POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Elektronický podpis a jeho aplikace v praxi

Diplomová práce

Electronic signature and its application in practice

Master thesis

VEDOUCÍ PRÁCE

RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE

Bc. Lukáš ZELENÝ

PRAHA

2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Psárech, dne 7. 3. 2022

Bc. Lukáš ZELENÝ

Poděkování

Chtěl bych touto cestou poděkovat paní Ing. Bc. Haně Švecové a panu RNDr. Václavovi Hníkovi, CSc. za odborné vedení práce a cenné rady, které mi pomohly tuto práci zkompletovat.

ANOTACE
Diplomová práce se zaměřuje na problematiku elektronického podpisu a jeho aplikaci v praxi. První část práce pojednává o východiscích elektronického podpisu. Následující kapitola blíže specifikuje možnosti zabezpečení elektronického podpisu pomocí kryptografických funkcí a certifikátů. Další část práce se věnuje využití principů elektronického podpisu v praxi včetně souvisejících nástrojů. Dále následuje praktická část, která je tvořena deskripcí procesu vytváření elektronického podpisu dokumentu, komparací dvou kvalifikovaných certifikátů od různých certifikačních autorit a analýzou certifikátu pomocí on-line nástroje. Jedná se především o analýzu bezpečnosti a využitelnosti elektronického podpisu s následným vyhodnocením.

KLÍČOVÁ SLOVA
elektronický podpis * certifikáty * certifikační autority * digitalizace * zabezpečení * šifrování

ANNOTATION
The master thesis focuses on the issue of electronic signature and its application in practice. The first part of the thesis deals with the basics of electronic signature. The following chapter specifies the possibilities of securing electronic signatures using cryptographic functions and certificates. The next part of the thesis is devoted to the application of the principles of electronic signature in practice, including the related tools. This is followed by the practical part, which consists of a description of the process of creating an electronic signature for a document, a comparison of two qualified certificates from different certification authorities and an analysis of the certificate using an on-line tool. This is mainly an analysis of the security and usability of the electronic signature with subsequent evaluation.

KEYWORDS
electronic signature * certificates * certification authorities * digitalization * security * encryption

Obsah

ÚVOD

Postupný a dlouhotrvající proces přechodu od analogové podoby nosičů dat do podoby elektronické je momentálně patrný napříč celou lidskou společností. Stejně jako tomu je v jiných oborech, také rozvoj v oblasti informačních a komunikačních technologií s sebou přináší nová rizika, která budou z počátku částí společnosti klasifikována jako nepřijatelná, kvůli čemuž dojde k získání odmítavého postoje k využívání nových technologií. Důležité je především se zaměřit na včasné odhalení negativních a rizikových aspektů za účelem přijetí adekvátních opatření, která budou směřovat k jejich eliminaci.

Mezi veřejností a politickou scénou je v posledních letech velmi populární téma digitalizace státní správy. Tento trend vnímám jako snahu o přiblížení se soukromému sektoru, v rámci kterého využívání digitálních technologií zpravidla dosahuje vyšší úrovně. Nové technologie na základě správné implementace a efektivního používání by měly především sloužit k úspoře finančních prostředků, časových nákladů a v neposlední řadě také fyzických sil. Jedná se primárně o evoluci systémů a postupů, které běžné stávající procesy zefektivní, zrychlí a usnadní, s čímž nepřímo souvisí také problematika elektronického podpisu.

Elektronické podepisování dokumentů, zpráv a jiných datových souborů v dnešní době ovlivňuje běžné pracovní i osobní aktivity spousty z nás, aniž bychom si to pokaždé uvědomovali. Vzhledem k tomu, že základní formou elektronického podpisu může být i uvedení jména v SMS zprávě, není pochyb o tom, že elektronické podepisování se stává společně s příchodem digitálních technologií nedílnou součástí našeho každodenního života. Elektronické podpisy jsou k dispozici v několika úrovních důvěryhodnosti, na základě kterých můžeme definovat jejich reálnou použitelnost. V osobní a pracovní rovině si můžeme vystačit i s těmi základnějšími variantami elektronického podpisu, nýbrž pro komunikaci se státní správou jsou již požadavky o něco vyšší.

Velkým impulzem pro občany k přechodu na elektronickou komunikaci s orgány státní správy byla celosvětová pandemie koronaviru SARS-CoV-2, která si svým rozsahem a zdravotními dopady vyžádala omezení osobních kontaktů na nezbytné minimum. Interpersonální komunikace byla z velké části takřka obratem přesunuta do on-line prostředí, což se mimo jiné v určitých oborech podnikání

ukázalo jako velmi efektivní a výhodné, avšak s on-line vyřizováním zákonných povinností vůči státním institucím to pro mnohé občany nebylo tak jednoduché, jelikož nejprve bylo třeba zvolit a zajistit vhodný nástroj splňující požadavky na důvěryhodnou komunikaci. Za tímto účelem se více do popředí mohly dostat nástroje, mezi které se řadí například informační systém datových schránek, elektronické podpisy nebo bankovní identita.

Masivní migrace komunikačních kanálů do on-line prostředí byla jednou z vnitřních pohnutek, která mě přinutila směřovat výběr tématu ke službám eGovernmentu se zaměřením na problematiku elektronických podpisů. Vzhledem k tomu, že z názorů mého okolí a veřejnosti bylo možné vycítit určitou nejistotu a mírné obavy z hlediska bezpečnosti v oblasti elektronické komunikace, diplomová práce je koncipována primárně na úrovně zabezpečení prvků z oblasti praktického využití elektronického podepisování.

Cílem práce je vytvoření souboru relevantních poznatků o problematice elektronického podpisu se zaměřením na jednotlivé úrovně důvěryhodnosti, související nástroje, technické principy a metody zabezpečení a v neposlední řadě také vhodné alternativy. Praktická část práce je tvořena deskripcí postupu vytvoření elektronického podpisu pomocí vhodného softwarového nástroje, což zahrnuje mimo jiné zajištění a implementaci kvalifikovaného certifikátu, dále komparací dvou nezávislých kvalifikovaných certifikátů a nakonec analýzou kvalifikovaného certifikátu pomocí on-line nástroje. Účelem praktické části je vyhodnocení dané problematiky a nastínění vlastních návrhů na zlepšení aktuálního stavu.

TEORETICKÁ ČÁST

1. Východiska elektronického podpisu

Aktuální doba s sebou přináší rozsáhlý a komplexní rozvoj informačních a komunikačních technologií, což má významné dopady především na snahu o masivní digitalizaci dat a úkonů nejen v soukromém sektoru, ale také v oblasti veřejné správy. Současný trend expanze IT sféry lze bezpochyby vnímat do značné míry pozitivně, jelikož se jedná o významný krok k usnadnění a urychlení běžných i specifických procesů, avšak společně s tím by neměly být upozaděny negativní aspekty, se kterými se můžeme setkat například v podobě nových bezpečnostních rizik.

Zavádění a rozšiřování digitálních technologií souvisí mimo jiné s konverzí materiálů a přesunem komunikace z listinné podoby a do podoby elektronické, přičemž tento proces musí nevyhnutelně reflektovat požadavky na vytváření a užívání systémů zabezpečení a ochrany dat před širokou škálou rizik. Mezi primární cíle z hlediska bezpečnosti patří zajištění ochrany před ztrátou, změnou nebo krádeží dat a citlivých údajů, zamezení možnému odposlechu komunikace nebo důraz na autentizaci a autentifikaci osob, s čímž do značné míry souvisí problematika elektronického podpisu, jehož základy se tato kapitola zabývá.

1.1 Digitalizace dokumentů

Pro účely této práce lze pojem dokument objasnit pomocí definice uvedené v zákoně č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, tedy že dokumentem se rozumí *každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena.*[1]

Písemný dokument, jehož obsah je tvořen určitou posloupností číslic, písmen, interpunkčních znamének a dalších znaků, může existovat v listinné nebo elektronické podobě.[2]

---

[1] Zákon č. 499/2004 Sb., *o archivnictví a spisové službě a o změně některých zákonů* v posledním znění

[2] viz str. 28, PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8.

Listinná podoba dokumentu nebo datové zprávy je základním kamenem pro vytvoření jeho digitální podoby. Nejtypičtějším nosičem dat pro dokumenty v listinné podobě je standardní papír, avšak v historii se ke stejnému účelu využívaly také jiné nosiče jako například pergamen. Pokud se na listinné dokumenty podíváme optikou nákladů, je třeba si uvědomit, že zpracování, správa, přeprava, skladování a archivace větších objemů takových dokumentů může být podstatně nákladnější než u digitálních dokumentů. Další významnou nevýhodou listinného neboli analogového dokumentu je pouze zdánlivá autenticita uživatele na základě vlastnoručního podpisu. V praxi to znamená, že druhá strana zpravidla není schopna posoudit pravost vlastnoručního podpisu, kvůli čemuž může dojít ke klamnému nebo podvodnému právnímu jednání.

Podstatně novější formou dokumentu je jeho elektronická podoba, která s sebou oproti listinné podobě přináší množství výhod. Elektronické neboli digitální dokumenty jsou ukládané na elektronických nosičích, ke kterým je častokrát možné zřídit také vzdálený přístup a vyhnout se tak nutnosti využití lokálních uložišť. Mezi stěžejní přínosy využívání digitálních dokumentů se řadí nižší náklady (za předpokladu zavedení vhodného systému pro práci s takovými dokumenty). Dokumenty v elektronické podobě je také možné o poznání snadněji sdílet s dalšími uživateli, tudíž se výrazně zefektivňuje kooperace uživatelů a koordinace společných aktivit. Mimo jiné elektronická forma dokumentů společně s internetovým připojením umožňuje výrazně rychlejší odesílání a přijímání souborů, což vede k úspoře času a zkrácení reakční doby. Další z řady výhod je možnost ukládání dat do databází, což vytváří vhodné podmínky pro jejich následné využívání v navazujících automatizovaných procesech. Neposledním, avšak pro účely této diplomové práce zcela stěžejním, benefitem používání elektronické formy dokumentu je možnost vkládání vyšších forem zaručeného elektronického podpisu, které oproti vlastnoručnímu podpisu dokáží zajistit garantovanou autenticitu uživatele.[3]

V současné době se dle obecně platných zásad na elektronickou a listinnou formu dokumentů pohlíží zcela rovnocenně, tudíž ani jedné variantě vyhotovení nelze přisuzovat větší váhu. S rovnoprávností těchto forem dokumentů se velmi

[3] BRUNCLÍK, Zdeněk. Listinná, nebo elektronická agenda?. *Moderní obec* [online]. [cit. 9.1.2022]. Dostupné z: https://www.moderniobec.cz/listinna-nebo-elektronicka-agenda/

často můžeme setkat například v oblasti účetnictví a daňové evidence, kdy daňový doklad vystavený a prokazatelně doručený elektronicky má shodné postavení a účinky jako daňový doklad v listinné podobě.[4]

Konverze

Proces, při kterém dochází k převodu dokumentu z listinné podoby do podoby elektronické nebo opačně, se nazývá konverze. Podstatou konverze je změna formy dokumentu takovým způsobem, jež zajišťuje shodu obsahu těchto dokumentů.[5]

Český právní řád zakotvuje autorizovanou konverzi dokumentů, jejíž právní úpravu nalezneme v zákoně č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Konverze ve smyslu tohoto zákona zajistí, že výstupní dokument má stejné právní účinky jako dokument vstupní. Ani autorizovaná konverze nepotvrzuje soulad obsahu dokumentu s právními předpisy a správnost nebo pravost údajů obsažených v konverzovaném dokumentu. Provedení konverze doprovází také připojení doložky o provedení konverze, která se následně ukládá do centrálního úložiště ověřovacích doložek. Při tomto procesu nedochází k ukládání samotného konverzovaného dokumentu, nýbrž pouze zmiňované doložky.

Autorizovaná konverze dokumentů může být provedena na žádost prostřednictvím kontaktních míst veřejné správy (Czech POINT) a advokáty za podmínek stanovených jiným právním předpisem nebo z moci úřední orgány veřejné moci pro výkon své působnosti.[6]

1.2 Podpis a jeho funkce

Pokud zazní slovo „podpis“, většina z nás si vybaví svůj vlastní podpis ručně napsaný na papír, jehož základní podobu si obvykle vytvořil již během svých

[4] VODIČKA, Milan. Elektronický doklad - kam s ním a jak? *Daně, účetnictví, právo, práce a mzdy pro profesionály* [online]. 4. 4. 2018 [cit. 9.1.2022]. Dostupné z: https://www.du.cz/33/elektronicky-doklad-kam-s-nim-a-jak-uniqueidmRRWSbk196FNf8-jVUh4Ese1lEiNjoMQoi3ehGYe2PDmmVIyNELpDA/

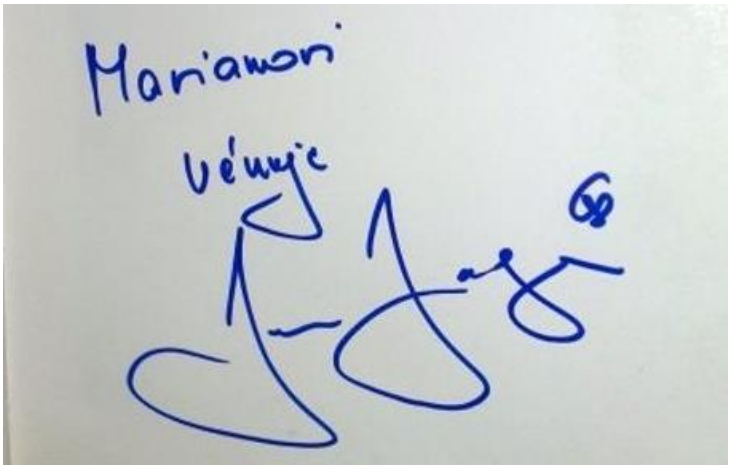
[5] Konverze. *Czech POINT* [online]. [cit. 9.1.2022]. Dostupné z: https://www.czechpoint.cz/public/verejnost/autorizovana-konverze/

[6] Zákon č. 300/2008 Sb., *o elektronických úkonech a autorizované konverzi dokumentů* v posledním znění

školních a studentských let. Používání podpisu se postupem času stává běžnou součástí našich životů, jelikož jej v dospělosti využíváme při nejrůznějších úkonech typicky pro identifikaci, odsouhlasení určitého obsahu listiny a zavázání se k stanovenému jednání (např. uzavírání smluv) nebo k prokázání své přítomnosti.

Vlastnoruční podpis

Výsledná grafická podoba vlastnoručního podpisu je tvořena nejčastěji specifickou zakřivenou čárou přenesenou na hmotný nosič (zpravidla na papír) prostřednictvím určitého psacího nástroje. Struktura a vzhled podpisu by měly být unikátní a obvyklé pro danou osobu. Vlastnoruční podpis by neměl být snadno napodobitelný jinou osobou, avšak podepisující osoba by naopak měla zvládnout podpis vytvořit opakovaně prostřednictvím svého podpisového vzoru. Podepsáním listiny dochází k projevu vůle navenek, tudíž není možné podpis vytvořit nevědomě nebo k vlastnoručnímu podpisu využít jinou osobu. Obsahem podpisu by mělo být alespoň příjmení osoby, avšak za přijatelný a platný lze v praxi považovat také zjednodušený nebo nečitelný podpis ve formě klikyháku. Podpis se zpravidla umísťuje společně s datem a místem podpisu na konec listiny za všechna její ustanovení.[7] Ukázka vlastnoručního podpisu je na obrázku 1 níže.[8]



Obrázek 1 – Fotografie vlastnoručního podpisu hokejisty Jaromíra Jágra včetně věnování

[7] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra. *Advokátní deník* [online]. 4. 5. 2020 [cit. 15.1.2022]. Dostupné z: https://advokatnidenik.cz/2020/05/04/podepisovani-soukromych-listin-vcera-dnes-a-zitra/

[8] Zdroj obrázku 1: KOLÁŘ, Milan. FOTO Jaromír Jágr a hokejové kluby jeho života. *Aktuálně.cz* [online]. 24. 7. 2013 [cit. 14.3.2022]. Dostupné z: https://sport.aktualne.cz/hokej/foto-jaromir-jagr-a-hokejove-kluby-jeho-zivota/r~c3196d5aef9111e2b9470025900fea04/

Ověřit pravost vlastnoručního podpisu na základě samotného vzhledu je pro laickou veřejnost velmi obtížné. Zpracovávání relevantních analýz písma je zejména v kompetenci grafologů, kteří zkoumají pomocí různých metod specifické rysy podpisu, jakým je například trajektorie tahu perem, sklon a tvar použitých znaků, nebo typ použitého inkoustu a papíru. Snazší variantou pro zajištění a doložení pravosti podpisu je možnost využití služeb ověření vlastnoručního podpisu prostřednictvím notáře nebo úředníka (např. na pobočkách Czech POINT).[9]

Biometrický podpis

Vzhledem k tomu, že tvorba a provedení vlastnoručního podpisu závisí do jisté míry také na biomotorických schopnostech daného člověka, autor Vojtěch Kment jej částečně zařazuje do kategorie biometrických podpisů. Rozdílem oproti dalším standardním biometrickým podpisům (otisk prstu, snímek duhovky nebo obličeje) je především v tvorbě vlastnoručního podpisu, která probíhá na základě volního uvážení člověka, což pro další typy biometrických podpisů neplatí. Jednou z variant biometrického podpisu je také v poslední době hojně používaný v bankovním sektoru tzv. dynamický biometrický podpis, kdy se osoba vlastnoručně podepíše speciálním dotykovým perem na tablet nebo sign pad, čímž vzniknou biometrická data, která se po zpracování softwarovým nástrojem vloží do podpisové části dokumentu.[10] Při tomto procesu dochází k určité kombinaci vlastnoručního, biometrického a elektronického podpisu.

