapitola také stanoví zásady pro autentizaci, tj. možnost ověřit platnost dat pro elektronickou identifikaci.

Třetí kapitola, respektive její první oddíl, obsahuje ustanovení o poskytovatelích důvěryhodných služeb, které poskytují fyzickým i právnickým osobám kvalifikované i nekvalifikované certifikáty, a stanovuje jim *„odpovědnost za škody způsobené nedbalostí*

[30] Evropská unie. Postup 2012/0146/COD: COM (2012) 238: Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 28. 8. 2014 [cit. 2022-12-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/HIS/?uri=celex:32014R0910&sortOrder=asc#421034

poskytovatele důvěryhodných služeb v důsledku nedodržení dobrých bezpečnostních postupů“.

Podle druhého oddílu musejí členské státy zřídit orgán dohledu, který dohlíží na dodržování bezpečnostních opatření. Kromě obecných si poskytovatelé musejí vytvořit vlastní technické a organizační bezpečnostní postupy. Jsou zde uvedeny také požadavky, které musejí splňovat kvalifikovaní poskytovatelé, aby byli za takové uznáni.

Třetí oddíl se věnuje elektronickým podpisům a stanoví požadavky na kvalifikované prostředky pro vytváření elektronického podpisu.

Čtvrtý oddíl se týká elektronických značek a pátý elektronických časových razítek, kde jsou obdobně ustanoveny požadavky na vytvoření a uznání.

Šestý oddíl se věnuje elektronickým dokumentům a stanovuje, že u *„elektronického dokumentu podepsaného kvalifikovaným elektronickým podpisem nebo opatřeného kvalifikovanou elektronickou značkou platí zvláštní právní domněnka ohledně jeho pravosti a integrity“.*

Sedmý oddíl se týká právního účinku dat odeslaných nebo obdržených prostřednictvím elektronického doručování. Osmý oddíl má zaručit pravost webových stránek, pokud jde o jejich vlastníka. K tomu se mohou užívat kvalifikované certifikáty speciálně určené k ověřování webových stránek.

Čtvrtá kapitola umožňuje, aby byl elektronický dokument užit jako důkaz v soudním nebo správním řízení. Nesmí mu být upírána právní platnost.

Pátá kapitola opravňuje Evropskou komisi, aby mohla vydávat prováděcí akty, které mohou doplňovat či zpřesňovat ustanovení uvedená v tomto nařízení, nesmějí ale změnit jejich význam.

Šestá kapitola nařizuje Komisi do 1. 7. 2020 podat zprávu o zhodnocení uplatňování tohoto nařízení a popřípadě navrhnout úpravy. Dále se zrušuje směrnice 1999/93/ES o elektronických podpisech. Přechodná ustanovení umožňují, aby prostředky vydané podle směrnice mohly být považovány za kvalifikované podle tohoto nařízení aspoň do konce jejich platnosti. Stejně se tak děje i u kvalifikovaných poskytovatelů, kteří musejí do 1. 7. 2017 podstoupit posouzení shody s novými pravidly. Do té doby jsou kvalifikovaní podle tohoto nařízení. Tato ustanovení zabraňují tomu, aby nový předpis působil retroaktivně. Poslední

článek stanovuje účinnost ode dne 1. 7. 2016, ovšem s několika výjimkami, které se stanou účinné až po schválení prováděcích aktů.[31]

2.3.4 Vymezení základních pojmů

Nařízení obsahuje speciální termíny, které jsou úplně nové, případně dosud neznámé, jelikož je původní zákon nedefinoval.

Proces **elektronické identifikace** je základní funkcí každého elektronického podpisu. Jedná se o *„postup užívání osobních identifikačních údajů v elektronické podobě, které jednoznačně identifikují fyzickou či právnickou osobu“*. Poté následuje proces **autentizace**, který potvrzuje elektronickou identifikaci fyzické či právnické osoby nebo také původ a integritu dat v digitální podobě.

K tomu všemu se využívá **kvalifikovaný elektronický podpis**, který má vlastnosti **zaručeného elektronického podpisu,** ale je vytvořen kvalifikovaným prostředkem pro vytváření podpisů a je založen na **kvalifikovaném certifikátu pro elektronické podpisy**. Ten na rozdíl od „obyčejného“ certifikátu musí být vydán kvalifikovaným poskytovatelem a musí splňovat požadavky tohoto nařízení. Měl by obsahovat jedinečné identifikační údaje poskytovatele a fyzické či právnické osoby, jež bude certifikát vlastnit. Dále například údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu, údaje o místu uložení, údaje o začátku a konci platnosti atd.

Zaručenému elektronickému podpisu postačí základní požadavky, tedy být jednoznačně spojen s podepisující osobou, musí umožnit její identifikaci a musí být připojen k dokumentu takovým způsobem, aby bylo možné zjistit následnou změnu dat. Může být založen na libovolném certifikátu. Osoba, která podpis použije, se nazývá **podepisující osoba.**

Dalším druhem elektronického podpisu je **elektronická pečeť**, která může být zaručená i kvalifikovaná. Pečeť obsahuje elektronická data, která se *„připojí k jiným datům s cílem zaručit jejich původ a integritu“*. Rozdíl je v tom, že pečeť může používat pouze právnická osoba či orgán veřejné správy. Požadavky na zaručenou i kvalifikovanou pečeť jsou obdobné jako u podpisu. Osoba, která pečeť použije, se nazývá **pečetící osoba**.

Elektronické časové razítko zaručuje, že elektronická data existovala v určitém okamžiku. Zároveň umožňuje detekovat změny, které se udály po času uvedeném v razítku, takže

[31] Evropská unie. Dokument 52012PC0238: Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 4. 6. 2012 [cit. 2022-12-01]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:52012PC0238

se zamezuje falšování dat. **Kvalifikované časové razítko** musí být dle nařízení použito spolu se zaručeným elektronickým podpisem nebo zaručenou elektronickou pečetí a musí být založeno na zdroji přesného času, který je spojen s „koordinovaným světovým časem“.

U všech těchto produktů platí, že nemohou být odmítnuty jako důkaz ve správním a soudním řízení. Pečeť ani časové razítko nemusejí dokonce splňovat požadavky na kvalifikovanou verzi, jen u nich pak neplatí domněnka původu a integrity elektronických dat.

Prostředky k elektronické identifikaci může vytvořit, ověřovat a uchovávat pouze **služba vytvářející důvěru**. Tu může provádět pouze **poskytovatel služeb vytvářející důvěru**. Poskytovatel, pokud chce vytvářet kvalifikované prostředky, musí být **kvalifikovaným** poskytovatelem. O tento status požádá orgán dohledu.

K vytvoření elektronického podpisu je zapotřebí speciální **prostředek**. Jde o konfigurované programové vybavení nebo technické zařízení.[32] Často se jedná o speciální software nebo čipovou kartu.

2.3.5 Prováděcí předpisy k nařízení eIDAS

Evropská komise může vydat prováděcí akt, pokud ji k tomu zmocní některé ustanovení v nařízení. Obvykle se to týká technických specifikací, které nemohou být kvůli možným změnám v technologiích upraveny v nařízení, neboť úpravy vyžadují zdlouhavý legislativní proces. Forma prováděcího aktu je mnohem rychlejší a akceschopnější.

Prováděcí akty se přijímají v souladu s čl. 47 nařízení. Pokud se prováděcí akt týká stanovení zvláštních kritérií pro posouzení shody kvalifikovaných prostředků s požadavky nařízení, mohl by akt zrušit Evropský parlament nebo Evropská rada. Taková námitka má být podána do 2 měsíců od zveřejnění normy.

Dosud bylo přijato 8 prováděcích aktů:

- *Prováděcí rozhodnutí Komise č. 2015/296, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace*

Věnuje se nastavením procesních pravidel mezi členskými státy v oblasti systémů elektronické identifikace. Podle čl. 3 je nařízeno členským státům určit jednotné kontaktní

[32] Evropská unie. 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. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 23. 7. 2014 [cit. 2022-12-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=CS

místo, které bude sloužit ke komunikaci s dalšími státy, aby se zajistilo hladké přeshraniční uznávání systémů a včasné řešení problémů. Jazykem pro komunikaci má být angličtina.