Ačkoliv proces vytváření dynamického biometrického podpisu se na první pohled může zdát velice podobný jako u vlastnoručního podpisu, ve skutečnosti se zde vyskytují větší rizika, jelikož druhé straně neposkytujeme pouze výslednou grafickou podobu podpisu, nýbrž i další jedinečná biometrická data vztahující se k osobnímu podpisovému vzoru. Vstupní hardware zaznamenává trajektorii dotykového pera, tlak, rychlost a další parametry, které jsou velice důležité pro zachování unikátnosti podpisu. Dalším negativním aspektem z hlediska

[9] viz str. 28–29, PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8.
[10] viz str. 59, KMENT, Vojtěch. *Elektronické právní jednání: Analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-814-8.

bezpečnosti je fakt, že výše uvedené služby fungují primárně na bázi smluvního vztahu a nevytvářejí důvěru podle nařízení eIDAS, neexistuje oficiální licence zaručující požadovanou úroveň zabezpečení ani zákonem stanovené požadavky na poskytovatele či samotná zařízení, tudíž je zde potenciálně vyšší riziko nežádoucího nakládání s biometrickými daty než u vlastnoručního či zaručeného elektronického podpisu.[11]

Biometrický a dynamický biometrický podpis lze vnímat jako prostý elektronický podpis, jelikož data jsou uchovávána v digitální podobě, avšak je zde absence právních a technických náležitostí, bez nichž se nemůže jednat o zaručený nebo uznávaný (kvalifikovaný) elektronický podpis. Dalším důvodem pro neoficiální zařazení biometrického podpisu do kategorie prostého elektronického podpisu je odlišnost výchozích dat. Zatímco u biometrických a vlastnoručních podpisů jsou základem biometrická data jako součást tělesné integrity člověka, zaručené a kvalifikované elektronické podpisy jsou postaveny především na matematických výpočtech.[12]

Elektronický podpis

V návaznosti na předchozí podkapitoly nám zbývá objasnit a definovat poslední ze základních a nejběžněji používaných druhů podpisů, tedy podpis elektronický, který je však pro účely této práce nejpodstatnější. Elektronický podpis svým účelem přímo navazuje na podstatu vlastnoručního a biometrického podpisu a za určitých okolností je dokonce nahrazuje. Základní pojem elektronický podpis zahrnuje všechny vytvořené důkazy dokládající, že daný dokument nebo zpráva byly zhotoveny nebo schváleny konkrétní osobou.[13] Jedná se obdobu projevu vůle člověka navenek v rámci odlišného elektronického prostředí. Jelikož je elektronický podpis postaven převážně na matematických a kryptografických

[11] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra. *Advokátní deník* [online]. 4. 5. 2020 [cit. 15.1.2022]. Dostupné z: https://advokatnidenik.cz/2020/05/04/podepisovani-soukromych-listin-vcera-dnes-a-zitra/

[12] tamtéž

[13] viz str. 30, DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* 2., aktualiz. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2619-6.

principech, můžeme jej definovat jako jedno velké číslo, které se pro zjednodušení vyjadřuje pomocí řetězce znaků vycházejících z kódování.[14]

Pokud se na elektronický podpis podíváme čistě z technického hlediska, můžeme pod tímto pojmem spatřovat hned několik různých metod identifikace osob běžně používaných v oblasti informačních a komunikačních technologií. Za užití elektronického podpisu může být považováno:

- uvedení jména na konci e-mailové zprávy
- uvedení jména v hlavičce e-mailové zprávy
- uvedení jména v podpisové části elektronického dokumentu
- zadání osobního PIN kódu
- odsouhlasení právního textu (např. obchodních podmínek) zaškrtnutím políčka a potvrzením akce
- naskenování vlastnoručního podpisu a následné vložení ve formátu obrázku do podpisové části elektronického dokumentu
- vytvoření dynamického biometrického podpisu prostřednictvím tabletu nebo sign padu a následné vložení do podpisové části dokumentu
- použití digitálního podpisu s kryptografickou ochranou[15]

Digitální podpis

Řada autorů, mezi které se řadí například Libor Dostálek, Marta Vohnoutová a Miroslav Knotek, odlišuje od elektronického podpisu také pojem digitální podpis. Digitální podpis bývá definován jako elektronický podpis vytvořený za využití asymetrické kryptografie, tudíž se stává pomyslnou specifickou podmnožinou elektronických podpisů. Aplikací digitálního podpisu dochází k ověření pravosti dokumentu či zprávy, což lze z hlediska důvěryhodnosti postavit na roveň vlastnoručního podpisu. Vzhledem k tomu, že digitální podpis popsaný

[14] viz str. 29, PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8.
[15] viz str. 59, KMENT, Vojtěch. *Elektronické právní jednání: Analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-814-8.

výše zaručuje, že obsah nebyl nikým neoprávněně upraven nebo pozměněn, můžeme jej označit také jako zaručený elektronický podpis.[16]

1.3 Druhy elektronického podpisu

Jak již bylo několikrát nastíněno v předchozí podkapitole, základní pojem elektronický podpis zahrnuje širokou škálu druhů, forem a variant elektronických podpisů v závislosti na technickém provedení nebo právní relevanci. Pokud se v praxi setkáme se slovním spojením „elektronický podpis“, zpravidla se bude jednat o podpis mající požadovanou úroveň důvěryhodnosti zaručenou příslušným certifikátem. Než se však pustíme do problematiky sofistikovanějších zaručených a uznávaných elektronických podpisů, nejprve si představíme takzvaný „prostý“ elektronický podpis.

„Prostý“ elektronický podpis

Hlavním důvodem pro použití uvozovek u doplňujícího slova „prostý“ je zdůraznění, že se jedná spíše o slovo použité za účelem lepšího odlišení od ostatních druhů elektronického podpisu než o oficiální název. Častokrát se v odborné literatuře můžeme setkat také s pojmenováním elektronický podpis „bez přívlastku“.

Prostý elektronický podpis je s ohledem na dostupnost a využitelnost elementárním druhem elektronického podpisu. Tato kategorie elektronického podpisu zahrnuje nejběžnější metody provedení podpisu, mezi které patří základní akce prováděné uživateli téměř na každodenní bázi. Jedná se například o napsání jména a příjmení v e-mailové zprávě, zaškrtnutí políčka „Souhlasím“ nebo „Přijímám“ na internetové stránce, naskenování vlastnoručního podpisu, vlastnoruční podpis vytvořený dotykovým perem nebo prstem v grafickém editoru a tak podobně (viz obrázek 2).

Své uplatnění prostý elektronický podpis nachází primárně v soukromoprávních vztazích (např. při uzavírání kupních smluv), kdy se jím může nahradit vlastnoruční podpis. Možnost nahradit vlastnoruční podpis prostým

[16] viz str. 30, DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* 2., aktualiz. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2619-6.

elektronickým podpisem reflektuje konkrétní dohodu soukromoprávních subjektů. Naopak subjekty si mohou na základě smluvní volnosti ujednat přísnější požadavky na aplikaci elektronických podpisů s větší důvěryhodností a vyšším stupněm ochrany.[17] Z pohledu orgánů státní správy a územně samosprávných celků je podepsání dokumentu nebo zprávy prostřednictvím prostého elektronického podpisu v rámci standardní oficiální komunikace soukromých subjektů s veřejnými institucemi zcela nepřípustná.

Obrázek 2 – Ukázka prostého elektronického podpisu vytvořeného v Adobe Acrobat Reader DC

Zásadní nevýhodou prostého elektronického podpisu je jeho velmi nízká důvěryhodnost, jelikož ve většině případů nelze zaručit shodu osoby, která podpis fakticky k dokumentu nebo zprávě připojila, s osobou, jež podpis vytvořila s vědomím dopadů takového jednání.[18] Riziko zkopírování a následného použití prostého elektronického podpisu osoby dalším nekompetentním subjektem lze považovat za poměrně vysoké, jelikož technické provedení jakékoliv z variant prostého elektronického podpisu obyčejně neobsahuje potřebné ochranné mechanismy proti neoprávněnému použití, a tudíž nelze zaručit jednoznačné spojení s podepisující osobou. Jiří Peterka ve své knize označuje prostý elektronický podpis za slabý, bez garance. Vypovídající hodnota takového podpisu je v praxi čistě informační, což nepřímo směřuje k postoji nepovažovat prostý elektronický podpis za elektronický podpis, k čemuž se různé zdroje ve svých výkladech často neoficiálně přiklání.[19]

---

[17] HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *EPRAVO.CZ: Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. 22. 1. 2020 [cit. 16.1.2022]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

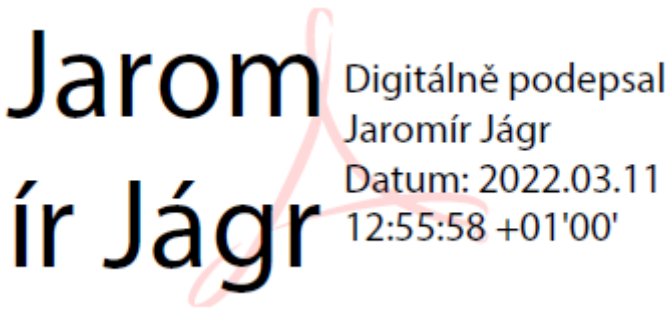
[18] NAVARA, David. Elektronický podpis prostý. *INOXI: Správa firemních IT & ICT sítí* [online]. 2. 4. 2021 [cit. 16.1.2022]. Dostupné z: https://www.elektronicky-podpis.info/pojmy/elektronicky-podpis-prosty.dot

[19] viz str. 29, PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8

Zaručený elektronický podpis

S ohledem na značná rizika a problémy s identifikací nebo garancí pravosti prostého podpisu, které jsou zmíněny v předchozí kapitole, je nasnadě zmínit potencionálně bezpečnější a důvěryhodnější formu elektronického podpisu, kterou je tzv. zaručený elektronický podpis (AdES – Advanced Electronic Signature). Současně s přesunem pozornosti na téma zaručeného elektronického podpisu bychom mohli teoreticky začít používat také pojmenování digitální podpis, jelikož do elektronického podpisu vstupuje významná forma ochrany, kterou je šifrování. Pro větší přehlednost a zachování ucelenosti však pojem digitální podpis pro účely této práce zůstane spíše v ústraní.

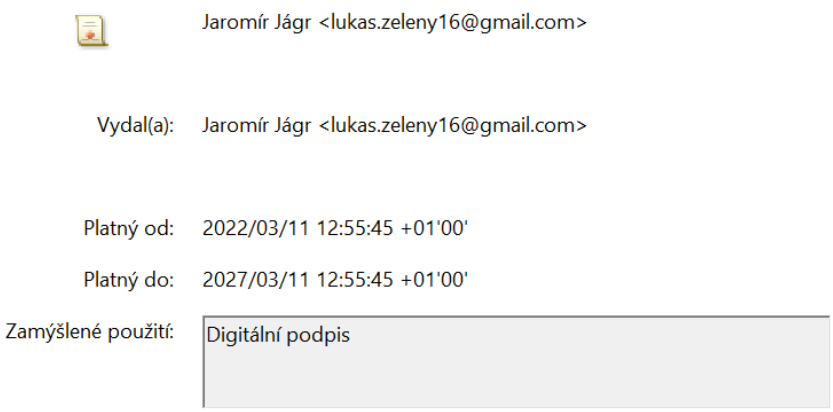
Jak již název napovídá, zaručený elektronický podpis poskytuje druhé straně (např. adresátovi dokumentu) určitou záruku, že obsah podepsaného dokumentu již nemůže být změněn, a zároveň použitý zaručený elektronický podpis nemůže být duplikován a vložen do jiného dokumentu. Technologické principy a postupy založené na asymetrické kryptografii používané pro zajištění záruky elektronického podpisu, o kterých bude řeč v následujících kapitolách této práce, jsou základním kritériem pro odlišení prostého a zaručeného elektronického podpisu.[20] Díky vyšší úrovni jistoty, kterou aplikace zaručeného elektronického podpisu poskytuje, mohou smluvní strany pohlížet na právní jednání výrazně bezpečněji, avšak samozřejmě ani zmiňovaná garance nemusí být vždy stoprocentní, tudíž obezřetnost je stále na místě (viz obrázek 3 a obrázek 4 níže).



Obrázek 3 – Ukázka vzhledu zaručeného elektronického podpisu založeného na nedůvěryhodném certifikátu se jménem hokejisty Jaromíra Jágra v Adobe Acrobat Reader DC

[20] HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *EPRAVO.CZ: Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. 22. 1. 2020 [cit. 16.1.2022]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

Základem zaručeného elektronického podpisu je certifikát, díky kterému je zaručena integrita dokumentu (celistvost) a zamezena možnost nežádoucího kopírování podpisu jinými osobami, avšak tento certifikát nedává automaticky záruku, že dokument byl podepsán skutečnou osobou, které podpis náleží. Nedostatečné zajištění identifikace a autentizace podepisující osoby výrazně omezuje postavení soukromoprávního subjektu (např. odesílatele zprávy) vůči orgánům státní správy a samosprávy, jelikož se nejedná o formu uznávaného elektronického podpisu, k němuž je třeba kvalifikovaný certifikát od uznávané certifikační autority. Jednou ze zásadních podmínek kvalitního zaručeného elektronického podpisu je tzv. nepopiratelnost, na základě níž podepisující osoba nemůže v budoucnu popřít, že podpis vytvořila ona, a tudíž se nemůže oprostit od důsledků svého podpisu. Takovou záruku nám však nedává jakýkoliv zaručený elektronický podpis, nýbrž pouze podpis založený na kvalifikovaném certifikátu.



Obrázek 4 – Ukázka informací o nedůvěryhodném certifikátu prostého elektornického podpisu

Zaručený elektronický podpis založený na nekvalifikovaném certifikátu od nedůvěryhodné certifikační autority by v praxi neměl být úředně uznáván, jelikož jeho aplikací nedochází k požadovanému ověření totožnosti signatáře.[21] V případě akceptace zaručeného elektronického podpisu bez kvalifikovaného certifikátu by úřady měly na takový dokument formálně nahlížet jako na dokument nepodepsaný, tudíž ve vztahu k dané situaci (pokud je vyžadována náležitost identifikace a autentizace osoby) jako na dokument irelevantní.

[21] DOLEČEK, Marek. Využívejte elektronické podpisy a elektronickou identitu. Poradíme, jak na to. *BusinessInfo.cz* [online]. 28. 11. 2021 [cit. 21.1.2022]. Dostupné z: https://www.businessinfo.cz/navody/elektronicke-podpisy-elektronicka-identita-ppbi/2/#zaruceny-elektronicky-podpis-zalozeny-na-nekvalifikovanem-certifikatu

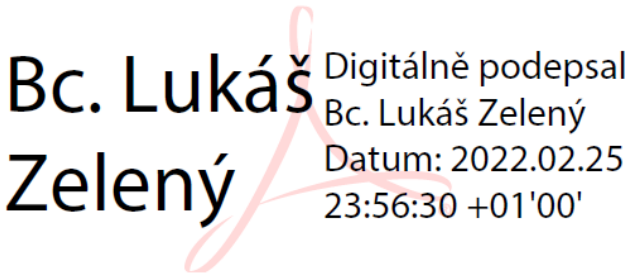
V soukromoprávních vztazích významně záleží na dohodě v rámci smluvní volnosti všech stran, jak si vzájemně nastaví míru přijatelnosti a uznávání jednotlivých druhů elektronických podpisů, díky čemuž je možné právně jednat mimo jiné také na základě použití „pouhého“ zaručeného elektronického podpisu.[22]

Zaručený elektronický podpis lze z technického hlediska považovat za druh elektronického podpisu s o poznání vyšší mírou zabezpečení, než jak je tomu u prostého elektronického podpisu, avšak stále zde postrádáme významnou složku autentizace podepisující osoby, kterou nabízí až další úrovně elektronického podpisu, jakými jsou uznávané a kvalifikované elektronické podpisy.

Uznávaný elektronický podpis

V případě záměru využít zaručený elektronický podpis fyzickou osobou vůči veřejnoprávnímu subjektu nebo jiné osobě v souvislosti s výkonem jeho působnosti, je třeba využít specifičtějšího uznávaného elektronického podpisu, jehož alternativním názvem může být také zaručený elektronický podpis založený na kvalifikovaném certifikátu (AdESQC – Advanced Electronic Signature based on a Qualified Certificate).

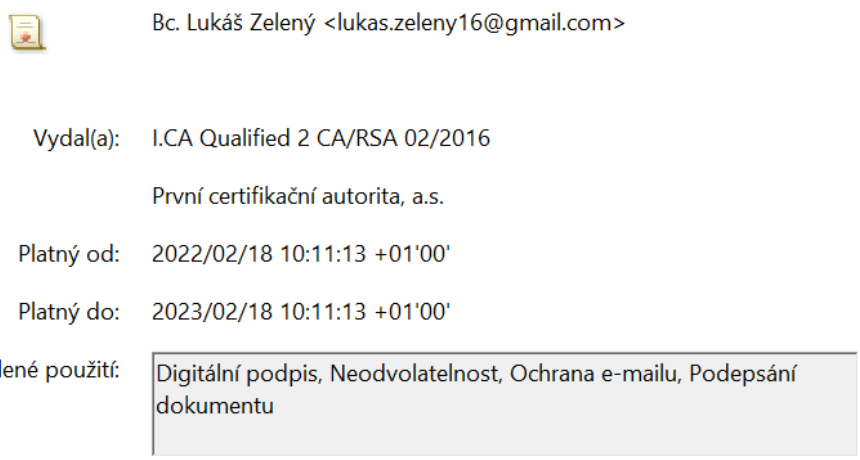
K transformaci „pouhého“ zaručeného elektronického podpisu na uznávaný elektronický podpis je nezbytně nutné, aby podpis byl založen na kvalifikovaném certifikátu vydaným jednou z oficiálně uznávaných certifikačních autorit, o kterých bude řeč v následujících kapitolách. Ukázka uznávaného elektronického podpisu se nachází na obrázku 5 a obrázku 6.



Obrázek 5 – Ukázka vzhledu uznáveného elektronického podpisu v Adobe Acrobat Reader DC

[22] PETERKA, Jiří. Elektronický podpis v praxi (1): uznávaný, nebo jen zaručený?. *Computerworld*. 2012, roč. 23, č. 3, s. 30. ISSN 1210-9924.

Kvalifikovaný certifikát uznávaného elektronického podpisu dává kromě záruky zajištění integrity dokumentu poskytované již běžným zaručeným elektronickým podpisem také dostatečnou garanci identifikace podepisující osoby, která je z pohledu standardního procesu podepisování (ať už vlastnoručního, biometrického nebo elektronického) velmi důležitá. Atribut identifikace a autentizace podepisující osoby vychází z ověření totožnosti, které bezpodmínečně předchází vydání kvalifikovaného certifikátu jednou ze tří akreditovaných certifikačních autorit. Vypovídající hodnota uznávaného elektronického podpisu koresponduje s hodnotou vlastnoručního podpisu, nikoliv však s hodnotou ověřeného vlastnoručního podpisu.[23]



Obrázek 6 – Ukázka informací o důvěryhodném certifikátu uznávaného elektronického podpisu

Úroveň technického zabezpečení uznávaného elektronického podpisu se zpravidla nikterak výrazně neliší od jiných variant zaručených elektronických podpisů, avšak zásadní roli hraje ověření použití podpisu skutečným vlastníkem. Na druhou stranu rozšíření uznávaného podpisu v podobě identifikace osoby s sebou stále nese riziko potencionálně nepřesné identifikace, jelikož může dojít například k neoprávněnému použití takového podpisu jinou osobou, která získá přístup k uznávanému elektronickému podpisu, případně použití podpisu jinou osobou rozdílnou od vlastníka na základě svolení k použití elektronického podpisu v zastoupení.

[23] HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *EPRAVO.CZ: Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. 22. 1. 2020 [cit. 21.1.2022]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

Kvalifikovaný elektronický podpis

Posledním elementárním druhem elektronického podpisu, kterým se v rámci této práce budeme zaobírat, je kvalifikovaný elektronický podpis (QES – Qualified Electronic Signature). Ve své podstatě se jedná o podpis postavený na stejném principu jako uznávaný elektronický podpis s tím rozdílem, že používání kvalifikovaného elektronického podpisu vyžaduje kromě samotného kvalifikovaného certifikátu také kvalifikovaný prostředek. Kvalifikovaný prostředek je určitá část kvalifikovaného certifikátu nazývaná jako soukromý klíč, který je na rozdíl oproti jiným typům zaručeného elektronického podpisu uložen na separovaném externím nosiči. Absence přítomnosti kvalifikovaného prostředku znamená nemožnost dokument nekompletním kvalifikovaným certifikátem řádně podepsat.[24]

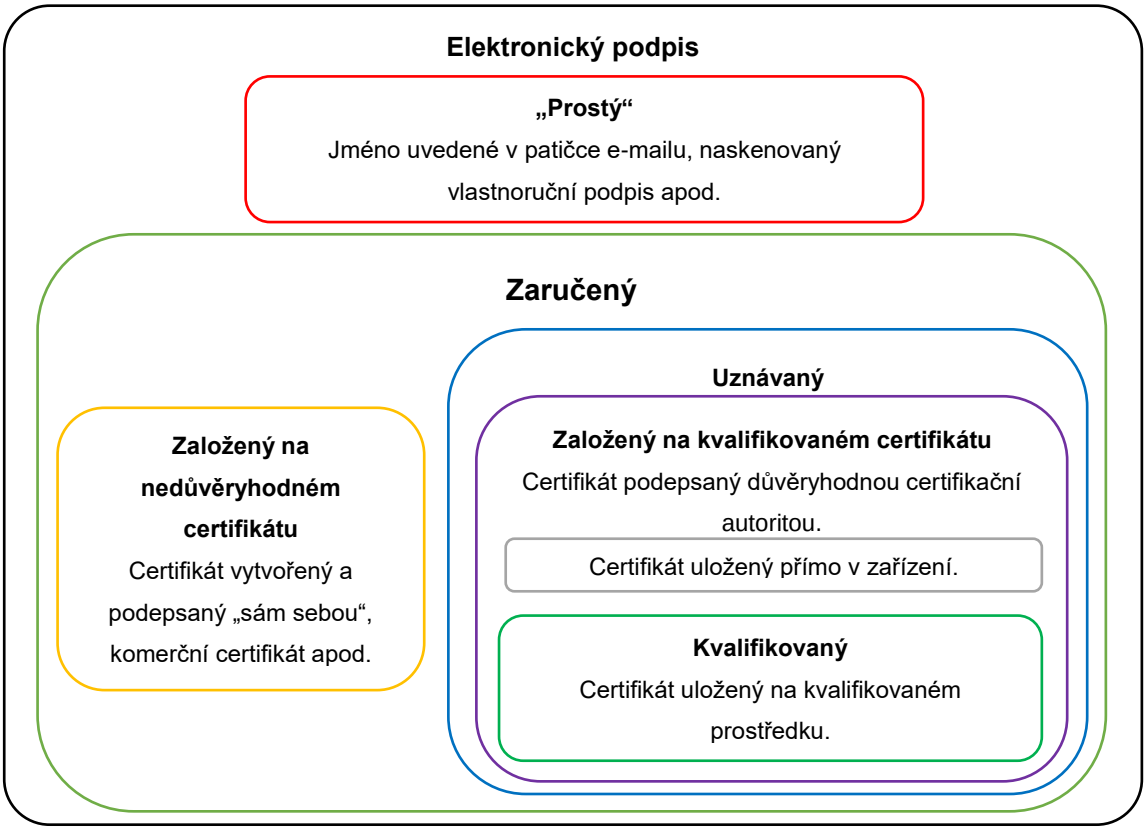
Před vydáním kvalifikovaného elektronického podpisu dochází stejně jako u uznávaného elektronického podpisu k ověření totožnosti osoby, avšak nestačí zde pouhé uložení soukromého klíče například na místním disku počítače, nýbrž je vyžadováno uchování na certifikované čipové kartě (např. novější verzi dokladu totožnosti zvané eObčanka) nebo jiném externím nosiči (např. USB tokenu). Data z nosiče kvalifikovaného prostředku nejsou převoditelná na jiné médium, čímž se zajistí, že k aplikaci kvalifikovaného podpisu je vyžadována fyzická přítomnost kvalifikovaného prostředku a jeho spojení s daným zařízením v reálném čase. Pozitivní praktické dopady onoho řešení můžeme spatřovat především v tom, že fyzická osoba by u podepisování měla být osobně přítomna (za předpokladu, že kvalifikovaný prostředek má stále k dispozici).[25]

Při komunikaci fyzických osob s veřejnoprávními orgány a institucemi postačí použití uznávaného elektronického podpisu, který nemusí být klasifikován jako kvalifikovaný, avšak nic nebrání, aby tomu tak bylo. Naopak osoby jednající za veřejnoprávní orgány nebo instituce jsou povinny ze zákona používat výhradně

[24] What is a Qualified Electronic Signature (QES) and its characteristics. *Electronic IDentification - IDentity Verification Solutions* [online]. 19. 4. 2021 [cit. 22.1.2022]. Dostupné z: https://www.electronicid.eu/en/blog/post/qualified-electronic-signature/en

[25] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra. *Advokátní deník* [online]. 4. 5. 2020 [cit. 22.1.2022]. Dostupné z: https://advokatnidenik.cz/2020/05/04/podepisovani-soukromych-listin-vcera-dnes-a-zitra/

kvalifikovaný elektronický podpis.[26] Nespornou výhodou kvalifikovaného elektronického podpisu je také jeho globální význam v podobě uznávání všemi státy EU na základě Nařízení eIDAS implementované do právních řádů jednotlivých členských států.



Obrázek 7 – Schéma systému elektronického podpisu

Jak je mimo jiné patrné ze schématu na obrázku 7, kvalifikovaný podpis můžeme v současné době zařadit na nejvyšší úroveň bezpečnosti a důvěryhodnosti v oblasti elektronických podpisů. Pokud se na věc díváme realistickým pohledem, je samozřejmě možné podpis aplikovat jinou osobou za předpokladu předání nebo zcizení kvalifikovaného prostředku. Tento postup však není možné aktuálně redukovat žádným jiným typem elektronického podpisu. Typickým příkladem nepřímé aplikace kvalifikovaného podpisu jinou osobou je předání kvalifikovaného prostředku podřízenému zaměstnanci nebo jiné odpovědné osobě (např. účetní) za účelem snížení své administrativní zátěže a zrychlení podpisového procesu. Ačkoliv kvalifikovaný prostředek se stává do

[26] Zákon č. 297/2016 Sb., *o službách vytvářejících důvěru pro elektronické transakce* v posledním znění

jisté míry osobním předmětem s určitou hodnotou, tudíž k jeho ztrátě nebo odcizení by nemělo docházet, zcela zamezit takovému nešvaru není možné. Riziko neoprávněného užití je však oproti certifikátu uloženému na lokálním uložišti výrazně sníženo. Další nepřímo navazující úrovní ověření podpisu je úřední nebo notářské ověření vlastnoručního podpisu, což však lze považovat za krok zpět z hlediska digitalizace.[27]

1.4 Elektronická pečeť

Během předchozího mapování problematiky elektronického podpisu jsme nepřímo několikrát narazili na to, že všechny formy zaručeného elektronické podpisu jsou určeny výlučně fyzickým osobám bez ohledu na to, zdali jednají za obchodní společnost, družstvo, státní orgán, veřejnoprávní korporaci nebo za sebe samotné. Možnost aplikovat elektronický podpis pouze fyzickou osobou je v jednoznačné analogii s vlastnoručním podpisem, který může vytvořit také pouze fyzická osoba, nikoliv osoba právnická. Vzhledem k tomu, že právnické osoby nemají možnost elektronicky podepsat dokument zaručeným elektronickým podpisem a zaručit tím jeho pravost, vznikla původně elektronická značka, která byla posléze nařízením eIDAS nahrazena elektronickou pečetí.

Elektronická pečeť do určité míry alternuje účelu elektronického podpisu, avšak pouze v rozsahu zajištění integrity a označení původce dokumentu nebo zprávy, nikoliv projevu vůle navenek. Podmínkou možnosti připojení elektronické pečeti k dokumentu je, aby právnická osoba byla jeho původcem, což je jeden z rozdílů oproti dříve používaným elektronickým značkám, které mohly být připojeny i na cizí dokumenty za účelem ověření jejich pravosti.[28]

Další zásadní odlišnost od elektronického podpisu se objevuje v procesu vytváření elektronické pečetě. Zatímco elektronický podpis připojuje k dokumentu fyzická osoba manuálně, elektronická pečeť může být připojena také softwarem

[27] HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *EPRAVO.CZ: Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. 22. 1. 2020 [cit. 22.1.2022]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

[28] PETERKA, Jiří. Kvalifikované elektronické pečeti: bude čím je vytvářet?. *Lupa.cz: server o českém internetu* [online]. [cit. 29.1.2022]. Dostupné z: https://www.lupa.cz/clanky/kvalifikovane-elektronicke-peceti-bude-cim-je-vytvaret/

bez účasti člověka v rámci určitého automatizovaného procesu nebo hromadné úpravy dokumentů.[29]

Elektronické pečeti se dělí na více druhů dle stupně zabezpečení a důvěryhodnosti, přičemž hlavní druhy ve své podstatě kopírují druhy elektronických podpisů, o nichž byla řeč v předchozích podkapitolách. Konkrétně se jedná o:

- „prostou“ elektronickou pečeť
- zaručenou elektronickou pečeť
- zaručenou elektronickou pečeť založenou na kvalifikovaném certifikátu
- kvalifikovanou elektronickou pečeť, založenou na kvalifikovaném certifikátu vytvořenou pomocí kvalifikovaného hardwarového prostředku

Stejně jako u elektronických podpisů i zde je povinnost pro veřejnoprávní orgány využívat k zapečetění výhradně kvalifikovanou elektronickou pečeť založenou na kvalifikovaném certifikátu vytvořenou pomocí kvalifikovaného prostředku. V souvislosti s činností státní správy a územní správy je důležité připomenout, že přidáním elektronické pečeti nedochází k nahrazení účelu úředního razítka. Praktickou využitelnost elektronické pečeti z pohledu veřejnoprávních orgánů lze spatřovat především v operacích, kdy nedochází k právnímu jednání úřední osoby vůči protistraně. Typickým příkladem možnosti použití elektronické pečeti je potvrzení přijetí dokumentu, doložka autorizované konverze dokumentu nebo výpis z informačního systému veřejné správy.[30]

1.5 Časové razítko

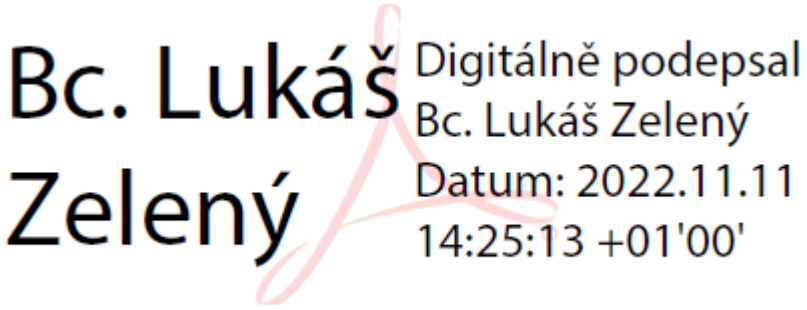
Základní způsoby zajištění integrity, ověření původu a identifikace uživatele v souvislosti s problematikou podepisování elektronických dokumentů a zpráv jsme si již nastínili v předchozích kapitolách, avšak ještě musíme vyřešit otázku, jakou roli hraje aspekt času a jaké máme způsoby jeho doložení?