Dalším důležitým prvkem je proces vzájemného hodnocení, jenž je zmíněn v čl. 12 odst. 6 písm. c) nařízení a jehož účelem je přezkoumat interoperabilitu a bezpečnost systému elektronické identifikace.[33]

- *Prováděcí nařízení Komise č. 2015/806, kterým se stanoví specifikace týkající se podoby značky důvěry EU pro kvalifikované služby vytvářející důvěru*

Umožňuje poskytovatelům přidat ke svým službám speciální značku, aby si klient mohl ověřit, že se jedná o kvalifikovanou službu vytvářející důvěru. Evropská komise byla k tomuto aktu zmocněna na základě čl. 23 odst. 3 nařízení.[34]

- *Prováděcí nařízení Komise č. 2015/1501 o rámci interoperability*

Podle čl. 12 odst. 8 nařízení stanovuje technické a provozní požadavky na rámec interoperability tak, aby bylo zajištěno vzájemné propojení systémů. Propojení budou zajišťovat tzv. uzly, které budou součástí IT architektury. Mezi uzly jsou vyměňovány identifikační údaje osob a další data o identifikačním prostředku.

V příloze jsou popsány minimální soubory identifikačních údajů (atributů) pro fyzické a právnické osoby, které mají umožnit jednoznačnou identifikaci těchto osob.[35]

- *Prováděcí nařízení Komise č. 2015/1502, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci*

Podle čl. 8 odst. 3 nařízení se věnuje úrovním záruky (nižší, značné, vysoké) a konkretizuje požadavky na procesy spojené s vydáváním prostředků, dále požadavky na vlastnosti těchto

[33] Evropská unie. Přijaté prováděcí akty k nařízení eIDAS: 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. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/

[34] Evropská unie. Přijaté prováděcí akty k nařízení eIDAS: 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. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/

[35] Evropská unie. 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). In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-narizeni-komise-eu-2015-1501-ze-dne-8-zari-2015-o-ramci-interoperability-podle-cl-12-odst-8-narizeni-evropskeho-parlamentu-a-rady-eu/

prostředků, a to zejména s ohledem na autentizační faktory, mechanismus autentizace a další aspekty spojené s vydáváním a správou prostředků pro elektronickou identifikaci.[36]

- *Prováděcí rozhodnutí Komise č. 2015/1505, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů*

Podle čl. 22 odst. 5 nařízení popisuje podobu důvěryhodného seznamu, který musí povinně zveřejnit každý členský stát a který musí obsahovat informace týkající se kvalifikovaných poskytovatelů služeb vytvářejících důvěru spolu s informacemi o jimi poskytovaných službách.[37]

- *Prováděcí rozhodnutí Komise č. 2015/1506, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru*

Podle čl. 27 odst. 5 a čl. 37 odst. 5 nařízení popisuje, v jakém formátu musejí členské státy uznávat zaručené elektronické podpisy. Jedná se o formáty XML, CMS nebo PDF. Stát může uznat i jiný formát, pokud poskytovatel nabídne možnost ověření podpisu.

- *Prováděcí rozhodnutí Komise č. 2015/1984, kterým se stanoví okolnosti, formáty a postupy pro oznamování*

Podle čl. 9 odst. 5 nařízení, obsahuje postup, jakým má členský stát oznámit systém elektronické identifikace Evropské komisi. Musí poskytnout komplexní údaje o systému a také o zapojených subjektech, případně o orgánech dohledu, vydavateli identifikačních prostředků atd.[38]

[36] Evropská unie. Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-narizeni-komise-eu-2015-1502-ze-dne-8-zari-2015-kterym-se-stanovi-minimalni-technicke-specifikace-a-postupy/

[37] Evropská unie. Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-rozhodnuti-komise-eu-2015-1505-ze-dne-8-zari-2015-kterym-se-stanovi-technicke-specifikace-a-formaty-duveryhodnych-seznamu/

[38] Evropská unie. Prováděcí rozhodnutí Komise (EU) 2015/1984 ze dne 3. listopadu 2015, kterým se stanoví okolnosti, formáty a postupy pro oznamování. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-rozhodnuti-komise-eu-2015-1984-ze-dne-3-listopadu-2015-kterym-se-stanovi-okolnosti-formaty-a-postupy-pro-oznamovani/

- *Prováděcí rozhodnutí Komise č. 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí*

Podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení, popisuje kritéria, podle kterých se má posuzovat bezpečnost produktů jako USB tokenů nebo čipových karet, které slouží jako kvalifikovaný prostředek pro vytváření elektronických podpisů nebo pečetí.[39]

[39] Evropská unie. Prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2016 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-rozhodnuti-komise-eu-2016-650-ze-dne-25-dubna-2016-kterym-se-stanovi-normy-pro-posuzovani-bezpecnosti-kvalifikovanych-prostredku-pro-vytvareni-elektronickych-podpisu-a-peceti-podle-cl-3/

3. PRAKTICKÁ ČÁST

Tato část obsahuje kvalitativní šetření v oblasti elektronických podpisů, podrobnosti o průběhu implementace nařízení eIDAS v České republice a popis klíčových změn, které nová evropská úprava přináší.

3.1 Kvalitativní výzkum

3.1.1 Popis výzkumu

Pro tuto bakalářskou práci byla vybrána metoda kvalitativního výzkumu. V první části půjde o metodu dotazování. Dne 9. 3. 2023 byly certifikačním autoritám rozeslány otázky se zaměřením na samotné procesy elektronického podepisování a implementaci nařízení eIDAS. Jedná se tedy o minulost a současnost elektronického podpisu. Otázek bylo celkem 6. O zaslání odpovědí do 17. 3. 2023 byly požádány tři certifikační autority, tedy PostSignum, První certifikační autorita a eIdentity. Dne 13. 3. 2023 přišly odpovědi od pana Vojtěcha Vajse z eIdentity a. s. a pana Pavla Plachého z PostSignum. Dne 16. 3. 2023 poslal odpovědi pan David Hoření z První certifikační autority.

Druhá část výzkumu spočívá v porovnání legislativních dokumentů, konkrétně zákona č. 227/2000 Sb., o elektronickém podpisu, a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Zákon o elektronickém podpisu již z důvodu nařízení eIDAS neplatí, a proto byl vytvořen nový zákon, který tento evropský právní předpis implementuje. Tyto normy mají několik odlišností, ať už se to týká názvosloví, nebo zavedení nových služeb. Cílem práce je tyto odlišnosti představit.

3.1.2 Certifikační autority

V současnosti jsou u Digitální a informační agentury akreditováni 4 kvalifikovaní poskytovatelé služeb vytvářejících důvěru (také jako certifikační autority), kteří mohou působit na území České republiky a vydávat kvalifikované certifikáty pro vytváření elektronického podpisu. Jedná se o První certifikační autoritu a. s., Českou poštu, s. p., eIdentity a. s. a Správu základních registrů. Česká pošta si pro tyto účely zřídila certifikační autoritu PostSignum.

Kromě vytváření elektronického podpisu nabízejí také další služby dle nařízení eIDAS. Všechny poskytují vydávání kvalifikovaných certifikátů pro elektronické pečetě a elektronická časová razítka.

První certifikační autorita (ve zkratce I. CA) a Správa základních registrů nabízejí kvalifikovanou službu ověřování platnosti certifikátů. I. CA a PostSignum nabízejí další službu podle eIDAS, a to vydání kvalifikovaného certifikátu pro autentizaci internetových stránek. Službu elektronického doporučeného doručování nenabízí žádná autorita a službu uchování kvalifikovaných elektronických podpisů a pečetí poskytuje pouze firma Software602 a. s.[40]

3.1.3 Seznam otázek

1. V jaké struktuře evidujete údaje o certifikátech? Můžete poskytnout seznam atributů u certifikátu?
2. Které osobní údaje evidujete u klientů?
3. Došlo ke změně rozsahu sledovaných atributů po zavedení eIDAS?
4. Stoupl zájem o elektronické podpisy po zavedení eIDAS? Můžete poskytnout statistiky vydaných certifikátů vaší společností za jednotlivé roky?
5. Používaly se před zavedením eIDAS jiné typy prostředků pro vytváření elektronických podpisů než dnes (USB klíče, chipy, diskety atd.)?
6. Přinesla směrnice eIDAS posun v kvalitě služby z pohledu zjednodušení přístupu k certifikátům ze strany klientů?