[29] VRÁNA, Ivo. Elektronická pečeť dle eIDAS – jak a co vlastně pečetit?. *Nástroje pro multifaktorovou autentizaci a PKI infrastrukturu – ProID* [online]. [cit. 23.1.2022]. Dostupné z: https://proid.cz/elektronicka-pecet-dle-eidas-jak-a-co-vlastne-pecetit/

[30] VRBA, Roman. *Metodický pokyn k elektronickým podpisům a pečetím pro veřejnoprávní původce* [online]. 12. 4. 2019 [cit. 29.1.2022]. Dostupné z: https://www.mvcr.cz/soubor/metodicky-material-k-problematice-peceteni-zsvd.aspx

Připojení zaručeného nebo uznávaného elektronického podpisu k dokumentu s sebou nese mimo jiné informaci o datu a času elektronického podepsání. Jedná se však pouze o údaje převzaté ze systému konkrétního zařízení. Takové údaje mohou být v závislosti na nastavení systémového času v době podpisu neaktuální, nepřesné, ba dokonce úmyslně zkreslené (viz obrázek 8). Platnost kvalifikovaného elektronického podpisu a pečeti bývá omezena a je zpravidla nastavena na 1 rok. Jakmile platnost elektronického podpisu pomine, nelze garantovat ani platnost podepsaného dokumentu.[31]

Prodloužení platnosti elektronického podpisu lze docílit přidáním tzv. časového razítka (TS – Time Stamp) vydaného autoritou časových razítek (TSA – Time Stamping Authority). Kvalifikované časové razítko je datová zpráva vydaná kvalifikovaným poskytovatelem certifikačních služeb, která důvěryhodně spojuje data v elektronické podobě s konkrétním časovým okamžikem a zaručuje existenci dokumentu v okamžiku orazítkování.[32]



Obrázek 8 – Ukázka uměle upraveného časového údaje elektronického podpisu na základě změny systémového nastavení času (Adobe Acrobat Reader DC)

Časové razítko je možné použít společně s kvalifikovaným elektronickým podpisem (popř. elektronickou pečetí), avšak není možné jej s elektronickým podpisem zaměňovat, jelikož jeho účelem není právní jednání, nýbrž důkaz o nezpochybnitelné existenci dokumentu v daném čase. Při aplikaci kvalifikovaného časového razítka je nezbytně nutné připojení k internetu, jelikož vytvoření časového razítka je v gesci autority časových razítek, nikoliv samotného

[31] Časové razítko. *EARCHIVACE.CZ* [online]. [cit. 29.1.2022]. Dostupné z: http://www.earchivace.cz/technologie/casove-razitko/

[32] viz str. 55, BUDIŠ, Petr, Ludwig GRAMLICH a Bohumír ŠTĚDROŇ. *Sichere elektronische Kommunikation: Rechtliche, wirtschaftliche und technische Perspektiven*. Chemnitz: GUC - Verlag der Gesellschaft für Unternehmensrechnung und Controlling, 2009. ISBN 978-3-934235-77-9.

uživatele (jako tomu je například při použití elektronického podpisu), která je zárukou přesného času. Platnost elektronického podpisu lze prostřednictvím časového razítka prodloužit zpravidla o 5 let, přičemž i tuto dobu je možné dále prodlužovat přidáváním dalších časových razítek.[33]

Časová razítka hrají důležitou roli také v oblasti archivnictví a spisové služby, jelikož subjekty veřejného sektoru s ohledem na stupňující se požadavky ukládání a archivaci dokumentů v elektronické podobě musí na základě zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů připojit údaje prokazující existenci dokumentu v čase, k čemuž slouží právě kvalifikovaná časová razítka.[34] Schéma doporučeného postupu jednání pověřených pracovníků veřejné správy včetně používání časových razítek je patrné z obrázku 9 viz níže.[35]

Obrázek 9 – Schéma doporučeného postupu jednání veřejné správy vůči třetím osobám

[33] Časová razítka. *Česká pošta* [online]. [cit. 29.1.2022]. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/casova-razitka
[34] viz str. 158–160, DONÁT, Josef, Martin MAISNER a Robert PIFFL. *Nařízení eIDAS: komentář.* Praha: C.H. Beck, 2017. ISBN 978-80-7400-633-3.
[35] Zdroj obrázku 9: VRBA, Roman. *Metodický pokyn k elektronickým podpisům a pečetím pro veřejnoprávní původce* [online]. 12. 4. 2019 [cit. 29.1.2022]. Dostupné z: https://www.mvcr.cz/soubor/metodicky-material-k-problematice-peceteni-zsvd.aspx

1.6 Související právní úprava

Pomyslným základním kamenem elektronického podpisu a navazující problematiky elektronického právního jednání byl v rámci českého právního řádu zákon pocházející z počátku milénia č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, který vycházel z původní Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. 12. 1999 o zásadách Společenství pro elektronické podpisy. Tento zákon byl 19. 9. 2016 společně se souvisejícím zákonem č. 440/2004 Sb., kterým se mění zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů zrušen v důsledku nabytí platnosti stěžejního Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES dne 1. 7. 2016.

Výše zmíněné nařízení obecně známé pod přezdívkou eIDAS (electronic IDentification, Authentication and trust Services) adaptovala Česká republika do právního řádu prostřednictvím zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, jež nabyl platnosti a účinnosti dne 19. 9. 2016, dále zákonem č. 250/2017 Sb., o elektronické identifikaci, který je účinný od 1. 7. 2018. Kromě přijetí základních zákonů proběhla implementace nařízení také prostřednictvím zakotvení prováděcích aktů k nařízení eIDAS.[36]

Ze všech základních druhů elektronických podpisů nařízení eIDAS staví na nejvyšší úroveň kvalifikovaný elektronický podpis, který je zároveň na stejné úrovni jako standardní vlastnoruční podpis (bez úředního nebo notářského ověření). V oblasti soukromoprávních vztahů je na roveň vlastnoručního podpisu postaven jakýkoliv elektronický podpis (např. prostý elektronický podpis v podobě uvedení jména v hlavičce e-mailu), což může být přinejmenším diskutabilní, jelikož míra důvěryhodnosti zde značně strádá.[37]

---

[36] SLUŽBY VYTVÁŘEJÍCÍ DŮVĚRU A ELEKTRONICKÁ IDENTIFIKACE: eIDAS, služby vytvářející důvěru a elektronická identifikace. *Ministerstvo vnitra České republiky* [online]. 14. 4. 2020 [cit. 23.1.2022]. Dostupné z: https://www.mvcr.cz/clanek/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace.aspx

[37] KORBEL, František a Dalibor KOVÁŘ. Nařízení eIDAS konečně adaptováno do českého práva, zákon o elektronickém podpisu končí. *Právní prostor* [online]. 13. 10. 2016 [cit. 23.1.2022]. Dostupné z: https://www.pravniprostor.cz/clanky/procesni-pravo/narizeni-eidas-konecne-adaptovano-do-ceskeho-prava-zakon-o-elektronickem-podpisu-konci

Určitá benevolence nastavení účinků elektronických podpisů v jednotlivých státech zůstala zachována, čehož využívá například i Česká republika, která odlišuje formu uznávaného elektronického podpisu od kvalifikovaného elektronické podpisu, čímž v podstatě snižuje nároky na komunikaci fyzických osob s orgány státní správy a samosprávy, jelikož občané nemusí striktně využívat nejvyšší formu, tedy kvalifikovaný elektronický podpis, ale postačí uznávaný elektronický podpis. Pouze uznávaný elektronický podpis však není dostatečný z opačné strany, kdy osoba jednající za veřejnoprávní orgán musí disponovat kvalifikovaným elektronickým podpisem.[38]

Pokud se na nařízení eIDAS podíváme optikou zaměřenou výhradně na problematiku elektronického podpisu, hlavním cílem zákonodárců bylo primárně sjednotit používání a uznávání elektronických podpisů soukromoprávních a veřejnoprávních subjektů napříč jednotlivými členskými státy, což může výrazně přispět k pokračování budování jednotného evropského trhu.

V návaznosti na podkapitolu „Zaručený elektronický podpis“ považuji za důležité zdůraznit jistý nesoulad definice zaručeného elektronického podpisu dle nařízení eIDAS s jeho technickým zpracováním. Dle článku 26 nařízení eIDAS *zaručený elektronický podpis musí splňovat tyto požadavky:*

a) *je jednoznačně spojen s podepisující osobou;*
b) *umožňuje identifikaci podepisující osoby;*
c) *je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a*
d) *je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.*[39]

Zejména první dva body označené písmeny a) a b) mohou být matoucí, jelikož definice počítá s identifikací osoby a spojením podpisu s podepisovatelem, avšak certifikát pro „pouhý“ zaručený elektronický podpis lze technicky vytvořit svépomocí i na jméno odlišené od podepisující osoby. Jako příklad mohu uvést

[38] Zákon č. 297/2016 Sb., *o službách vytvářejících důvěru pro elektronické transakce* v posledním znění
[39] 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* v posledním znění

mnou vytvořený testovací certifikát zaručeného elektronického podpisu Jaromíra Jágra (viz obrázek 3, str. 18). Dle mého názoru definice zaručeného elektronického podpisu v aktuálním znění dle nařízení eIDAS odpovídá z technického hlediska možná o něco více zaručenému elektronickému podpisu založeném na kvalifikovaném certifikátu než pouhému zaručenému elektronickému podpisu.

2. Zabezpečení elektronického podpisu

V návaznosti na první kapitolu této práce, jejímž obsahem byla primárně východiska elektronického podpisu včetně souvislostí s dalšími objekty elektronického právního jednání a elektronické komunikace, se nyní podíváme blíže na technologické zajištění elektronického podpisu se zaměřením na prvky a funkce, které mají význam především pro jeho zabezpečení.

Pokud se podíváme na vizuální podobu elektronického podpisu na obrazovce zařízení pouhým okem, zpravidla uvidíme podobný vzhled a informace, které je možné vyčíst z běžného vlastnoručního podpisu. V případě „prostého“ elektronického podpisu můžeme vidět například jméno a příjmení napsané standardně v textovém editoru nebo křivku v grafické podobě připomínající trajektorii psací potřeby u podpisu vlastnoručního. Vizuální vzhled zaručeného nebo kvalifikovaného elektronického podpisu v dokumentu zpravidla může obsahovat jméno, příjemní, titul, datum podpisu a informaci o tom, že se jedná o elektronický/digitální podpis. Pro běžné uživatele jsou tyto informace dostačující a častokrát se s nimi spokojí, ale ve skutečnosti elektronický podpis tvoří spousta dalších údajů založených na matematických a kryptografických principech, které zajišťují požadované vlastnosti, jakými jsou zajištění integrity, identifikace osoby a tak podobně.

2.1 Symetrická a asymetrická kryptografie

Než se dostaneme k samotnému objasnění technologie vytváření elektronického podpisu, je vhodné nejprve nastínit informace o vědě zvané kryptologie, na jejíž disciplínách jsou elektronické podpisy ve své podstatě postaveny. Kryptologie je věda zabývající se problematikou ochrany a utajování obsahu zpráv nebo dokumentů za pomocí kryptografie (šifrování) a kryptoanalýzy (dešifrování). Základní funkcí kryptografie je šifrování vstupních dat (např. obsahu zprávy nebo dokumentu) do takové podoby, aby je neoprávněná osoba nemohla za normálních okolností bez dalších prostředků číst.[40]

[40] viz str. 4, DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1

Zašifrování dat probíhá na základě specifického postupu zvaného šifrovací algoritmus, přičemž hlavním účelem takového procesu je snaha o zachování důvěrnosti dat a ochranu před neoprávněným čtením. Aby data mohla být zašifrována a následně dešifrována (odkryta) osobou oprávněnou, musí kromě šifrovacího algoritmu, který může být všeobecně známý, být k dispozici také specifický klíč, u nějž je třeba zajistit bezpečné uchování v tajnosti. Kryptografii můžeme dále rozdělit na symetrickou a asymetrickou.[41]

Symetrické šifrování

Jedním z nejjednodušších způsobů, jak převést data (např. text dokumentu) do utajené a nečitelné podoby, je využití symetrického šifrování. Šifrování a následné dešifrování prostřednictvím metod a technik symetrické kryptografie probíhá, jak již název napovídá, na základě jednoho symetrického tajného klíče a příslušného šifrovacího algoritmu.[42]

Výhodou symetrického šifrování je především nízká náročnost a vyšší rychlost daného procesu. Symetrické šifrování můžeme využít například k zabezpečení dat za účelem jejich následného uchování, jelikož tajný klíč v takovém případě zůstává stále u původce a nevzniká tak riziko odposlechu během komunikace. Naopak nevýhodou může být potřeba transferu symetricky šifrovaných dat jinému příjemci, jelikož tajný klíč je nutné předat tak, aby jej nemohla odposlechnout neoprávněná osoba. V takovém případě je třeba využít zabezpečené komunikace mezi příjemcem a odesilatelem, aby nedošlo k nežádoucímu odposlechu tajného klíče a případnému dešifrování dat útočníkem. Pokud se již tajný klíč podaří bezpečně předat a bude jej mít v držení příjemce i odesilatel, nabízí se další riziko v podobě odcizení tajného klíče útočníkem jedné ze zúčastněných osob, a tím pádem i potencionální ohrožení šifrovaných dat.[43]

---

[41] viz str. 131, HUSEBY, Sverre H. *Zranitelný kód*. Brno: Computer Press, 2006. ISBN 80-251-1180-6.
[42] viz str. 56–57, STALLINGS, William. *Cryptography and network security: principles and practice*. 5th ed. Boston: Prentice Hall, 2011. ISBN 978-0-13-705632-3.
[43] DURČÁK, Pavel. Symetrické a asymetrické šifrování. *NaPočítači.cz* [online]. 18. 9. 2018 [cit. 29.1.2022]. Dostupné z: https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/

Asymetrické šifrování

Základní nevýhodu symetrického šifrování, která spočívá v náročnějším zajištění bezpečného předání tajného klíče v rámci komunikace, může vyřešit asymetrická kryptografie, jež využívá místo jednoho tajného klíče dvojici veřejného a soukromého klíče, které jsou na sebe vzájemně navázány a tvoří tzv. klíčový pár. Jeden z dvojice klíčů se použije k zašifrování dat (zpravidla veřejný klíč) a druhý naopak k jejich dešifrování (zpravidla soukromý klíč). Není vyloučena ani možnost využít klíče obráceně tzn. soukromý klíč k zašifrování dokumentu a veřejný klíč k jeho dešifrování, což odkrývá riziko odposlechu v rámci komunikace, avšak využitelnost je například právě u elektronického podepisování, jak si vysvětlíme později.[44]

Vzhledem k tomu, že soukromý klíč není odvoditelný z klíče veřejného, veřejný šifrovací klíč může být volně dostupný pro všechny účastníky komunikace a je možné jej bez obav předávat i prostřednictvím nezabezpečené komunikace. Opačná odvoditelnost veřejného klíče od klíče soukromého možná je. S ohledem na vyšší složitost celého asymetrického šifrovacího procesu můžeme spatřovat nevýhodu v náročnějším způsobu výpočtu a ve větší časové nákladnosti.[45]

2.2 Hashovací funkce

Další významnou technologií využívanou nejen při vytváření elektronického podpisu, ale také při ukládání hesel do databází, je tzv. hashovaní. Hashovací funkce slouží k převodu řetězce znaků variabilní délky (např. textu dokumentu) na řetězec znaků s fixní délkou. Výstupní řetězec se nazývá hash a jedná se o jakýsi digitální otisk vstupního textu, který obsahuje směs číslic a písmen. Výhodou hashovaní je jednosměrnost dané funkce, díky které je možné ze vstupního textu vytvořit výstupní hash, ale opačný proces z výstupního řetězce znaků vytvořit původní text možné není.[46]

---

[44] Kapitola 6 – Šifrování a elektronický podpis. *Univerzita Tomáše Bati ve Zlíně* [online]. [cit. 30.1.2022]. Dostupné z: https://www.utb.cz/cvt/bezpecnost-sifrovani-elektronicky-podpis/

[45] DURČÁK, Pavel. Symetrické a asymetrické šifrování. *NaPočítači.cz* [online]. 18. 9. 2018 [cit. 29.1.2022]. Dostupné z: https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/

[46] viz str. 352–353, STALLINGS, William. *Cryptography and network security: principles and practice*. 5th ed. Boston: Prentice Hall, 2011. ISBN 978-0-13-705632-3.