3.1.4 Struktura zápisu atributů a evidované atributy

Například autorita PostSignum spravuje certifikáty v softwaru UniCERT od firmy CyberTrust. Jeho hlavní funkcí je automatická manipulace s digitálními certifikáty v návaznosti na požadavky klientů a zabezpečování elektronické komunikace.[41] Respektuje parametry infrastruktury PKI (Public Key Infrastructure), která zajišťuje distribuci veřejných klíčů tak, aby si mohl kdokoliv ověřit platnost elektronického podpisu[42]. Atributy čili údaje svých klientů eviduje v databázi Oracle od firmy Oracle Corporation. Ostatní autority používaný software nespecifikovaly.

---

[40] Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru. *MV ČR* [online]. Praha: Ministerstvo vnitra ČR, 19. 10. 2022 [cit. 2023-03-26]. Dostupné z: https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx

[41] Security Target for Cybertrust UniCERT 5: Common Criteria EAL4 Evaluation. *The Common Criteria Portal* [online]. 2006 [cit. 2023-03-30]. Dostupné z: https://www.commoncriteriaportal.org/files/epfiles/Cybertrust_UniCERT_5.2.1_ST.pdf

[42] SLAVÍK, Petr. Obecný úvod do Infrastruktury veřejných klíčů (PKI). *Infrastruktura veřejných klíčů: Public Key Infrastructure* [online]. 2009 [cit. 2023-03-30]. Dostupné z: http://pki.petrslavik.com/index.php?page=obecne

Atributy se používají pro strojové čtení certifikátu a pro lepší vyhledání jeho údajů. Například společnost Eidentity uvádí ve své certifikační politice následující strukturu:

- „Country“ = kód státu, kde má žadatel trvalý pobyt, např. „CZ“.
- „Organization“ = název organizace žadatele, pokud žadatel není v organizaci, kolonku vyplní poskytovatel certifikačních služeb.
- „Organizational Unit“ = organizační jednotka, kde žadatel pracuje, nepovinný atribut, např. „elektronická podatelna“.
- „Locality“ = adresa sídla organizace nebo bydliště, nepovinný atribut.
- „Name“ = celé jméno žadatele vč. titulů, nepovinný atribut.
- „Given name“ = křestní jméno.
- „Surname“ = příjmení.
- „Common name“ = Obsahem pole je celé jméno nebo pseudonym s označením „- PSEUDONYM“ uživatele.
- „Email Address“.
- „Pseudonym“ = vyplňuje se, pokud žadatel chce používat pseudonym.
- „Title“ = akademický titul či pracovní role.
- „Serial Number“ = Obsahuje údaj spravovaný ústředním orgánem státní správy, na jehož základě je možné osobu jednoznačně identifikovat, jde např. o číslo OP nebo cestovního pasu.

3.1.5 Změna rozsahu evidovaných atributů po zavedení eIDAS

U kvalifikovaných certifikátů se přidával atribut Qualified certificate statement, který potvrzuje, že daný certifikát byl vydán v Evropské unii a byl vydán jako kvalifikovaný. Nachází se zde také informace, k čemu lze certifikát použít, o době uchování registračních informací a také informace o prostředku pro vytváření elektronického podpisu.[43]

Byly provedeny i další změny (např. přidání samostatných položek pro jméno a příjmení, IČO se přesouvalo do samostatné položky atd.).

3.1.6 Zájem o elektronické podpisy po zavedení eIDAS

Certifikační autority se shodují, že počet vydaných certifikátů stoupá bez ohledu na implementaci nařízení eIDAS nebo postupnou digitalizaci. Velmi záleží na počtu agend,

[43] ETSI TS 101 862 V1. 3. 2: Qualified Certificate profile. *ETSI* [online]. Evropský ústav pro telekomunikační normy [cit. 2023-04-09]. Dostupné z: https://www.etsi.org/deliver/etsi_ts/101800_101899/101862/01.03.02_60/ts_101862v010302p.pdf

kde lze elektronický podpis použít. Přibyly také nové povinnosti vyplývající z legislativy, kdy pro některé úřední úkony se smí používat pouze uznávaný elektronický podpis. Je také možné, že publicita, které se eIDAS dostalo, byla hnacím motorem ke vzniku dalších digitalizovaných agend, a tedy i zájmu o certifikáty. Například ze statistiky poskytnuté autoritou PostSignum vyplývá, že po účinnosti nového zákona nedošlo ke skokovému zájmu o certifikáty, nárůst se navyšuje postupně každým rokem. Třeba v roce 2016 bylo vydáno 1 334 963 certifikátů, zatímco v roce 2020 to bylo již 2 372 403 certifikátů.

3.1.7 Historie typů prostředků pro vytváření elektronických podpisů

Certifikační autorita PostSignum uvádí, že se dříve používaly čipové karty a USB tokeny, ale nemusely mít povinnou certifikaci dle Common Criteria jako dnes. Common Criteria je *„společný rámec pro informační technologie, který zajišťuje vysoký bezpečnostní standard produktu. Takto certifikované prostředky mohou být používány bez dalšího přehodnocování“*.[44] Dříve se u autority používala certifikace FIPS, *„jež byla standardem státní správy v USA, který definoval minimální bezpečnostní požadavky v produktech informačních technologií“*.[45] Nově se také musí zapisovat atributy, jestli je certifikát generován na čipové kartě nebo tokenu.

3.1.8 Názory na nařízení eIDAS

Ohlasy na zavedení eIDAS jsou smíšené, autority zmiňují výhody, ale i komplikace.

Například I. CA nařízení uvítala, před tím byly na úrovni EU legislativně upraveny pouze služby vydávání kvalifikovaných certifikátů, eIDAS zásadním způsobem spektrum služeb rozšířil. Nově je umožněno přeshraniční uznávání kvalifikovaných služeb např. časových razítek a elektronických pečetí. Drobnou komplikací byl přechod od českých elektronických značek k evropským elektronickým pečetím, které nebyly zcela totožné, např. pečetit může pouze původce dokumentu.

PostSignum kvituje posílení bezpečnosti, které je ale na úkor uživatelského komfortu. Zjednodušení lze vnímat pouze při využití elektronické identity pro získání certifikátu online bez nutnosti osobní návštěvy.

eIdentity si nemyslí, že by nová právní úprava přinesla zlepšení.

[44] About The Common Criteria. *The Common Criteria Portal* [online]. [cit. 2023-04-01]. Dostupné z: https://www.commoncriteriaportal.org/ccra/index.cfm

[45] Dodržování předpisů standardu FIPS (Federal Information Processing Standard) pro .NET Core. *Microsoft* [online]. Microsoft, 28. 11. 2022 [cit. 2023-04-01]. Dostupné z: https://learn.microsoft.com/cs-cz/dotnet/standard/security/fips-compliance

3.2 Průběh implementace nařízení eIDAS

3.2.1 Činnost pracovní skupiny Ministerstva vnitra

Odpovědnost za provedení nařízení eIDAS mělo Ministerstvo vnitra České republiky. K tomuto účelu ustanovilo Řídicí výbor pro nařízení eIDAS, a to pokynem ministra vnitra č. 55/2015 ze dne 7. října 2015. Měl tvořit koordinační a komunikační platformu, kde úředníci ministerstva a další účastníci získají potřebné vstupy a informace, které využijí při své rozhodovací činnosti.[46] Samotný výbor je tedy pouze poradním orgánem.

V rámci výborů působilo 6 pracovních podskupin, z nichž každá z nich se věnovala jednotlivým službám a dalším legislativním opatřením, které eIDAS přináší. Hned první skupina se věnovala elektronickým podpisům a pečetím, časovým razítkům a autentizaci webu. Další z nich se zabývaly např. elektronickým doporučeným doručováním, elektronickou identitou nebo rozvojem přeshraniční spolupráce.

Během práce se členové účastnili také odborných porad v orgánech Evropské komise jako eIDAS Working Group nebo Cooperation Network. Výbor také sledoval počínání jiných států EU při implementaci eIDAS.[47]

Výbor vypracoval návrh zákona o službách vytvářejících důvěru pro elektronické transakce, který, pokud by byl přijat, počítal s přechodným obdobím, aby se veřejná správa, podniky i fyzické osoby mohly na nová pravidla připravit. *„Nicméně nařízení eIDAS začalo platit již od 1. 7. 2016, tedy ještě před předpokládaným začátkem účinnosti nového zákona. Od té doby byl dokument podepsaný elektronickým kvalifikovaným podpisem roven vlastnoručně podepsanému dokumentu a žádný orgán veřejné moci ho nesměl odmítnout. eIDAS také dal časový prostor certifikačním autoritám, aby se akreditovaly podle nové právní úpravy, a 1 rok měly tedy dočasný status kvalifikovaného poskytovatele služeb vytvářejících důvěru, aby nemusely svoji činnost ukončit. Pokud by se do 1. 7. 2017 neakreditovaly, dočasný status by ztratily.*

Od 1. 7. 2016 také začala platit povinnost odpovědnosti za škodu způsobenou členskými státy a poskytovateli služeb vytvářejících důvěru. Sankcionovalo se porušení pravidel služeb či jejich nedostupnost.

---

[46] TRETERA, Jan. Poskytnutí informace dle zákona č. 106/1999 Sb. In: *MV ČR* [online]. Praha: odbor eGovernmentu MV ČR, 2. 10. 2020 [cit. 2023-04-10]. Dostupné z: https://www.mvcr.cz/soubor/mv-105227-10-eg-2020.aspx

[47] PIFFL, Robert. eIDAS… aneb co nám přináší nařízení EU č. 910/2014 ze dne 23. 7. 2014. In: *Egovernment* [online]. Praha: Ministerstvo vnitra ČR, září 2015 [cit. 2023-04-09]. Dostupné z: https://www.egovernment.cz/soubor/eidas-aktualni-situace-robert-piffl/

Zákon o službách vytvářejících důvěru pro elektronické transakce nabyl účinnosti až 19. 9. 2016. Poskytl taktéž přechodné období, kdy se mohly používat kvalifikované elektronické podpisy a elektronické značky podle staré právní úpravy. Měly tedy omezenou dobu stejnou platnost jako nová elektronická pečeť nebo kvalifikovaný elektronický podpis podle nařízení eIDAS. Plná účinnost nastala 28. 9. 2018.“[48]

3.2.2 Studie o dopadu nařízení eIDAS na certifikační autoritu PostSignum

Analýza je uvedena v případě společnosti PostSignum, která poskytla zprávu o průběhu implementace eIDAS ve firmě. PostSignum je jedna z certifikačních autorit působících na území České republiky. Jejím provozovatelem je státní podnik Česká pošta. Poskytuje především komerční a kvalifikované certifikáty a časová razítka. Vedle toho nabízí i doplňkové služby a produkty například bezpečné uložení soukromých klíčů nebo SW produkty pro archivaci elektronických dokumentů.

PostSignum musela v roce 2016 reagovat na zavedení nařízení eIDAS a následně na český zákon č. 297/2016 Sb., *o službách vytvářejících důvěru pro elektronické transakce*, který evropský předpis implementoval do českého právního řádu.

Certifikační autoritě byl na přechodnou dobu jeden rok udělen status kvalifikovaného poskytovatele služeb vytvářejících důvěru pro poskytování kvalifikovaných certifikátů pro elektronický podpis. Pokud by se do konce lhůty, tedy do 1. 7. 2017, nepřizpůsobila novým legislativním požadavkům, tento status by ztratila.[49]

Ve společnosti se tedy museli připravit na komplexní audit od certifikovaného subjektu posuzujícího shodu. Auditní zpráva je následně předložena orgánu dohledu nad kvalifikovanými poskytovateli služeb, který poskytovatele a jeho kvalifikované služby zveřejní na důvěryhodných seznamech, jež jsou z hlediska uznávání závazné pro celou EU.

Do té doby mohla společnost poskytovat jako kvalifikované produkty pouze prostředky pro vytváření elektronických podpisů i pečetí a certifikáty pro elektronické podpisy. Změny se týkaly také oblasti služeb.

Aby společnost PostSignum mohla přizpůsobit své služby novým podmínkám, musela provést analýzu, aby se mohla včas připravit.

---

[48] PIFFL, Robert a Ondřej FELIX. Nařízení eIDAS – Cíle, nástroje, důsledky. Metodický seminář – Dopady nařízení eIDAS po 1. 7. 2016. In: *MV ČR* [online]. Praha: Ministerstvo vnitra ČR, 2017 [cit. 2023-04-09]. Dostupné z: https://www.mvcr.cz/soubor/1-eidas-narizeni-eidas-cile-nastroje-dusledky.aspx

[49] Výroční zpráva 2016. *Česká pošta* [online]. Praha, 2017 [cit. 2023-02-08]. Dostupné z: https://www.ceskaposta.cz/documents/10180/4349406/VZ-CP-2016.pdf/db8a57aa-f2b8-4bda-be97-4741634a1b07

V případě prostředků pro vytváření elektronických podpisů a pečetí se doposud užívaly USB tokeny a čipové karty různých typů, které ale neměly certifikaci dle eIDAS. Proto byl na jaře roku 2016 registrován USB token s obchodním názvem TokenME. Prostředek je povinný pro zaměstnance veřejné správy a pro ty, kteří užívají služby v přeshraničním styku. Namísto pošt bude nyní distribuován prostřednictvím e-shopu PostShop.

PostSignum nabízí dvě varianty kvalifikovaných certifikátů pro elektronické prostředky: s prostředkem pro vytváření e-podpisů a bez něho. Tato varianta je vhodná pro zaměstnance veřejného sektoru, kteří kvůli nařízení tyto prostředky musejí začít používat povinně, a dále pro ty, kteří budou e-podpis využívat přeshraničně. PostSignum se muselo připravit na výběrová řízení veřejných institucí, jež poptávají tyto služby. Revizí prošly také služby klientské a externí registrační autority, aby bylo možné tyto služby bezproblémově provozovat i v budoucnu.

Kvalifikované certifikáty bez prostředků jsou vhodné pro fyzické i právnické osoby, které e-podpis budou uplatňovat v rámci ČR. Zde se neplánovaly žádné změny v poskytování.

Zcela novou službou jsou kvalifikované certifikáty pro elektronické pečetě, které nahrazují dřívější elektronické značky. Začaly se prodávat až po vydání nového zákona jako nekvalifikované produkty, po úspěšném posouzení shody s nařízením jako kvalifikované. Prodávají se s prostředkem i bez prostředku. Totožný postup byl stanoven i pro elektronická časová razítka.

PostSignum začalo také provozovat službu ověřování kvalifikovaných podpisů a pečetí, která je určena hlavně pro veřejnoprávní subjekty. Mohou to sice dělat svépomocí, ale vybudování vlastního systému ověřování je finančně a časově náročné. Vzhledem k očekávanému růstu elektronických podání se předpokládalo, že bude o tuto službu zájem.

Další novou službou, kterou zavedlo nařízení eIDAS, je uchování kvalifikovaných certifikátů a pečetí. Česká pošta má elektronickou archivaci pouze pro své interní potřeby, nicméně v analýze byl zmiňován projekt „Bezpečné úložiště dokumentů“, který by se v budoucnu mohl stát základem této služby. Byla by nabízena jako komerční služba, v případě zájmu by se nabízela jako kvalifikovaná.

Poslední službou dle eIDAS by mělo být elektronické doporučené doručování dokumentů. Podle analýzy to spadá do oblasti datových schránek, což není v působnosti PostSignum, musel by být vytvořen obdobný systém na komerční bázi.[50]

3.2.3 Studie o průběhu implementace ve vybraných městských částech a na Magistrátu hlavního města Prahy

Tato studie zjišťuje, jak jsou povinnosti stanovené nařízením Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu prováděny a dodržovány v České republice, konkrétně ve čtyřech pražských městských částech (Praha 1, Praha 2, Praha 4 a Praha 11) a na Magistrátu hlavního města Prahy. Pomocí dotazníku autoři zjišťují, jak jsou nové povinnosti pro respondenty časově a finančně náročné nebo jaký mají na ně subjektivní názor. Studie závěrem získaná data analyzuje a vyhodnocuje.

Autoři na úvod shrnují důvody, které vedly Evropskou unii k zavedení eIDAS. Standardizovaný elektronický podpis povede k větší interoperabilitě mezi členskými státy, které budou nuceny používat jednotnou infrastrukturu. Zesílí se transparentnost a důvěryhodnost elektronické komunikace, to by mělo vést k větší kooperaci a spolupráci veřejného a soukromého sektoru. Pro občana a podniky to tak znamená dostupnější různé služby v celé EU a lepší komunikaci se státními orgány. Členské státy EU proto musejí vytvořit a podílet se na společném rámci pro tuto elektronickou komunikaci, která uznává, kontroluje a ověřuje eID z různých členských států EU.