Jelikož se jedná o jednosměrnou funkci a nelze tedy vstup ověřit převedením hashe do původní podoby, pro spolehlivé zjištění vstupního textu se musí dojít ke shodě výstupů, která v logické návaznosti zaručí také shodu vstupů. V případě aplikace hashovací funkce na delší text se můžeme bavit také o přidané hodnotě v podobě jakési komprese textu a velikosti, jelikož výstupní délka hashe je vždy pevná (např. z textu o délce několik stovek nebo tisíců znaků pomocí hashovací funkce SHA256 lze vytvořit řetězec o délce pouhých 64 znaků).

2.3 Mechanismus elektronického podpisu

Problematika šifrování a hashování byla v předchozích kapitolách nastíněna především z důvodu nepostradatelnosti jednotlivých funkcí při tvorbě elektronického podpisu. Vytvoření zaručeného elektronického podpisu je založeno na kombinaci metod asymetrické kryptografie a hashování, přičemž využití jednotlivých metod má svá specifika.

Standardně v rámci aplikace metod asymetrické kryptografie zpravidla dochází k využívání veřejného klíče k zašifrování dat (např. dokumentu nebo zprávy) a soukromého klíče k jejich následnému dešifrování. Technicky lze samozřejmě využít klíčový pár také opačným způsobem, kdy data zašifrujeme soukromým klíčem a dešifrujeme klíčem veřejným, což však na první pohled není příliš výhodné, jelikož to dává možnost dešifrovat data veřejným klíčem, který bývá předáván společně s dokumentem, nebo dokonce může být plně přístupný veřejnosti například na on-line serveru. Pro případy standardního užití šifrování například k zabezpečení dat při ukládání nebo přenosu je samozřejmě výhodnější dešifrovat soukromým klíčem, avšak pro potřeby elektronického podpisu tomu tak není.

Účelem elektronického podpisu není zabezpečit data (dokument nebo zprávu) proti neoprávněnému čtení, zcizení nebo zajištění jejich bezpečného uložení, ale cílem je především ověřit identitu podepisující osoby a zajistit integritu dat, čehož právě je možné docílit kombinací hashovací funkce a asymetrické kryptografie.

Na proces vytváření elektronického podpisu lze pohlížet z více úhlů pohledu. Doposud jsme hovořili primárně o metodách a funkcích založených na matematických výpočtech a informačních technologiích, prostřednictvím kterých

dochází k elektronickému podepisování. Jak ale v praxi tyto nástroje použít tak, aby vše fungovalo a plnilo svůj účel?

Jak již z logiky věci vyplývá, jedná se o úkony, které musí někdo nebo něco realizovat za přesně stanovených podmínek a v předem definovaném pořadí. Běžní uživatelé elektronického podpisu nedokáží technicky všechny potřebné procesy provést, tudíž k jejich realizaci potřebují další prostředky, které na základě požadavku značnou část úkonů provedou za ně. Podle autora Jiřího Peterky můžeme takové prostředky rozdělit na:

- Univerzální prostředky – shodné a přístupné pro všechny uživatele
- Individuální prostředky – pro každého uživatele odlišné

Mezi univerzální prostředky můžeme zařadit především softwarové vybavení určené pro vytváření elektronického podpisu. Uživateli pak stačí pouze vydat pokyn k podepsání a aplikace na základě předdefinovaných algoritmů dokáže provést jednotlivé kroky sama. Univerzalita tkví v tom, že jediný program (např. Adobe Acrobat) může využívat široká skupina uživatelů k jednomu konkrétnímu účelu. Do skupiny individuálních prostředků se řadí certifikáty a soukromé klíče, které jsou pro každého uživatele jedinečné. Takové prostředky není možné je nahradit žádným jiným univerzálním prostředkem.[47]

Fáze vytvoření podpisu

Prvním krokem technického postupu vytvoření zaručeného elektronického podpisu je aplikace hashovací funkce na dokument, díky čemuž získáme z podepisovaného dokument hash. Vzhledem k tomu, že při hashování dochází k převodu dat o různé délce nebo velikosti na hash s pevnou délkou, je třeba brát na vědomí riziko kolize. S určitou pravděpodobností tedy může nastat situace tzv. kolize dokumentů, kdy dva dokumenty s rozdílným obsahem budou mít stejný hash. Aby se takové riziko maximálně snížilo, je třeba zajistit co největší časovou náročnost na výpočet stejného hashe tak, aby se nikomu nevyplatilo pokusit se kolizi dokumentů vytvořit úmyslně.[48]

[47] viz str. 66–68, PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8
[48] viz str. 70–73, tamtéž

Jakmile je dokument převeden na hash, nastává fáze jeho zabezpečení prostřednictvím metody asymetrického šifrování. Zašifrování hashe probíhá pomocí soukromého klíče, díky kterému jej může zašifrovat pouze osoba, která má tento klíč k dispozici. Z hlediska dosažení jednoho z účelů elektronického podpisu, kterým je identifikace podepisující osoby, je nutné k zašifrování použít soukromý klíč, jehož párovým protějškem bude veřejný klíč ověřený kvalifikovanou certifikační autoritou, jimiž se budeme zaobírat v dalších kapitolách této práce. Zašifrovaný hash se následně přiloží k originálnímu dokumentu, čímž fakticky dochází k jeho „podepsání“, a společně se postoupí příjemci.[49]

Fáze ověření platnosti podpisu

Druhá strana po přijetí podepsaného dokumentu by měla nejprve ověřit platnost celého podpisového procesu. Prvním krokem procesu ověření platnosti podpisu je kontrola zachování integrity dokumentu, k čemuž se opět využívá primárně hashovací funkce. Příjemce, respektive software k tomu určený, nejprve originální dokument převede na hash. Současně s tím je třeba původní hash vytvořený odesílatelem dešifrovat prostřednictvím veřejného klíče. Následuje komparace původně vytvořeného hashe odesílatelem a nového hashe od příjemce, přičemž jejich shoda zajišťuje záruku neměnnosti dokumentu od okamžiku podepsání dokumentu až do chvíle jeho ověření.

Ověření identity podepisující osoby, které se týká pouze zaručených elektronických podpisů založených na kvalifikovaném certifikátu, probíhá na základě informace o důvěryhodnosti certifikační autority, která certifikát obsahující veřejný klíč vystavila. Pokud se totiž jedná o kvalifikovanou certifikační autoritu, znamená to, že před vystavením certifikátu došlo k ověření totožnosti podepisujícího a tím pádem (za předpokladu, že soukromý klíč opravdu zůstane v jeho držení) na základě kontroly platnosti certifikátu dochází k ověření identity a autenticity podepisující osoby.[50]

[49] Digitální podpis. *EARCHIVACE.CZ* [online]. [cit. 5.2.2022]. Dostupné z: http://www.earchivace.cz/technologie/digitalni-podpis/

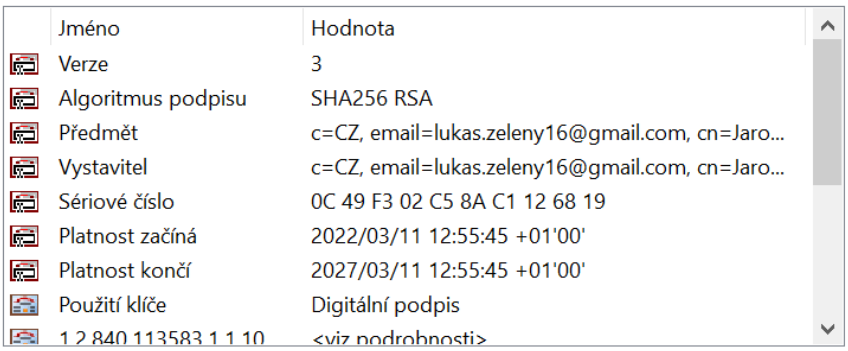
[50] DURČÁK, Pavel. Symetrické a asymetrické šifrování. *NaPočítači.cz* [online]. 18. 9. 2018 [cit. 5.2.2022]. Dostupné z: https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/

2.4 Certifikáty

Jak již několikrát bylo zmíněno, velmi důležitou roli u elektronických potažmo digitálních podpisů hrají certifikáty. Z pohledu technologické struktury elektronického podpisu je certifikát důležitý především kvůli veřejnému klíči, jehož je nositelem a uchovatelem. Kromě veřejného klíče však certifikát obsahuje řadu dalších důležitých informací o vlastníkovi nebo certifikační autoritě, která certifikát vystavila. Podle některých autorů certifikát lze do určité míry přirovnat k dokladu totožnosti, přičemž hlavním rozdílem je forma. Zatímco občanský průkaz nebo pas je zpravidla vydáván fyzicky v tištěné podobě, certifikát je v podstatě elektronický soubor dat s určitou strukturou.

Samotné certifikáty obsahují řadu informací, které jsou důležité především pro ověření jejich platnosti a důvěryhodnosti (viz obrázek 10). Mezi základní informace, které lze z certifikátu vyčíst, můžeme zařadit:

- **Verze** – varianta použité datové struktury
- **Algoritmus podpisu** – označení algoritmu použitého k asymetrickému šifrování
- **Předmět** – údaje o vlastníkovi certifikátu
- **Vystavitel** – údaje o certifikační autoritě
- **Sériové číslo** – jedinečný identifikátor certifikátu
- **Datum a čas začátku platnosti** – přesné vymezení začátku intervalu platnosti včetně časového pásma
- **Datum a čas konce platnosti** – přesné vymezení konce intervalu platnosti včetně časového pásma
- **Veřejný klíč** – hodnota veřejného klíče
- **Použitelnost veřejného klíče** – účel certifikátu



Jméno	Hodnota
Verze	3
Algoritmus podpisu	SHA256 RSA
Předmět	c=CZ, email=lukas.zeleny16@gmail.com, cn=Jaro...
Vystavitel	c=CZ, email=lukas.zeleny16@gmail.com, cn=Jaro...
Sériové číslo	0C 49 F3 02 C5 8A C1 12 68 19
Platnost začíná	2022/03/11 12:55:45 +01'00'
Platnost končí	2027/03/11 12:55:45 +01'00'
Použití klíče	Digitální podpis
1.2.840.113583.1.1.10	<viz podrobnosti>

Obrázek 10 – Ukázka základních informací o nedůvěryhodném certifikátu

Certifikáty můžeme pomyslně rozdělit do vícero kategorií například dle svého účelu, vystavitele nebo vlastníka. Základně lze certifikáty rozčlenit na důvěryhodné certifikáty, které může vystavit pouze důvěryhodná certifikační agentura, a certifikáty nedůvěryhodné, které může vystavit kdokoliv z nás. Vzhledem k tomu, že certifikáty hrají důležitou roli především z pohledu ověření identity podepisující osoby, zaměříme se primárně na důvěryhodné certifikáty, na kterých je uznávaný elektronický podpis založen. Certifikáty můžeme dále dle typu vlastníka rozdělit na osobní, které patří vždy konkrétní fyzické osobě, a certifikáty systémové určené pro technická zařízení. Certifikáty jsou součástí určité hierarchické struktury, přičemž základ tvoří tzv. kořenový certifikát. Kvalifikovanému certifikátu vydanému určité osobě je nadřazen vždy kořenový certifikát akreditované certifikační autority, který důvěru zastřešuje.

Kvalifikovaný certifikát

Aktuálně nejvyšší formou certifikátu veřejného klíče, který může být k elektronickému podpisu použit, je tzv. kvalifikovaný certifikát. Kvalifikovaný certifikát je základním a stěžejním komponentem kvalifikovaného a uznávaného elektronického podpisu neboli zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu. Kvalifikovaný certifikát se od jiných certifikátů odlišuje především tím, že jej mohou vydávat pouze autorizované certifikační autority. Kvalifikované certifikáty jsou založeny na nutnosti ověření totožnosti vlastníka, které probíhá během procesu žádosti o daný certifikát. Díky tomu kvalifikované certifikáty slouží primárně k ověření identity a zajištění integrity dat, což dává možnost vlastníkům certifikátů prostřednictvím nich komunikovat se státními orgány a dalšími veřejnoprávními institucemi. Naopak primárním účelem kvalifikovaných certifikátů není šifrování dat, k čemuž se využívají spíše komerční certifikáty.[51]

[51] Jaký je rozdíl mezi kvalifikovaným a komerčním certifikátem?. *Digitální Podpis* [online]. [cit. 6.2.2022]. Dostupné z: https://www.digitalni-podpis.cz/rozdil-mezi-komercnim-a-kvalifikovanym-certifikatem/

Komerční certifikát

Další velmi rozšířenou skupinou certifikátů jsou komerční certifikáty, které se při elektronickém podepisování prakticky nevyužívají, jelikož jejich primární účel ve své podstatě kontrastuje s účelem kvalifikovaného certifikátu. Komerční certifikáty jsou určeny například k zajištění bezpečné komunikace, zvýšení zabezpečení při přihlašování nebo k šifrování zpráv. Komerčních certifikátů je nepřeberné množství od různých známých i neznámých vystavitelů, tudíž je třeba si uvědomit, že ne všechny takové certifikáty budou uznávané státními a veřejnoprávními institucemi.[52]

Oblast využití certifikátu je poměrně široká a rozhodně se nezaměřuje pouze na problematiku elektronického podpisu. Velmi rozšířené jsou například bezpečnostní certifikáty, které šifrují komunikaci mezi klientem a serverem v rámci prohlížení nebo jiných interakcí na různých webových stránkách. Jedná se o tzv. SSL nebo TLS certifikáty, které zabezpečují šifrování komunikace prostřednictvím asymetrické kryptografie a zabraňují nežádoucímu odposlechu dat útočníky během přenosu. Běžný návštěvník webových stránek se tak s těmito typy certifikátů setkává takřka na denní bázi, aniž by o tom věděl.

2.5 Certifikační autority

Jak je možné usoudit z předcházející části práce, problematika certifikačních autorit je s tématem předchozí kapitoly, která se týkala certifikátů, velmi úzce provázána. Certifikační autority (CA – Certification Authority) jsou zásadními subjekty procesu distribuce certifikátu veřejného klíče. Důvěryhodnost certifikátu se opírá a důvěryhodnost samotné certifikační autority, tudíž se jedná o tzv. princip přenosu důvěry.[53]

Kromě akreditovaných a kvalifikovaných certifikačních autorit však existuje také celá řada globálně nedůvěryhodných certifikačních autorit, které mohou fungovat například pouze na lokální bázi. Nedůvěryhodnou certifikační autoritou se ve své podstatě může stát kdokoliv z nás tím, že sami sobě nebo někomu

[52] Komerční certifikát. *Elektronický Podpis* [online]. [cit. 6.2.2022]. Dostupné z: https://www.elektronickypodpis.cz/komercni-certifikat/

[53] Vyznejte se v elektronické archivaci III: Princip elektronického podpisu. *EDIZONE: Informační portál* [online]. 17. 03. 2016 [cit. 6.2.2022]. Dostupné z: https://www.edizone.cz/technologie-a-trh/vyznejte-se-v-elektronicke-archivaci-iii-princip-elektronickeho-podpisu/

jinému vystavíme vlastní certifikát pro elektronický podpis. Stejně tak globálně nedůvěryhodnou, ale samozřejmě lokálně (v rámci dané společnosti) důvěryhodnou, certifikační autoritu mohou provozovat například zaměstnavatelé a vystavovat certifikáty pro své zaměstnance pro potřeby interních procesů.[54]

Z pohledu významu pro uznávaný nebo kvalifikovaný elektronický podpis je důležité zaměřit se primárně na akreditované a kvalifikované certifikační autority, které mají pravomoc vydávávat na základě žádosti za předpokladu ověření totožnosti kvalifikované certifikáty pro elektronické podpisy. Certifikační autorita ve vztahu podepisující osoby a protistrany vystupuje jako třetí nezávislá strana (důvěryhodný prostředník), která za se za podepisující osobu zaručí na základě své důvěryhodnosti, díky čemuž protistrana nemusí mít žádné pochybnosti o nedůvěryhodnosti certifikátu podepisující osoby.