Česká republika následně přijala zákon č. 297/2016 Sb., *o službách vytvářejících důvěru pro elektronické transakce,* který nařízení implementoval do českého právního řádu. Autoři zmiňují, že je mnohem přísnější než samotný právní předpis EU. Zákon rozlišuje různé typy podepisujících osob a příjemců a nařizuje, aby orgány veřejného sektoru jednající prostřednictvím elektronických dokumentů musely používat kvalifikovaný elektronický podpis, tedy elektronický podpis založený na kvalifikovaném certifikátu. K dokumentu musejí připojit ještě kvalifikované časové razítko.

Veřejná správa musí mít tedy potřebné technické vybavení a také pověřenou osobu, která má u sebe tzv. bezpečnostní klíč (token, čipovou kartu) s kvalifikovanou pečetí. Bez něho není možné podepisovat oficiální dokumenty za obec. Autoři se v dotazníku ptali zástupců pražských obecních úřadů, jaké používají bezpečnostní prostředky, kolik peněz je stálo

[50] *Dopady nařízení eIDAS na poskytované služby certifikační autority PostSignum: analýza*. Praha, 2016. Interní dokument.

technické vybavení, kolik mají pověřených osob k podepisování a jak ověřují platnost certifikátů. Největší náklady z dotazovaných úřadů má Magistrát hl. m. Prahy, který se také stará o nejvíce občanů. Na zajištění infrastruktury bylo vynaloženo 323 tisíc korun. U ostatních jde o řádově menší částky, Praha 2 a Praha 1 zaplatily kolem 90 tisíc korun, Praha 11 dvě stě tisíc korun a Praha 4 nejméně, a to 11 tisíc korun. Pověřených osob k podepisování měl opět nejvíce magistrát, a to 542 zaměstnanců, další části uvedly kolem 100 lidí. Nejméně měla Praha 11, a to pouhých 25 pracovníků. Tyto údaje jsou platné k roku 2018.

Úřady mají nejčastěji jako bezpečnostní prostředky čipové karty nebo USB tokeny od různých firem. K ověření platnosti certifikátů používají nejčastěji weby certifikačních autorit, které tyto seznamy zveřejňují.

Autoři konstatují, že oslovené úřady si svoje povinnosti uvědomují, snaží se k nim přistupovat efektivně a s péčí řádného hospodáře. Vědí, že si musejí zajistit kvalitní kvalifikovaný podpis a že by neměly plýtvat. Nicméně nedělají nic, co je nad rámec povinností, a to například informační činnost pro veřejnost, technickou podporu nebo další vzdělávání, protože očekávají vytvoření projektu od Magistrátu hl. m. Prahy, který by měl tyto činnosti integrovat pod jeden úřad a řídit centrálně.[51]

3.3 Klíčové změny

Níže jsou představeny největší změny, které byly nově legislativně zavedeny.

Změny:

- Nařízení zesílilo spolupráci v Evropské unii. Členské státy spolu mohou díky zavedení kontaktních míst lépe komunikovat ohledně systémů elektronické identifikace, vzájemně si je hodnotit, vyměňovat si zkušenosti a koordinovat opatření při poruše systému. Evropská komise určila jednotná technická pravidla, aby bylo možné vzájemné propojení systémů, tudíž státy nemusejí vymýšlet vlastní pravidla.
- Byl zaveden systém elektronické identifikace, která umožňuje ztotožnění fyzické i právnické osoby v online prostoru. Díky tomu jsou na vzestupu elektronické služby soukromých subjektů i orgánů veřejné správy. Osoba se tak nemusí osobně dostavit na určité místo kvůli vyřízení svých záležitostí.
- Výše sankcí se zvýšila.

[51] MACGREGOR PELIKÁNOVÁ, Radka, Eva Daniela CVIK a Robert MACGREGOR. Qualified Electronic Signature – eIDAS Striking Czech Public Sector Bodies. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis* [online]. 2019, **67**(6), 1551–1560 [cit. 2023-06-28]. ISSN 1211-8516. Dostupné z: doi:10.11118/actaun201967061551

Stávající pravidla:

- Pravomoc dohledu i udělování sankcí zůstává na Digitální a informační agentuře, která má také na starost provoz systému na svém území. Evropská komise plní pouze roli prostředníka mezi členskými státy, spravuje seznam důvěryhodných prostředků a stanovuje technologické rámce pro služby vytvářející důvěru.
- Pro uživatele kvalifikovaných služeb se nic nemění. Je na nich, jestli nové funkce využijí nebo ne.
- Výše sankcí se pro právnické osoby snížila z 10 000 000 Kč na nejvýše 2 000 000 Kč. Sankce pro fyzické osoby se naopak zvýšila z 250 000 Kč na 2 000 000 Kč.

Nové pojmy:

- Byly zavedeny nové pojmy „služby vytvářející důvěru“ a „poskytovatel služeb vytvářejících důvěru“. Služba „elektronická značka“ změnila svůj název na „elektronická pečeť“.

3.3.1 Vzájemné uznávání

Každý elektronický identifikační prostředek (jako např. kvalifikovaný certifikát), který je vydaný v jedné členské zemi Evropské unie, musí být podle čl. 6 uznán i ve všech dalších. To platí ale pouze v případě, že daný prostředek odpovídá požadavkům nařízení eIDAS, byl oznámen Evropské komisi a zveřejněn ve veřejně přístupném seznamu.

Zákon o elektronickém podpisu byl v souladu s tehdejším právem Evropského společenství, proto § 16 ukládal povinnost uznávat i zahraniční kvalifikované certifikáty, pokud byly vydány na území Evropského hospodářského prostoru nebo ve Švýcarské konfederaci. Podmínkou je, aby byl takový certifikát akreditován v některém členském státu, jenž by převzal odpovědnost za správnost a platnost kvalifikovaného certifikátu. Česká republika mohla uznat i certifikát vydaný v jiném státě, pokud to vyplývalo z mezinárodní smlouvy.[52]

Nařízení eIDAS tedy nastavuje pravidla celoevropské spolupráce a více ji upevňuje díky jednotné koordinaci ze strany Evropské komise a společným technickým specifikacím. Zároveň je systém díky veřejně přístupným seznamům certifikačních prostředků mnohem transparentnější.

[52] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

3.3.2 Elektronická identifikace

Kapitola III., čl. 3, odst. 1 nařízení definuje elektronickou identifikaci jako *„postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu“*. Předpis dále obsahuje také čl. 8, který stanovuje úrovně záruky, jež rozlišují systémy elektronické identifikace podle míry zabezpečení a spolehlivosti. Systém kvalifikovaného poskytovatele může mít úroveň nízkou, značnou a vysokou. Každá úroveň má také své speciální postupy, jakými jsou metody ověřování totožnosti fyzických či právnických osob nebo mechanismus autentizace.[53]

Před nařízením eIDAS nebyla elektronická identifikace v ČR obecně právně upravena. Až 1. července 2018 nabyl účinnost zákon o elektronické identifikaci č. 250/2017 Sb., který implementoval evropskou právní úpravu elektronické identifikace.[54] Zákon o elektronickém podpisu také explicitně nerozlišoval úrovně záruky identifikačních prostředků podle míry bezpečnosti. Obecně by se dalo říci, že kvalifikované certifikáty jsou spolehlivější než nekvalifikované, jelikož musejí splnit zákonné požadavky.[55]

Elektronická identifikace se v České republice využívá zejména pro online komunikaci s orgány veřejné správy, se kterými lze vyřešit řadu životních situací online. Každým rokem roste počet uživatelů, k roku 2022 je od spuštění služby evidováno 33 milionů přihlášení. Nejvyužívanějšími službami v roce 2022 byly datové schránky, portál pomoci ukrajinským uprchlíkům a ePortál ČSSZ.[56]

3.3.3 Oznámení

Dle čl. 21 nařízení je vydavatel povinen oznámit všechny aspekty identifikačního prostředku jako úroveň záruky, systém ochrany osobních údajů nebo údaje o odpovědnosti za prostředek. Spolu s oznámením o úmyslu poskytovat služby vytvářející důvěru musí poskytovatel orgánu dohledu předložit ještě zprávu o posouzení shody. Pokud je jeho žádost schválena, udělí

[53] Evropská unie. 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. In: EUR-Lex: Úřední věstník Evropské unie [online]. Úřad pro publikace EU, 23. 7. 2014 [cit. 2022-12-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=CS

[54] ŠPETA, Sebastian. *Elektronická identifikace* [online]. Brno, 2019 [cit. 2023-05-09]. Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Radim Polčák. Dostupné z: https://is.muni.cz/th/yrpa5/

[55] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

[56] Identita občana v roce 2022: souhrnné vybrané statistiky. *NAKIT* [online]. Národní agentura pro komunikační a informační technologie, 21. 2. 2023 [cit. 2023-05-09]. Dostupné z: https://nakit.cz/identita-obcana-v-roce-2022-souhrnne-vybrane-statistiky/

orgán dohledu status kvalifikovaného poskytovatele a zašle oznámení Evropské komisi. Poskytovatel je pak zapsán do Seznamu kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru.

V případě narušení bezpečnosti nebo funkčnosti se ihned musejí informovat ostatní zapojené státy a Evropská komise. Také je nutné pozastavit proces přeshraniční autentizace a vypojení rizikových částí systému. Udílení sankcí za tyto skutky je věcí národního orgánu dohledu.[57]

Zákon o elektronickém podpisu také ukládal oznamovací povinnost poskytovatelům certifikačních služeb při zahájení poskytování služeb, ale rozlišoval, zda jsou akreditovaní či neakreditovaní. Neakreditovaný poskytovatel musel podle § 6 odst. 2 oznámit ministerstvu úmysl poskytovat kvalifikované certifikační služby nejméně 30 dní před zahájením a k návrhu musel přiložit k ověření kvalifikovaný systémový certifikát. Akreditovaný poskytovatel tento krok činit nemusel, jelikož tato fáze byla provedena současně s žádostí o akreditaci. Ta se řídila podle § 10. Musel ale tento krok udělat znovu, pokud chtěl rozšířit své služby o další kvalifikované produkty, a to aspoň 4 měsíce před zahájením. Musel také doložit věcné, personální a organizační předpoklady pro zajištění těchto služeb.

Členské státy již měly povinnost zveřejňovat a udržovat seznamy důvěryhodných služeb na základě rozhodnutí Komise č. 2009/767/ES. Seznamy ale v tomto případě musely povinně obsahovat pouze údaje o poskytovatelích certifikačních služeb, kteří vydávají kvalifikované certifikáty pro veřejnost v daném státu a kteří jsou zároveň akreditováni Ministerstvem vnitra. Důvěryhodné seznamy podle nařízení eIDAS nicméně musejí povinně obsahovat informace nejen o kvalifikovaných poskytovatelích služeb vytvářejících důvěru vydávajících kvalifikované certifikáty, ale i o ostatních kvalifikovaných poskytovatelích poskytujících kvalifikovanou službu vytvářející důvěru (například vydávání kvalifikovaných elektronických časových razítek).

Zákon o elektronickém podpisu přesně nespecifikoval, jak má poskytovatel oznámit ohrožení bezpečnosti vlastních produktů a riziko jejich zneužití. Nicméně platí, že zákon (v § 6 odst. 1 písmen c) a d)) předepisoval poskytovatelům povinnost zachovávat bezpečnost svých produktů jako ochranu dat, zajištění jednoznačnosti dat a provést opatření proti padělání certifikátů. Pokud ministerstvo zjistilo porušení zákona, mohlo poskytovatele pokutovat nebo

[57] Evropská unie. 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. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 23. 7. 2014 [cit. 2022-12-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=CS

mu kvalifikované certifikáty zneplatnit. U akreditovaného poskytovatele mu ještě mohlo odebrat akreditaci.[58]

3.3.4 Odpovědnost

V preambuli nařízení se v odstavci 18 uvádí, že *„by měla být stanovena odpovědnost členského státu, poskytovatele služeb vytvářejících důvěru a strany provozující autentizaci za nedodržení povinností a způsobení případné škody. Nicméně by však mělo být uplatňováno v souladu s vnitrostátními pravidly odpovědnosti.“* To znamená, že Evropská komise či jiný orgán EU nemůže sankce vymáhat.

Podrobněji se otázce odpovědnosti věnuje kapitola III. oddíl 1. čl. 13. Poskytovatel zodpovídá za nedbalostní i úmyslnou škodu, ale pokud zákazník služby poruší smluvní pravidla či jiná omezení, je odpovědný on. U nekvalifikovaného poskytovatele nese důkazní břemeno zákazník, který uplatňuje nárok na náhradu škody, kvalifikovaný poskytovatel musí naopak prokázat, že škoda nastala bez jeho úmyslu či nedbalosti.

Nařízení výslovně nestanovuje výši sankce, ale musí být účinné, přiměřené a odrazující.[59]

Až prováděcí zákon č. 297/2016 Sb., konkrétně § 16 a 17, specifikuje přestupky, za které je možné udělit sankci pro právnické osoby do výše 500 000 Kč, 1 000 000 Kč nebo do 2 000 000 Kč. Výše sankce se odvíjí od toho, o jaký přestupek se jedná, což je taxativně uvedené v zákoně. Pokutuje se například nepodrobení se posouzení shody, neplnění informační povinnosti nebo nedostatečné ztotožnění fyzických osob. Fyzické osobě může být udělena pokuta do výše 2 000 000 Kč, a to pouze u přestupku použití značky EU v rozporu s nařízením.[60]

Zákon o elektronickém podpisu v § 18 a v § 18a stanovil výši sankce až do 10 000 000 Kč u právnických osob nebo u fyzických osob do výše 250 000 Kč.[61] Na rozdíl od prováděcího zákona tedy nebyla zavedena spodní hranice pokuty. Oba právní předpisy ponechávají uvážení a rozhodnutí o výši pokuty na správním orgánu, a to podle míry provinění.

---

[58] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

[59] Evropská unie. 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. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 23. 7. 2014 [cit. 2022-12-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=CS

[60] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (znění od 1. 4. 2023).

[61] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

Zákon oproti nařízení eIDAS neupravoval důkazní břemeno, tedy kdo musí způsobenou škodu prokázat. Původní právní úprava ale obsahovala například ustanovení v § 19, že poskytovatel nemusí být za škodu odpovědný, pokud dokáže, že vyvinul veškeré úsilí, aby ke škodě nedošlo. Také ve stejném paragrafu lépe konkretizovala, jak má správní orgán rozhodnout. Muselo se přihlédnout k závažnosti deliktu, ke způsobu jeho provedení, k jeho následkům a okolnostem provedení. Prováděcí zákon pouze stanoví povinnosti a přestupky za jejich porušení.

3.3.5 Spolupráce a operabilita mezi zeměmi EU

Oznámené vnitrostátní systémy jsou podle čl. 12 nařízení interoperabilní, tudíž musejí existovat standardizované technologické specifikace pro všechny členské státy. Není tak upřednostňován žádný vnitrostátní systém, vše řeší evropské nebo mezinárodní právo. Rámec je také technologicky neutrální a vedle technických specifikací řeší otázku provozní bezpečnosti a ochrany osobních údajů. Obsahuje také minimální soubor identifikačních údajů, které slouží ke ztotožnění osob.

Spolupráce mezi členskými státy podle odstavce 20 preambule slouží *k „usnadnění technické interoperability a zájmu podpory vysoké úrovně důvěryhodnosti a bezpečnosti odpovídající míře rizika“*. Důležitá je výměna informací a sdílení zkušeností a osvědčených postupů.[62]

Zákon o elektronickém podpisu tehdy nepředpokládal spolupráci mezi evropskými státy, stanovoval pouze povinnost uznávat certifikáty vydané na území Evropského hospodářského prostoru. Evropské dimenzi se věnoval § 16.

3.3.6 Služby vytvářející důvěru

V zákonu o elektronickém podpisu existoval pojem „kvalifikované certifikační služby“, který v sobě zahrnoval tehdy definované služby jako elektronický podpis, elektronickou značku a časová razítka. Ten, kdo vydával certifikáty k těmto službám, se nazýval „poskytovatel certifikačních služeb“.

Dle § 2 písmene h) se jedná o *„fyzickou osobu, právnickou osobu nebo organizační složku státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy“*.