Hierarchie certifikačních autorit v praxi reflektuje hierarchii samotných certifikátů, kdy může existovat kořenová certifikační autorita (např. PostSignum Root QCA 4), která disponuje podřízenými autoritami (např. PostSignum Qualified CA 4 a PostSignum Public CA 4).[55] Finální certifikát vystavovaný fyzické nebo právnické osobě podepisuje certifikační autorita svým soukromým klíčem, čímž dochází k potvrzení jeho pravosti.

Dle nařízení eIDAS lze důvěryhodnou certifikační autoritu podřadit pod právně přesnější pojem poskytovatel služeb vytvářející důvěru. Činnost poskytovatelů služeb vytvářející důvěru může vykonávat pouze subjekt, který úspěšně absolvoval posouzení shody (certifikaci) a byl zapsán do veřejného rejstříku důvěryhodných poskytovatelů služeb vytvářejících důvěru (tzv. Trusted List).[56]

Seznam těchto subjektů splňujících všechny požadavky můžeme nalézt na webových stránkách orgánu dohledu, kterým je v případě České republiky Ministerstvo vnitra, a také na webu Evropské komise. Ke dni 6. 2. 2022 aktuálně

[54] viz str. 42, PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8
[55] viz str. 44–45, tamtéž
[56] BLÜMELOVÁ, Kristina Kadlas. Nařízení eIDAS je základem spolehlivé elektronické identifikace a služeb vytvářejících důvěru. *Technický týdeník* [online]. 25. 10. 2021 [cit. 6.2.2022]. Dostupné z: https://www.technickytydenik.cz/rubriky/ict/narizeni-eidas-je-zakladem-spolehlive-elektronicke-identifikace-a-sluzeb-vytvarejicich-duveru_54320.html

mezi kvalifikované poskytovatele služeb vytvářející důvěru dle nařízení eIDAS patří subjekty uvedené v následující Tabulce 1.[57]

Tabulka 1 – Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru

Kvalifikovaní poskytovatelé služeb vytvářejících důvěru	**Kvalifikované služby**
První certifikační autorita, a. s.	Vydávání kvalifikovaných certifikátů pro elektronické podpisy Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí Vydávání kvalifikovaných certifikátů pro elektronické pečetě Vydávání kvalifikovaných elektronických časových razítek Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek
Česká pošta, s. p.	Vydávání kvalifikovaných certifikátů pro elektronické podpisy Vydávání kvalifikovaných certifikátů pro elektronické pečetě Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek Vydávání kvalifikovaných elektronických časových razítek
eIdentity a. s.	Vydávání kvalifikovaných certifikátů pro elektronické podpisy Vydávání kvalifikovaných elektronických časových razítek Vydávání kvalifikovaných certifikátů pro elektronické pečetě
Software602 a. s.	Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí Kvalifikovaná služba uchování kvalifikovaných elektronických podpisů a pečetí
Správa základních registrů,	Vydávání kvalifikovaných certifikátů pro elektronické podpisy Vydávání kvalifikovaných certifikátů pro elektronické pečetě Vydávání kvalifikovaných elektronických časových razítek
SEFIRA spol. s r.o.	Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí

[57] Zdroj tabulky 1: Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru. *Ministerstvo vnitra České republiky* [online]. 6. srpna 2019 [cit. 14.3.2022]. Dostupné z: https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx

3. Využití principů elektronického podpisu v praxi

Předcházející kapitoly teoretické části práce nám odkryly a přiblížily mnoho forem elektronického podpisu, jehož škála využitelnosti je velmi různorodá a patřičně široká, díky čemuž je elektronický podpis nutné považovat za velmi důležitou a nedělitelnou součást každodenního pracovního nebo soukromého života řady z nás.

Praktická využitelnost není pro všechny elektronické podpisy shodná, nýbrž závisí na typu elektronického podpisu, který v rámci procesu podepisování používáme, na konkrétní situaci a také na protistraně, vůči které má mít elektronický podpis účinky. Pokud podepisujeme dokument pouze prostým elektronickým podpisem nebo zaručeným elektronickým podpisem založeným na nekvalifikovaném certifikátu, nelze očekávat jeho akceptaci veřejnoprávními orgány, avšak v určitých případech (zpravidla dohodnutých) je taková forma podpisu přijatelná. Prostý elektronický podpis se hojně využívá při běžné e-mailové komunikaci, nebo například v rychle expandující oblasti internetového prodeje (e-commerce).

Vyšší formy podpisu, mezi které se řadí uznávaný a kvalifikovaný elektronický podpis, mají již podstatně rozšířenější oblast využitelnosti, jelikož jejich zásadní výhodou je možnost využívat je také při komunikaci s úřady. V soukromoprávních vztazích je podobně jako u prostého a zaručeného elektronického podpisu akceptovatelnost uznávaného nebo kvalifikovaného podpisu primárně postavena na vzájemné dohodě smluvních stran, přičemž charakteristickým způsobem použití je podepisování e-mailů, elektronických faktur nebo smluvní dokumentace. Uznávaný a kvalifikovaný elektronický podpis můžeme používat ve veřejnoprávních vztazích typicky k činnostem, které zahrnuje následující demonstrativní výčet:

- Podání dokumentů Finanční správě
    - Přiznání k dani z příjmů fyzických osob
    - Přiznání k DPH
    - Přiznání k silniční dani
    - Přiznání k dani z nemovitosti
- Podání dokumentů České správě sociální zabezpečení

    - Evidenční listy důchodového pojištění
    - Přehled o příjmech a výdajích OSVČ
    - Přihláška k dobrovolné účasti na nemocenském pojištění OSVČ
- Podání dokumentů zdravotním pojišťovnám
    - Přehled o výši daňového základu ze samostatné výdělečné činnosti
- Podání dalším veřejnoprávním orgánům a institucím
    - Žádost o dotace EU
    - Individuální žádost krajskému, městskému nebo obecnímu úřadu [58]

3.1 Výhody a nevýhody elektronického podpisu

I přes to, že výhody a nevýhody elektronického podpisu byly v práci nepřímo několikrát zmiňovány, považuji za vhodné vytvořit konzistentní souhrn hlavních argumentů pro a proti používání zaručeného elektronického podpisu založeném na kvalifikovaném certifikátu.

Mezi hlavní výhodu používání zaručeného elektronického podpisu patří zajištění integrity dokumentu nebo zprávy, díky čemuž vzniká garance neměnnosti datové struktury po podepsání. Protistrana má tedy záruku, že nedošlo k nežádoucí úpravě písemnosti (například kupní smlouvy), která by mohla mít významné negativní dopady. Další hlavní výhodou je ověření identity podepisující osoby, která ujišťuje příjemce, že podepisující osobou je opravdu ta osoba, která se za odesilatele vydává. Uznávaný a kvalifikovaný elektronický podpis je navíc na rozdíl od vlastnoručního podpisu díky používané technologii nenapodobitelný a jednoduše ověřitelný. Vyšší formy elektronického podpisu dále nezpochybnitelně propojují dokument nebo zprávu s podepisující osobou. V neposlední řadě elektronická komunikace s využíváním elektronického podpisu vede k úspoře času a nákladů.

S problematikou elektronického podepisování je samozřejmě spjata také řada nevýhod. Nejvýznamnější nevýhodou jsou náklady na pořízení certifikátu pro uznávaný nebo kvalifikovaný elektronický podpis, které se pohybují v řádu

[58] K čemu lze použít elektronický podpis?. *Digitální podpis.cz* [online]. [cit. 12.2.2022]. Dostupné z: https://www.digitalni-podpis.cz/k-cemu-lze-pouzit-elektronicky-podpis/

několika stovek korun. S tím souvisí i další nevýhoda v podobě relativně krátké platnosti certifikátu, která bývá zpravidla nastavena na jeden rok od vystavení. Další prodloužení platnosti certifikátu je opět zpoplatněno, tudíž náklady na používání elektronického podpisu v dlouhodobém horizontu rostou. Další nevýhoda se týká možnosti ztráty nebo odcizení soukromého klíče, která vystavuje uživatele riziku stát se obětí neoprávněného použití elektronického podpisu jinou osobou. Pokud se podíváme na elektronický podpis z pohledu komunikace, můžeme za nevýhodu označit také nemožnost prokázat doručení elektronicky podepsaného dokumentu jiné osobě bez využití dalšího informačního systému (např. datové schránky). Z osobního úhlu pohledu mohu také za jistou nevýhodu označit relativně nízkou důvěru k elektronickému podpisu mezi širokou veřejností, avšak předpokládám, že tento pocit může vyvolávat především nedostatečné povědomí o této problematice a spousta dalších individuálních aspektů.

3.2 Další nástroje související s elektronickým podpisem

Vzhledem k tomu, že různé formy elektronického podpisu nás provází již od 90. let minulého století, můžeme jej označit za jeden z nejstarších globálně akceptovaných nástrojů při zabezpečení elektronických dokumentů, zpráv a dalších datových formátů před nežádoucími úpravami s další nespornou výhodou v podobě zajištění ověření totožnosti původce. V souvislosti s rychle expandující oblastí digitalizace soukromé a státní správy samozřejmě postupem času přicházely a stále přicházejí další nástroje, které mohou nabídnout podobné, ba dokonce dokonalejší funkce jako uznávaný a kvalifikovaný elektronický podpis. Jedná se však zpravidla o takové nástroje, které funkce elektronického podpisu nenahrazují, avšak je vhodné je používat v souběhu, jelikož do značné míry usnadňují, zjednodušují a zpřehledňují procesy na elektronický podpis nepřímo navazující.

Datové schránky

Ačkoliv se na první pohled může zdát, že informační systém datových schránek s problematikou elektronických podpisů příliš nesouvisí, opak je pravdou. Jedná se totiž o jeden z nejkomplexnějších nástrojů, který za určitých

podmínek dokáže některé funkce elektronického podpisu převzít, a dokonce je rozšířit o oblast vzájemné komunikace subjektů.

Informační systém datových schránek funguje na základě zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů v platném znění, přičemž se jedná o informační systém splňující kritéria stanovená zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů v platném znění. Datovou schránku lze definovat jako určitou interní sekci informačního systému, do níž má přístup pouze držitel nebo jiná osoba s příslušným oprávněním. Účelem informačního systému datových schránek je zefektivnění, zrychlení a snížení nákladů dotčených osob oproti standardnímu způsobu doručovaní v listinné podobě, což zároveň koresponduje s jedním z hlavních důvodů digitalizace veřejné správy.[59]

Prostřednictvím datové schránky může uživatel (fyzická nebo právnická osoba) komunikovat s dalšími uživateli datových schránek, přičemž se může jednat o veřejnoprávní orgány (např. úřady práce, finanční úřady), nebo také jiné soukromoprávní subjekty, které mají datovou schránku zřízenou (např. bankovní instituce, pojišťovny). Smyslem komunikace uživatelů pomocí systému datových schránek je odesílání nebo přijímání dokumentů v elektronické podobě. Datové schránky neslouží primárně k archivaci přijatých a odeslaných zpráv, avšak pro tyto účely je k dispozici nadstandardní služba zvaná „Datový trezor“.

Jedním ze základních principů datových schránek je stejně jako u uznávaných a zaručených elektronických podpisů identifikace odesilatele. Samotný proces odeslání dokumentu formou datové zprávy zajistí identifikaci odesilatele (držitele datové schránky nebo oprávněné osoby), aniž by odesílaný dokument musel být vlastnoručně nebo elektronicky podepsán. Autenticitu dokumentu zajistí přímo systém datových schránek, protože identita držitele byla ověřena v rámci procesu zakládání datové schránky. V tuto chvíli je provozovatel informačního systému datových schránek, kterým je Česká pošta s. p., v obdobném postavení, jaké má důvěryhodná certifikační autorita při vystavení kvalifikovaného certifikátu pro elektronický podpis. Výjimku ze zajištění autenticity

[59] Informační systém datových schránek. *Datové schránky* [online]. [cit. 12.2.2022]. Dostupné z: https://www.datoveschranky.info/o-datovych-schrankach/zakladni-informace

tvoří takové úkony, jejichž provedení vyžaduje zúčastnění více osob (např. více jednatelů za společnost jedná společně). V takových případech nestačí pouhé odeslání dokumentu prostřednictvím datové schránky, ale dokument musí zároveň obsahovat uznávané nebo kvalifikované elektronické podpisy zúčastněných osob.

Další předností datových schránek je jednotné on-line aplikační prostředí dostupné na adrese www.mojedatovaschranka.cz, díky čemuž je možné informační systém využívat i bez jakékoliv dalšího softwarového vybavení s výjimkou internetového prohlížeče, což u uznávaného nebo kvalifikovaného elektronického podpisu možné není, jelikož technické procesy v rámci elektronického podpisu dokumentu provádí softwarový nástroj (např. Adobe Acrobat Reader nebo VerisignIT).

Vzhledem k tomu, že informační systém datových schránek je primárně určen ke komunikaci mezi subjekty, jeho nespornou výhodou jsou aktuální informace o podání, přijetí a doručení, na jejichž základě uživatel získá jistotu a důkaz, že protistrana datovou zprávu obdržela včetně časových údajů. Doložitelný je také obsah datové zprávy, což u listinných poštovních služeb zpravidla není možné. Tato výhoda datové schránky souvisí především s právními účinky doručení.[60]

Oproti zpoplatněným certifikátům pro uznávaný nebo kvalifikovaný elektronický podpis s omezenou časovou platností můžeme další výhodu informačního systému datových stránek spatřovat také v bezplatném zřízení a časově neomezené platnosti datové schránky. Zřízení datové schránky může vycházet buď přímo ze zákona pro orgány veřejné moci, právnické osoby zapsané v obchodním rejstříku, advokáty, daňové poradce a insolvenční správce, nebo na základě žádosti fyzické osoby, podnikající fyzické osoby a právnické osoby, která není zapsána v obchodním rejstříku.[61]

Ačkoliv informační systém datových schránek zajišťuje zabezpečenou a šifrovanou komunikaci mezi odesilatelem a příjemcem, nedokáže zajistit

[60] Elektronický podpis vs. datová schránka: Potřebujete obojí?. *Elektronický podpis* [online]. [cit. 12.2.2022]. Dostupné z: https://www.elektronickypodpis.cz/elektronicky-podpis-vs-datova-schranka-potrebujete-oboji/

[61] Datové schránky. *Ministerstvo vnitra České republiky* [online]. [cit. 12.2.2022]. Dostupné z: https://www.mvcr.cz/clanek/datove-schranky-datove-schranky.aspx

integritu konkrétního dokumentu, což je naopak jedna z hlavních předností zaručených elektronických podpisů. Další určitou nevýhodou je omezená teritoriální využitelnost datových schránek vztahující se pouze na subjekty vykonávající svou činnost v České republice, kdežto kvalifikovaný elektronický podpis je uznávaný a využitelný také v zahraničí.[62]

V neposlední řadě bych rád zdůraznil jistou podobnost principů elektronického podpisu a informačního systému datových schránek v možnosti využitelnosti certifikátu. Datové schránky umožňují kromě standardních metod přihlašování pomocí identity občana, uživatelského jména a hesla, mobilního klíče, SMS nebo bezpečnostního kódu také za účelem zvýšení bezpečnosti využívat přihlášení pomocí komerčního certifikátu. Certifikát může být instalovaný přímo na lokálním uložišti počítače nebo na tokenu či čipové kartě, což je principiálně velmi podobné kvalifikovanému elektronickému podpisu.[63]

Občanský průkaz

I když škála využitelnosti posledních verzí občanských průkazů je díky integrovaným čipům podstatně větší, než se na první pohled může zdát, z osobní zkušenosti si dovolím tvrdit, že spousta občanů přidané hodnoty nevyužívá. Čím to může být? Mohlo by se jednat o nedostatečnou informovanost a marketingovou propagaci ze strany státu nebo jednoduše o nezájem o funkce z oblasti elektronického podepisování a identifikace.

Historie občanských průkazů, jakožto prostředků k prokázání totožnosti, sahá bezpochyby daleko do minulosti, avšak poslední dekáda, ve které došlo k přetvoření obyčejných papírových nosičů občanských průkazů na čipové karty, nám otevřela z pohledu elektronického podepisování nové možnosti.