[62] Evropská unie. 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. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 23. 7. 2014 [cit. 2022-12-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=CS

Nařízení oproti původní úpravě nově zavádí pojem „služby vytvářející důvěru“, který definuje čl. 3 odst. 16. Takto se budou označovat vytváření, ověřování shody a ověřování platnosti elektronických podpisů a pečetí a další služby podle eIDAS. Tyto služby nabízejí poskytovatelé služeb vytvářejících důvěru. Mohou se označovat za „kvalifikované“ a mohou poskytovat „kvalifikované služby“, pokud budou mít sídlo v EU a budou splňovat požadavky nařízení eIDAS, ale stejně tak mohou poskytovat i služby nekvalifikované.

Evropské nařízení rozšiřuje seznam certifikačních služeb, kterých je mnohem více než v zákoně o elektronickém podpisu. Novinkami jsou tak například služba elektronického doporučeného doručování nebo autentizace webových stránek. Také se mění některé názvy těchto služeb, například z „elektronických značek“ se stává „elektronická pečeť“.

3.3.7 Dohled

Zákon o elektronickém podpisu podle § 9 určil jako orgán dohledu Ministerstvo vnitra České republiky. To mělo právo udělovat akreditaci na základě podané žádosti a splnění stanovených podmínek, jakými jsou doložení oprávnění k podnikatelské činnosti, poskytnutí seznamu nabízených služeb nebo doložení technické a personální připravenosti k tomuto poskytování. Za nedodržování podmínek mohlo udělit pokutu nebo akreditaci úplně odejmout.[63]

Podle kapitoly III čl. 17 nařízení musí každá členská země vybrat orgán dohledu a subjekt posuzování shody pro kontrolu dodržování tohoto nařízení. Tento orgán musí také spolupracovat s orgánem na ochranu osobních údajů. Kvalifikovaní poskytovatelé služeb se sídlem v EU podléhají předběžnému (tedy před spuštěním služeb) a následnému dohledu. V případě potřeby orgán dohledu přijme opatření i proti nekvalifikovaným poskytovatelům, pokud se domnívá, že porušují pravidla stanovená v nařízení.[64]

V začátcích plnilo roli dohledového orgánu Ministerstvo vnitra, od roku 2023 se jedná o Digitální a informační agenturu. Práce dohledových orgánů je vesměs podobná. Musejí vykonávat dozor nad poskytovateli certifikačních služeb, vyzývají je k nápravě chyb, a pokud je to nutné, udělují sankce. Novinkou je nutnost vzájemné pomoci zakotvená v čl. 18, pokud

[63] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).
[64] Tamtéž.

bude chtít dohledový orgán jiného státu doplnit informace o určitém poskytovateli důvěryhodných služeb nebo společně prošetřit možné porušení nařízení.[65]

Další novinkou je také rozdělení role dohledového orgánu a subjektu posuzování shody, který přezkoumává, zda jsou splněny požadavky nařízení eIDAS kladené na kvalifikovaného poskytovatele služeb vytvářejících důvěru a na kvalifikovanou službu vytvářející důvěru. Čl. 17 mu takovou pravomoc nesvěřuje. Zatímco podle staré právní úpravy (§ 9 odst. 2 písm. f), tyto pravomoci plnilo pouze Ministerstvo vnitra ČR, shodu nyní posuzuje nezávislý orgán Český institut pro akreditaci o. p. s., který poté agentuře předává zprávu o shodě.[66]

[65] Evropská unie. 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. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 23. 7. 2014 [cit. 2022-12-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=CS

[66] Ministerstvo vnitra zveřejňuje upřesňující dokument pro účely akreditace subjektů posuzování shody. *MV ČR* [online]. Praha: Ministerstvo vnitra ČR, 21. 9. 2022 [cit. 2023-05-02]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-zverejnuje-upresnujici-dokument-pro-ucely-akreditace-subjektu-posuzovani-shody.aspx

4. ZÁVĚR

V práci jsem představil rozdíly v právních předpisech v oblasti elektronických podpisů založených na kvalifikovaném certifikátu. V roce 2000 byl přijat zákon o elektronickém podpisu, který tuto možnost v ČR zavedl. V roce 2014 bylo přijato nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, který předchozí právní úpravu zrušil a vytvořil nové podmínky pro fungování elektronického podpisu a souvisejících záležitostí.

V teoretické části jsem popsal proces legislativního přijetí, byly vysvětleny základní pojmy obsažené v zákonech a byly představeny jejich prováděcí předpisy, které jednotlivá ustanovení konkretizují a uvádějí do praxe.

Hlavní částí praktické části práce byl kvalitativní výzkum, ve kterém byl certifikačním společnostem působícím na území ČR rozeslán dotazník s šesti otázkami týkajícími se konkrétních změn a názoru na novou právní úpravu. Z výzkumu vyplynulo, že přibylo více sledovaných atributů, tedy identifikátorů fyzických i právnických osob například nový atribut Qualified certificate statement nebo přesuny osobních údajů do nových položek. Také nebylo zjištěno, že by po zavedení evropského nařízení významně narostly počty udělených certifikátů. Růst spíš vychází ze stále většího počtu agend, kde lze elektronické podpisy využít. Certifikační společnosti evropský předpis hodnotí jako prospěšný z hlediska rozšíření poskytovaných služeb a přeshraničního uznávání certifikátů. Mnozí ale zmiňují také komplikace jako horší uživatelský komfort kvůli vyšším požadavkům na bezpečnost. Podařilo se mi získat odpovědi na všechny otázky, i když některé z nich byly dosti stručné.

Další část popisovala průběh implementace nařízení eIDAS, konkrétně činnost pracovní skupiny Ministerstva vnitra a úpravu přechodného období, které poskytlo čas na přípravu pro firmy či orgány veřejné správy. Dále jsem uvedl případové studie, v nichž byl demonstrován průběh implementace eIDAS v certifikační autoritě PostSignum či v hlavním městě Praze. Od společnosti PostSignum jsem zjistil, že si musela nechat registrovat nový kvalifikovaný prostředek USB token TokenMe, který splňuje podmínky nařízení eIDAS. Dále také spustila nové služby jako Kvalifikovaný certifikát pro elektronickou pečeť nebo Ověřování elektronických podpisů a pečetí. V analýze věnující se průběhu implementace nařízení eIDAS v úřadech hlavního města Prahy lze nalézt informace o výši finančních nákladů vynaložených na pořízení technického vybavení nebo o typech užívaných bezpečnostních prostředků.

V závěru práce byly popsány hlavní rozdíly evropského nařízení oproti staré právní úpravě. Identifikoval jsem klíčové oblasti jako přeshraniční uznávání, procesy oznámení, odpovědnost poskytovatelů i států nebo spolupráci mezi zeměmi EU. Z nařízení jsem zjistil, že byl například nově zaveden systém elektronické identifikace, který umožňuje využívat elektronické služby se zajištěním jednoznačné identifikace fyzické či právnické osoby. Členské státy EU budou více spolupracovat, mohou si vyměňovat zkušenosti a řešit případné technické potíže. I přes koordinační roli Evropské komise si státy nadále ponechávají pravomoc spravovat certifikáty elektronických podpisů, udělovat je a sankcionovat uživatele a poskytovatele certifikačních služeb za porušení podmínek.

Získané informace mohou sloužit zájemcům o poznání problematiky elektronického podpisu u nás a také jako prezentace úspěšného zavedení standardu eIDAS v ČR.

SEZNAM POUŽITÝCH ZDROJŮ

DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-7169-479-7.

PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8.