První příležitost k integraci kontaktního čipu do občanského průkazu byla veřejnosti nabídnuta v roce 2012, kdy občané žádající o občanský průkaz mohli za poplatek takovou možnost využít. Čipová karta však nedisponovala

[62] Elektronický podpis vs. datová schránka: Potřebujete obojí?. *Elektronický podpis* [online]. [cit. 12.2.2022]. Dostupné z: https://www.elektronickypodpis.cz/elektronicky-podpis-vs-datova-schranka-potrebujete-oboji/

[63] Přihlašování certifikátem. *Datové schránky* [online]. [cit. 12.2.2022]. Dostupné z: https://www.datoveschranky.info/doplnkove-sluzby/prihlasovaci-metody/prihlaseni-certifikatem

využitelností ke svému primárnímu účelu, tedy elektronické identifikaci osoby a přihlašování, nýbrž pouze k elektronickému podepisování, jelikož na čipovou kartu bylo možné nahrát pouze kvalifikovaný certifikát. Nahráním kvalifikovaného certifikátu se z občanského průkazu ve své podstatě stal kvalifikovaný prostředek potřebný k vytvoření kvalifikovaného elektronického podpisu.[64] Na základě dostupných dat od obchodního ředitele Státní tiskárny cenin Radka Mušky však zájem o původní variantu občanského průkazu s čipem nebyl příliš velký, jelikož pouze 0,38 % občanů zvolilo čipovou kartu na úkor běžného občanského průkazu.[65]

Další typ elektronického občanského průkazu byl uveden do oběhu v roce 2018, přičemž tato verze již disponuje integrovanými kontaktními čipy bez nutnosti příplatku. Inovace čipové karty kromě zachování a vylepšení původní funkce využitelné především při vytváření kvalifikovaného elektronického podpisu nově nabízí také možnost elektronické identifikace, jelikož čipová karta je již od výroby vybavena identifikačním certifikátem průkazu, který mimo jiné obsahuje základní informace o jeho držiteli. Aktivace elektronické identifikace je však výhradně v kompetenci držitele OP, který se sám může rozhodnout, zdali má o rozšíření zájem nebo nikoliv. Pro správu elektronického občanského průkazu slouží aplikace eObčanka, pomocí které může držitel importovat nebo mazat certifikáty a měnit přístupové kódy.[66]

Vydávání aktuálně nejnovější verze elektronického občanského průkazu bylo spuštěno v roce 2021. Hlavní inovací oproti předchozím verzím OP je přidání biometrických údajů na integrované bezkontaktní čipy na základě nařízení Evropského parlamentu. Cílem přidání dvou otisků prstu a fotografie obličeje má být zefektivnění boje proti terorismu a zjednodušení ověření pravosti občanského

[64] PETERKA, Jiří. Jaké jsou a jak fungují nové elektronické občanky?. *Lupa.cz* [online]. 4. 7. 2018 [cit. 13.2.2022]. Dostupné z: https://www.lupa.cz/clanky/jake-jsou-a-jak-funguji-nove-elektronicke-obcanky/
[65] MUŠKA, Radek. KLÍČ K e-IDENTITĚ. *Magazín Egovernment* [online]. [cit. 13.2.2022]. Dostupné z: https://www.egovernment.cz/soubor/klic-k-e-identite-radek-muska-stc/
[66] PEŠEK, Michal. JE UŽ eIDENTITA ZA DVEŘMI?. *Magazín Egovernment: elektronizace veřejné správy v ČR* [online]. 31. 5. 2018 [cit. 13.2.2022]. Dostupné z: https://www.egovernment.cz/soubor/je-uz-eidentita-za-dvermi-michal-pesek-szr/

průkazu při překračování státních hranic.[67] Funkce předchozí verze občanského průkazu byly zachovány, tudíž je i nadále možné s čipovou kartou prostřednictvím čtečky elektronicky podepisovat dokumenty, autentizovat držitele a přihlašovat se do různých informačních systémů.

Bankovní identita

Budování komplexního národního systému zvaného eGovernment, jehož účelem je zefektivnit fungování veřejné správy za pomocí informačních systémů v návaznosti na technologický pokrok, probíhá již řadu let. Jedny ze základních prvků eGovernmentu jsme již představili v předchozích kapitolách, avšak kromě datových schránek a elektronických občanských průkazů se na pomyslnou scénu teprve před nedávnem dostal nový, relativně jednoduchý, způsob identifikace a autentizace uživatelů prostřednictvím bankovních institucí, díky kterému je možné využívat služby veřejné správy, do kterých bylo mnohdy poněkud složité získat přístup.

Podstata celého projektu s názvem Bankovní identita, který je pod záštitou Ministerstva vnitra, tkví v propojení bankovních institucí se systémy veřejné správy. Před nástupem další varianty přihlašování prostřednictvím bankovní identity bylo možné se do jednotlivých portálů veřejné správy přihlásit například prostřednictvím datové schránky, eObčanky nebo mobilním klíčem eGovernmentu, avšak žádný ze způsobů přihlášení nebyl pro občana, který vlastní bankovní účet u některé z bankovních institucí, tak snadný, jelikož registrační procesy ostatních přihlašovacích metod zpravidla vyžadují úkony směřující k fyzickému ověření totožnosti před aktivací přihlašovacích údajů. V případě přihlašování prostřednictvím bankovní identity však povinnost ověření totožnosti prakticky proběhla pracovníky bankovní instituce v souběhu s podpisy smluv o poskytování bankovních služeb. Změna souvisejících zákonů umožnila bankovním institucím získat akreditaci a stát se tak poskytovatelem elektronické identity v souladu se zákonem č. 250/2017 Sb., o elektronické identifikaci. V rámci problematiky elektronického podpisu můžeme banky opět přirovnat k postavení

[67] DLUBALOVÁ, Klára. Nové občanky s biometrickými údaji začnou úřady vydávat již od srpna. *Ministerstvo vnitra České republiky: elektronizace veřejné správy v ČR* [online]. [cit. 13.2.2022]. Dostupné z: https://www.mvcr.cz/clanek/nove-obcanky-s-biometrickymi-udaji-zacnou-urady-vydavat-jiz-od-srpna.aspx

důvěryhodné certifikační autority, která garantuje ověření totožnosti a identifikaci uživatele.

Přihlášení do některého z informačních systémů veřejné správy (např. Portál MOJE daně nebo Portál Občana) prostřednictvím bankovní identity probíhá tak, že uživatel je přesměrován na internetovou stránku své banky, kde zadá přihlašovací údaje do internetového bankovnictví, čímž dojde k jeho identifikaci. Po zadání údajů následuje přesměrování do požadovaného informačního systému. V praxi se jedná se o velmi jednoduchý a časově nenáročný proces přihlášení bez nutnosti předchozí individuální registrace, což dalo možnost téměř 5,5 milionu občanů, kteří vlastní bankovní účet, komunikovat elektronicky se státní správou a využívat další on-line služby.[68]

Samotný projekt bankovní identity sice nemá přímou souvislost s problematikou elektronického podpisu, avšak dle mého názoru se jedná o jeden ze zásadních kroků digitalizace veřejné správy, který zpřístupnil on-line služby téměř každému občanovi ČR, což může mít pozitivní vliv na zájem o využívání efektivnějších metod komunikace v rámci běžného života nás všech.

[68] O projektu: Jeden z největších digitalizačních projektů českého bankovního sektoru. *Bankovní identita* [online]. [cit. 13.2.2022]. Dostupné z: https://bankovni-identita.cz/o-projektu/

PRAKTICKÁ ČÁST

4. Východiska praktické části

Následující kapitola zahrnuje primární cíle praktické části diplomové práce, metody a způsoby, pomocí kterých budou stanové cíle naplněny. Dále kapitola obsahuje předem definované hypotézy, jejichž ověření platnosti bude součástí závěrečného vyhodnocení praktické části diplomové práce.

4.1 Cíle a metody

Cílem praktické části diplomové práce je vyhodnocení bezpečnosti a využitelnosti zaručeného elektronického podpisu, který je založený na kvalifikovaném certifikátu, za pomocí deskripce procesu vytvoření elektronického podpisu dokumentu (včetně pořízení a implementace vhodného kvalifikovaného certifikátu na základě aktuální nabídky certifikačních autorit), dále komparace dvou kvalifikovaných certifikátů od různých certifikačních autorit a analýzy kvalifikovaného certifikátu on-line nástrojem.

K vytvoření diplomové práce bude využito primárně metod analýzy, syntézy, deskripce a komparace. Získávání relevantních informací bude probíhat také pomocí metod indukce a dedukce a bude vycházet z příslušných odborných publikací, článků, internetových zdrojů a také vlastních poznatků.

4.2 Hypotézy

Zpracování diplomové práce zahrnuje stanovení následujících hypotéz, jejichž platnost bude následně ověřena:

- Hypotéza č. 1: Kvalifikované certifikáty od různých certifikačních autorit nabízí shodnou úroveň bezpečnosti.
- Hypotéza č. 2: Zaručený elektronický podpis je vhodným nástrojem k zabezpečení dokumentu proti nežádoucím úpravám.

5. Vytváření elektronického podpisu

Finální fáze podepsání digitálního dokumentu nebo zprávy prostřednictvím zaručeného elektronického podpisu, který je založený na kvalifikovaném certifikátu od důvěryhodné certifikační autority, bývá díky uživatelsky přívětivým aplikacím velmi jednoduchá a intuitivní, avšak proces, který možnosti vytvořit takový podpis předchází, vyžaduje sérii nezbytných činností a postupů, které nemusí být každému příjemné.

První kapitola praktické části této práce se věnuje nastínění postupu, který musí fyzická osoba absolvovat, aby mohla vytvářet zaručený elektronický podpis založený na kvalifikovaném certifikátu. Vzhledem k tomu, že elementárním prvkem takového podpisu je kvalifikovaný certifikát, prvotní fáze se budou týkat především výběru certifikační autority, podávání příslušné žádosti a jejímu schvalování. Následovat bude fáze implementace certifikátu do lokálního uložiště počítače a způsoby použití.

5.1 Zajištění kvalifikovaného certifikátu

Základem elektronického podepisování dokumentů a zpráv pomocí zaručeného elektronického podpisu je získání vhodného certifikátu. Certifikát pro zaručený elektronický podpis si může vytvořit svépomocí kdokoliv, avšak nebude se jednat o certifikát kvalifikovaný, který je důležitý především pro zajištění důvěryhodnosti samotného elektronického podpisu.

Výběr vhodného certifikátu

Podepisující osoby si nejprve musí zvolit vhodný certifikát na základě dostupné nabídky od různých kvalifikovaných certifikačních autorit. Jelikož certifikáty jsou po technické stránce velmi podobné a častokrát můžeme spatřovat nuance pouze pro běžné uživatele v nepodstatných parametrech (např. síla šifrovacího algoritmu), zřejmě zásadním rozhodovacím aspektem bude cena služby za vystavení kvalifikovaného certifikátu. Postupy vytvoření kvalifikovaného certifikátu pro elektronický podpis u jednotlivých certifikačních autorit se také mírně liší, přičemž podmínkou vydání kvalifikovaného certifikátu je osobní návštěva kontaktního pracoviště dané certifikační autority za účelem ověření

totožnosti a signace smlouvy o poskytování certifikačních služeb. Pro mnohé žadatele bude tedy dalším hlediskem při posuzování volby certifikační autority také dislokace jednotlivých kontaktních pracovišť.

Společnosti Software602 a. s. a SEFIRA spol. s. r. o., které jsou také zařazené do seznamu kvalifikovaných poskytovatelů služeb vytvářejících důvěru, se na základě internetové prezentace své nabídky specializují primárně na komplexnější řešení oblasti vzdáleného elektronického podepisování dokumentů, které bezpochyby mají mnoho výhod především díky široké škále využití na různých typech zařízení, avšak jejich služby cílí spíše na firemní zákazníky, což z mého pohledu pro běžné potřeby fyzické osoby není zcela relevantní. Výběr se tedy zúžil na nabídku služeb od společností První certifikační autorita, a. s., Česká pošta, s. p., a eIdentity a. s., přičemž kromě výše poplatků a lokality kontaktních míst jsem značnou váhu přisuzoval také uživatelským recenzím, které zpravidla reflektují zkušenost s administrativní a technickou podporou daného poskytovatele služeb. Na základě vyhodnocení objektivních a subjektivních kritérií jsem zvolil kvalifikovaný certifikát od společnosti První certifikační autorita, a. s. Náklady na pořízení kvalifikovaného certifikátu se standardní platností na 1 rok činí 545 Kč vč. DPH.

Pořízení kvalifikovaného certifikátu

Proces získání kvalifikovaného certifikátu pro elektronický podpis od společnosti První certifikační autorita, a. s. se skládá z více fází, kterými musí každý žadatel projít. První část procesu se uskutečňuje on-line přímo na internetových stránkách certifikační autority a až poté následuje off-line fáze, která zahrnuje osobní návštěvu kontaktního místa certifikační autority.

Žadatel musí nejprve vyplnit žádost prostřednictvím webového formuláře na stránkách první certifikační autority v sekci “Získání certifikátu“ (www.mujcertifikat.cz/zadost-o-certifikat). Elektronická žádost je rozdělena do několika etap, přičemž prvotním krokem je volba statusu žadatele. Z hlediska plánované využitelnosti kvalifikovaného podpisu jsem v rámci vyplnění žádosti v prvním kroku zvolil „Fyzická osoba“.

Další krok zahrnuje možnosti volby účelu, ke kterému žadatel certifikát plánuje využívat. Kromě využití kvalifikovaného certifikátu pro elektronický podpis

v České republice, který byl zvolen mnou, nebo na Slovensku certifikační autorita poskytuje také komerční certifikáty nebo kombinace kvalifikovaných a komerčních certifikátů pod produktovým názvem TWINS. Po zaškrtnutí varianty „Kvalifikovaný certifikát pro elektronický podpis“ se zobrazí doplňkové možnosti způsobu uložení certifikátu. Pokud žadatel zvolí uložení na čipové kartě nebo občanském průkazu, bude se za předpokladu využití takového kvalifikovaného prostředku jednat o kvalifikovaný elektronický podpis, tedy nejvyšší formu elektronického podpisu.

Ačkoliv by se mohlo zdát, že následující krok bude obsahovat formulář s údaji potřebnými pro vytvoření certifikátu, není tomu tak, protože certifikační autorita nejprve požaduje provedení kontroly způsobilosti počítače. Webová aplikace požaduje zahájení testu počítače, který ověří minimální požadavky pro bezproblémový průběh generování žádosti. Mezi základní parametry, které jsou předmětem ověřovacího testu, patří verze operačního systému, typ a verze webového prohlížeče, podpora skriptovacího jazyka JavaScript, stav instalace rozšíření v prohlížeči (Komponenta I.CA PKI Service pro Google Chrome), stav instalace aplikace v počítači (Komponenta I.CA PKIServiceHost pro Windows) a podpora ukládání cookies (viz obrázek 11). Obě výše uvedené komponenty I.CA PKI Service slouží k práci s certifikáty a čipovou kartou. Pokud žadatel některý z těchto softwarových nástrojů nemá nainstalovaný, ověřovací test se automaticky pozastaví a zobrazí žadateli postup jejich stažení a instalace.

Obrázek 11 – Kontrola způsobilosti zařízení před podáním žádosti

Pokud jednotlivé kroky validačního testu proběhnou úspěšně, může žadatel procesem žádosti pokračovat dále na formulář s údaji. Kromě povinných osobních údajů o žadateli, mezi které patří jméno, příjmení, e-mailová adresa, je možné vyplnit také nepovinné položky jako například adresu bydliště nebo identifikátor fyzické osoby (např. číslo občanského průkazu). Z pohledu komunikace se státní správou je důležité zaškrtnout pole „Certifikát obsahující IK MPSV pro komunikaci s orgány státu“, díky čemuž certifikační autorita vloží identifikátor klienta MPSV do certifikátu. Identifikátor klienta MPSV slouží k jedinečné identifikaci klienta vůči Ministerstvu práce a sociálních věcí, finančnímu úřadu, České správě sociálního zabezpečení a úřadu práce. Formulář dále zahrnuje technické atributy certifikátu. Žadatel si dále vybírá požadovaný typ klíče, heslo pro zneplatnění certifikátu pro případ prozrazení soukromého klíče a v neposlední řadě typ úložiště klíče.