Internetové zdroje

About The Common Criteria. *The Common Criteria Portal* [online]. [cit. 2023-04-01]. Dostupné z: https://www.commoncriteriaportal.org/ccra/index.cfm

Dodržování předpisů standardu FIPS (Federal Information Processing Standard) pro .NET Core. *Microsoft* [online]. Microsoft, 28. 11. 2022 [cit. 2023-04-01]. Dostupné z: https://learn.microsoft.com/cs-cz/dotnet/standard/security/fips-compliance

Elektronický podpis. *Jak na internet* [online]. CZ.NIC, 2023 [cit. 2023-01-15]. Dostupné z: https://www.jaknainternet.cz/page/1249/elektronicky-podpis/

ETSI TS 101 862 V1. 3. 2: Qualified Certificate profile. *ETSI* [online]. Evropský ústav pro telekomunikační normy [cit. 2023-04-09]. Dostupné z: https://www.etsi.org/deliver/etsi_ts/101800_101899/101862/01.03.02_60/ts_101862v010302p.pdf

Evropská unie. Dokument 52012PC0238: Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 4. 6. 2012 [cit. 2022-12-01]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:52012PC0238

Evropská unie. 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. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 23. 7. 2014 [cit. 2022-12-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=CS

Evropská unie. Postup 2012/0146/COD: COM (2012) 238: Návrh nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu. In: *EUR-Lex: Úřední věstník Evropské unie* [online]. Úřad pro publikace EU, 28. 8. 2014 [cit. 2022-12-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/HIS/?uri=celex:32014R0910&sortOrder=asc#421034

Evropská unie. 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). In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-narizeni-komise-eu-2015-1501-ze-dne-8-zari-2015-o-ramci-interoperability-podle-cl-12-odst-8-narizeni-evropskeho-parlamentu-a-rady-eu/

Evropská unie. Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-narizeni-komise-eu-2015-1502-ze-dne-8-zari-2015-kterym-se-stanovi-minimalni-technicke-specifikace-a-postupy/

Evropská unie. Prováděcí nařízení Komise (EU) 2015/806 ze dne 22. května 2015, kterým se stanoví specifikace týkající se podoby značky důvěry EU pro kvalifikované služby vytvářející důvěru. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-narizeni-komise-eu-2015-806-ze-dne-22-kvetna-2015-kterym-se-stanovi-specifikace-tykajici-se-podoby-znacky-duvery-eu-pro-kvalifikovane-sluzby-vytvarejici-duveru/

Evropská unie. Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-rozhodnuti-komise-eu-2015-1505-ze-dne-8-zari-2015-kterym-se-stanovi-technicke-specifikace-a-formaty-duveryhodnych-seznamu/

Evropská unie. Prováděcí rozhodnutí Komise (EU) 2015/1505 ze dne 8. září 2015, kterým se stanoví technické specifikace a formáty důvěryhodných seznamů. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-

elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-rozhodnuti-komise-eu-2015-1505-ze-dne-8-zari-2015-kterym-se-stanovi-technicke-specifikace-a-formaty-duveryhodnych-seznamu/

Evropská unie. Prováděcí rozhodnutí Komise (EU) 2015/1984 ze dne 3. listopadu 2015, kterým se stanoví okolnosti, formáty a postupy pro oznamování. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-rozhodnuti-komise-eu-2015-1984-ze-dne-3-listopadu-2015-kterym-se-stanovi-okolnosti-formaty-a-postupy-pro-oznamovani/

Evropská unie. Prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2016 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/provadeci-rozhodnuti-komise-eu-2016-650-ze-dne-25-dubna-2016-kterym-se-stanovi-normy-pro-posuzovani-bezpecnosti-kvalifikovanych-prostredku-pro-vytvareni-elektronickych-podpisu-a-peceti-podle-cl-3/

Evropská unie. Přijaté prováděcí akty k nařízení eIDAS: 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. In: *DIA: Digitální a informační agentura* [online]. EUR-Lex: Úřední věstník Evropské unie, 2015 [cit. 2023-05-31]. Dostupné z: https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/prijate-provadeci-akty-k-narizeni-eidas/

Identita občana v roce 2022: souhrnné vybrané statistiky. *NAKIT* [online]. Národní agentura pro komunikační a informační technologie, 21. 2. 2023 [cit. 2023-05-09]. Dostupné z: https://nakit.cz/identita-obcana-v-roce-2022-souhrnne-vybrane-statistiky/

Jednotný digitální trh. *Jak na internet* [online]. CZ.NIC, 2019 [cit. 2022-12-01]. Dostupné z: https://www.jaknainternet.cz/page/3052/jednotny-digitalni-trh/

Ministerstvo vnitra zveřejňuje upřesňující dokument pro účely akreditace subjektů posuzování shody. *MV ČR* [online]. Praha: Ministerstvo vnitra ČR, 21. 9. 2022 [cit. 2023-05-

02]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-zverejnuje-upresnujici-dokument-pro-ucely-akreditace-subjektu-posuzovani-shody.aspx

PIFFL, Robert a Ondřej FELIX. Nařízení eIDAS – Cíle, nástroje, důsledky. Metodický seminář – Dopady nařízení eIDAS po 1. 7. 2016. In: *MV ČR* [online]. Praha: Ministerstvo vnitra ČR, 2017 [cit. 2023-04-09]. Dostupné z: https://www.mvcr.cz/soubor/1-eidas-narizeni-eidas-cile-nastroje-dusledky.aspx

PIFFL, Robert. eIDAS… aneb co nám přináší nařízení EU č. 910/2014 ze dne 23. 7. 2014. In: *Egovernment* [online]. Praha: Ministerstvo vnitra ČR, září 2015 [cit. 2023-04-09]. Dostupné z: https://www.egovernment.cz/soubor/eidas-aktualni-situace-robert-piffl/

Security Target for Cybertrust UniCERT 5: Common Criteria EAL4 Evaluation. *The Common Criteria Portal* [online]. 2006 [cit. 2023-03-30]. Dostupné z: https://www.commoncriteriaportal.org/files/epfiles/Cybertrust_UniCERT_5.2.1_ST.pdf

Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru. *MV ČR* [online]. Praha: Ministerstvo vnitra ČR, 19. 10. 2022 [cit. 2023-03-26]. Dostupné z: https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx

SKLENÁK, Vilém. Digitální podpis. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR, 2003 [cit. 2022-11-20]. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000000597&local_base=KTD

SLAVÍK, Petr. Obecný úvod do Infrastruktury veřejných klíčů (PKI). *Infrastruktura veřejných klíčů: Public Key Infrastructure* [online]. 2009 [cit. 2023-03-30]. Dostupné z: http://pki.petrslavik.com/index.php?page=obecne

Sněmovní tisk 415/0: Návrh zákona o elektronickém podpisu. *PSP* [online]. Praha: Poslanecká sněmovna Parlamentu České republiky, 1999 [cit. 2022-11-04]. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=3&CT=415&CT1=0

SVÁROVSKÝ, Martin. Co je to subsidiarita? Módní zaklínadlo, nebo základ evropanství? In: *Forum 24* [online]. Praha: FORUM 24, 4. 2. 2021 [cit. 2022-12-01]. Dostupné z: https://www.forum24.cz/co-je-to-subsidiarita-modni-zaklinadlo-nebo-zaklad-evropanstvi/

ŠPETA, Sebastian. *Elektronická identifikace* [online]. Brno, 2019 [cit. 2023-05-09]. Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Radim Polčák. Dostupné z: https://is.muni.cz/th/yrpa5/

TRETERA, Jan. Poskytnutí informace dle zákona č. 106/1999 Sb. In: *MV ČR* [online]. Praha: odbor eGovernmentu MV ČR, 2. 10. 2020 [cit. 2023-04-10]. Dostupné z: https://www.mvcr.cz/soubor/mv-105227-10-eg-2020.aspx

Výroční zpráva 2001. *ÚOOU* [online]. Praha: Úřad pro ochranu osobních údajů, 2002 [cit. 2022-11-12]. Dostupné z: https://www.uoou.cz/files/vz_2001.pdf

Výroční zpráva 2016. *Česká pošta* [online]. Praha, 2017 [cit. 2023-02-08]. Dostupné z: https://www.ceskaposta.cz/documents/10180/4349406/VZ-CP-2016.pdf/db8a57aa-f2b8-4bda-be97-4741634a1b07

Odborné články

MACGREGOR PELIKÁNOVÁ, Radka, Eva Daniela CVIK a Robert MACGREGOR. Qualified Electronic Signature – eIDAS Striking Czech Public Sector Bodies. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis* [online]. 2019, **67**(6), 1551–1560 [cit. 2023-06-28]. ISSN 1211-8516. Dostupné z: doi:10.11118/actaun 201967061551

PETERKA, Jiří. Česká cesta k elektronickému podpisu? *IT-NET*. Praha: Vogel Publishing, 2000, **1**(6), 28.

Právní předpisy

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (znění od 1. 4. 2023).

Ostatní zdroje

Dopady nařízení eIDAS na poskytované služby certifikační autority PostSignum: analýza. Praha, 2016. Interní dokument.

Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.