Po vyplnění požadovaných údajů a přechodu na další krok poskytovatel překládá souhrn vyplněných údajů ke kontrole, jelikož po uložení žádosti a dokončení celého procesu není možné údaje měnit. Po odsouhlasení správnosti údajů dochází k vygenerování a uložení soukromého klíče, přičemž žadatel má možnost v dialogovém okně programu I.CA PKIServiceHost nastavit úroveň zabezpečení použití privátního klíče na střední (při použití požadovat oprávnění) nebo na vysokou (při použití požadovat oprávnění s heslem). Na základě mého osobního požadavku maximalizovat úroveň zabezpečení jsem zvolil vysokou úroveň, díky čemuž bude v budoucnu při každé aplikaci elektronického podpisu vyžadováno heslo k uživatelskému účtu Windows.

Po odsouhlasení předchozí fáze dojde k přesměrování na poslední krok on-line procesu žádosti o kvalifikovaný certifikát. Tento krok lze označit spíše za formální, jelikož žadatel nemusí provádět žádné akce, nýbrž je poučen o dalším postupu spočívajícím v off-line návštěvě kontaktního pracoviště certifikační autority. Informační systém certifikační autority zároveň automaticky odešle na uvedený e-mail označení žádosti v podobě šestimístného kódu včetně záložního souboru, který může žadatel použít alternativně v případech, kdy se pracovníkovi CA při osobní návštěvě kontaktního místa nepodaří dohledat žádost na základě číselného kódu například z důvodu automatického smazání žádosti ze serveru po 30 dnech.

Jak již bylo několikrát v práci zmiňováno, po dokončení žádosti na internetových stránkách je třeba navštívit některé z kontaktních míst certifikační autority, aby mohl být celý proces řádně zkompletován a vystaven certifikát. První certifikační autorita, a.s. aktuálně disponuje 36 kontaktními místy, přičemž pouze dvě místa jsou spravována přímo jejími pracovníky. Ostatní kontaktní místa zřizují jiné společnosti nebo orgány samosprávy, přičemž úkony spjaté s vydáváním certifikátů vykonávají na základě dohody s certifikační autoritou.[69] Společnost První certifikační autorita, a.s. mimo jiné nabízí příplatkovou službu tzv. mobilní registrační autority, v rámci které pracovník CA navštíví žadatele přímo na požadované adrese za účelem splnění úkonů před vystavením certifikátu. S ohledem na osobní preference jsem v rámci procesu pořízení certifikátu navštívil hlavní pobočku, která je zároveň sídlem společnosti První certifikační autorita, a.s., na adrese Podvinný mlýn 2178/6, 190 00, Praha 9.

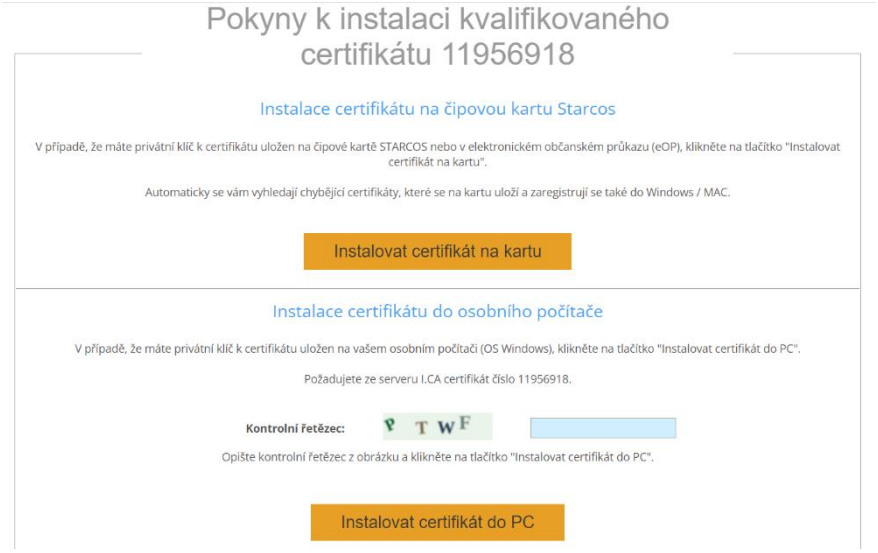
Při osobní návštěvě pobočky žadatel nejprve sdělí pracovníkovi číselné označení žádosti nebo případně poskytne vygenerovaný soubor s žádostí o certifikát. Dále jsou od žadatele vyžadovány dva platné doklady totožnosti, přičemž jedním z dokladů musí být občanský průkaz, cestovní pas nebo obdobný doklad stejné právní váhy. Dalším dokladem může být například karta zdravotní pojišťovny, cestovní pas nebo řidičský průkaz. Pokud žadatel disponuje vysokoškolským titulem, který nemá uveden v dokladu totožnosti, ale přeje si jej mít v certifikátu, musí skutečnost doložit originálem vysokoškolského diplomu.[70] Pracovník certifikační autority následně připraví k podpisu protokol o podání žádosti o vydání kvalifikovaného certifikátu pro elektronický podpis a smlouvu o vydání a používání kvalifikovaného certifikátu pro elektronický podpis ve dvou vyhotoveních, kterou žadatel a pověřený zaměstnanec vzájemně podepíší. K vystavení certifikátu je dále nutné uhradit poplatek ve výši 545 Kč.

[69] Registrační autority I.CA. *I.CA* [online]. [cit. 19.2.2022]. Dostupné z: https://www.ica.cz/pobocky-registracni-autority

[70] Dokumenty pro získání certifikátu: Nepodnikající fyzická osoba. *I.CA* [online]. [cit. 19.2.2022]. Dostupné z: https://www.ica.cz/Dokumenty-kvalifikovany-certifikat-pro-ePodpis

5.2 Implementace kvalifikovaného certifikátu

Finální fází procesu získávání kvalifikovaného certifikátu je jeho instalace do příslušného zařízení. Informační systém certifikační autority automaticky po splnění všech výše uvedených požadavků odešle na e-mailovou adresu uvedenou v žádosti zprávu obsahující interaktivní postup pro instalaci certifikátu. Pokyny k instalaci kvalifikovaného certifikátu zahrnují možnost naistalovat certifikát na čipovou kartu v případech, kdy soukromý klíč je uložený na čipové kartě nebo na elektronickém občanském průkazu, nebo instalovat certifikát do osobního počítače za předpokladu, že soukromý klíč se nachází na pevném disku (viz obrázek 12). Kromě výběru uložiště certifikátu může držitel také pohodlně pomocí aplikace ICARootMan.exe registrovat kořenové certifikáty I.CA, pokud je již v operačním systému nemá k dispozici.



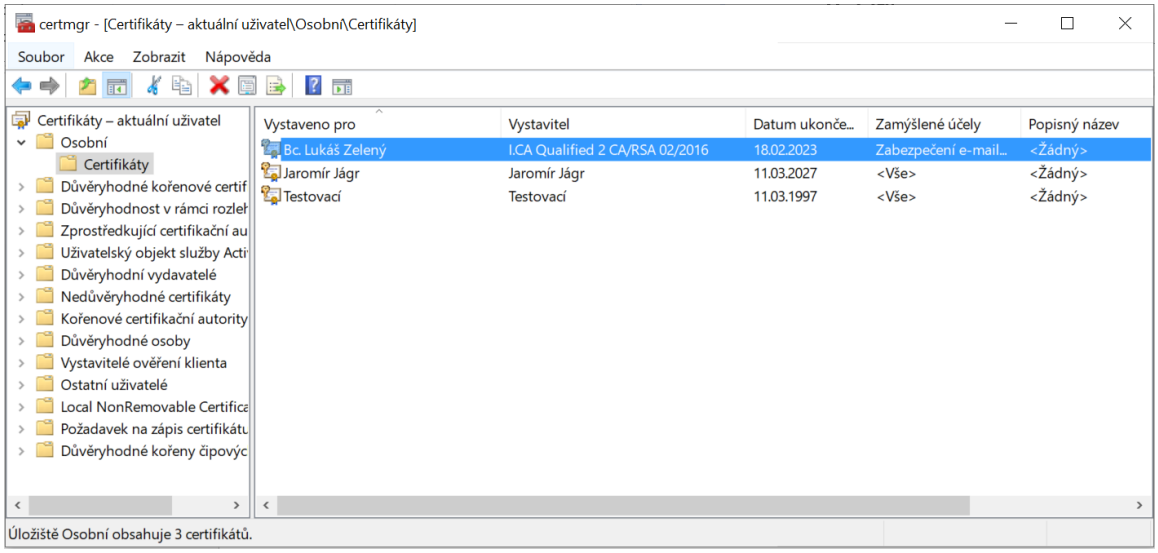
Obrázek 12 – Interaktivní okno s možnostmi instalace kvalifikovaného certifikátu

Dále certifikační autorita nabízí řadu návodů týkajících se samotného používání certifikátu v e-mailových klientech, internetových prohlížečích nebo ostatních aplikacích pro práci s PDF dokumenty (např. Acrobat Adobe Reader). Poslední, avšak velmi důležitou položkou interaktivního postupu je odkaz na návod na zálohu privátního klíče a certifikátu, kterou je vhodné vytvořit pro potřeby obnovy v případě neočekávaných událostí (např. mechanického poškození), nebo pro potřeby přenosu certifikátu na jiné zařízení. Záloha soukromého klíče však

z bezpečnostních důvodů není možná z kvalifikovaných prostředků (např. čipová karta nebo USB token).[71]

Pokud vlastník certifikátu nevyužije možnost jeho instalace prostřednictvím interaktivního postupu, může k instalaci použít zazipovaný soubor, který je obsahem přílohy konfirmačního e-mailu. K instalaci certifikátu slouží u zařízení s operačním systémem Windows Průvodce importem certifikátu, pomocí kterého soubor s příponou .cer může vlastník nahrát do systému. Další variantou, jak získat a naimportovat certifikát, je jeho vyhledání a stažení v požadovaném formátu ze seznamu veřejných certifikátů vedeného certifikační autoritou.

Zkontrolovat správný import certifikátu v operačním systému Windows 10 lze prostřednictvím Správy certifikátů uživatele (certmgr.msc). Pakliže import certifikátu proběhl úspěšně, ve složce Osobní – Certifikáty bude certifikát označený jménem vlastníka k dispozici (viz obrázek 13).



Obrázek 13 – Ověření importu certifikátu pomocí Správy certifikátů uživatele (certmgr.msc)

Při importu certifikátu je vhodné si uvědomit, že se jedná pouze o veřejnou část, která neobsahuje soukromý klíč, jehož vygenerování bylo předmětem vytvoření žádosti. V případě importu certifikátu do zařízení, kde absentuje svázaný soukromý klíč, nebude možné dokument nebo zprávu kvalifikovaným certifikátem podepsat. Pokud tedy vlastník bude mít zájem zaručený elektronický podpis založený na kvalifikovaném certifikátu aplikovat i na jiných zařízeních, než na

[71] Záloha certifikátu. *I.CA* [online]. [cit. 20.2.2022]. Dostupné z: https://www.ica.cz/Zaloha-certifikatu

kterém vytvářel žádost, bude třeba provést kompletní export certifikátu včetně soukromého klíče s následným importem v jiném zařízení.

5.3 Elektronické podepsání dokumentu

Jakmile máme kvalifikovaný certifikát správně naimportován v zařízení, můžeme přistoupit ke kýženému procesu elektronického podepisování. Zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu je možné podepisovat různé datové formy, přičemž mezi nejtypičtější objekty elektronického podpisu patří dokumenty nebo e-mailové zprávy. Ačkoliv následující kapitola praktické části práce se věnuje primárně elektronickému podepisování dokumentů, rád bych na úvod zmínil princip podepisování e-mailových zpráv. Kvalifikovaný certifikát pro elektronické podepisování lze s ohledem na zachování bezpečnosti soukromého klíče využít výhradně u e-mailových klientů nainstalovaných na konkrétním zařízení (např. Microsoft Outlook), nikoliv v rámci webových rozhraní.

K elektronickému podepisování dokumentů mají uživatele k dispozici širokou škálu aplikací od různých vývojářů. Nejčastěji se můžeme setkat s komplexními softwarovými nástroji, jejichž primárním účelem není přímo elektronické podepisování dokumentů, ale spíše jejich vytváření, úprava a další související činnosti. Možnost elektronického podepisování lze chápat spíše jako doplňkovou funkci. Mezi nejznámější a nejčastěji používané programy se řadí například Microsoft Word nebo Adobe Acrobat Reader. Kromě zmiňovaných univerzálních softwarů existuje také řada aplikací, které se na elektronické podepisování specializují.

Velmi často aplikace se zaměřením přímo na elektronické podepisování nabízí certifikační autority společně s nabídkou kvalifikovaných a komerčních certifikátů, kvalifikovaných prostředků a dalších doplňkových služeb a produktů. První certifikační autorita, a. s. má ve svém produktovém portfoliu aplikaci I.CA Secom®2, mezi jejíž primární funkce patří vytváření a ověřování elektronických podpisů. Aplikace dokáže podepisovat dokumenty, textové soubory nebo také obrázky v libovolných formátech a přidávat časová razítka.[72] Podobnou nabídku

[72] I.CA Secom®2. *I.CA* [online]. [cit. 22.2.2022]. Dostupné z: https://www.ica.cz/secom

softwaru určeného k podepisování dokumentů má také Česká pošta, s. p. (PostSignum). Jedná se o aplikace PDF Signer nebo VerisignIT, prostřednictvím kterých uživatel dokáže vytvářet a ověřovat elektronické podpisy jak u standardních textových dokumentů, tak i u obrázků.

Ačkoliv spousta uživatelů si pod slovním spojením „elektronický podpis“ představí zpravidla grafické vyjádření jména podepisující osoby v dokumentu nebo zprávě, jelikož zde platí jistá analogie k vlastnoručnímu podpisu, pro softwarové nástroje pracující s elektronickými podpisy bývá grafické znázornění podpisu pouze formálním a minoritním krokem. Dokument se stává elektronicky podepsaným aplikací příslušných technologických postupů, čímž zároveň získává požadované vlastnosti (např. integritu), nikoliv vizuálním zobrazením nacionálií, které některé programy pro práci s elektronickými podpisy dokonce ani nemusí podporovat.

Adobe Acrobat Reader DC

Pro účely demonstrace uživatelského procesu vytvoření elektronického podpisu dokumentu byla použita bezplatná verze aplikace Adobe Acrobat Reader DC, která je primárně určena k prohlížení, podepisování, sdílení a přidávání poznámek k dokumentům ve formátu PDF. Ačkoliv společnost Adobe má ve svém portfoliu další aplikace s rozšířenými funkcemi v oblasti elektronického podepisování (např. Adobe Acrobat Pro DC nebo Adobe Sign), pro účely vytvoření a ověření zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu postačí základní aplikace.[73]

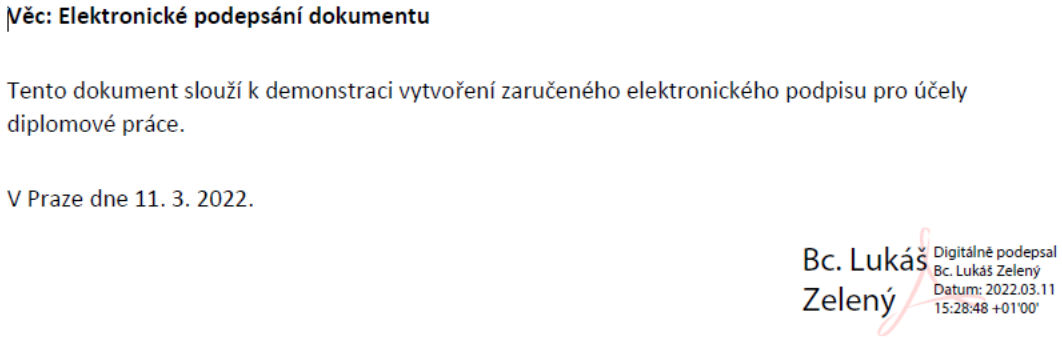
Za předpokladu, že podepisující osoba má již správně implementovaný kvalifikovaný certifikát v uložišti počítače, postup vytvoření elektronického podpisu je relativně jednoduchý a intuitivní. Prvním krokem je otevření příslušeného dokumentu a následně panelu nástrojů. Vytvořit zaručený elektronický podpis je možné pomocí nástroje „Certifikáty“. Uživateli se zobrazí nabídka, prostřednictvím které může dokument digitálně podepsat, přidat časové razítko nebo ověřit platnost všech podpisů. Jakmile uživatel zvolí možnost “Digitálně podepsat“,

[73] Adobe Acrobat Reader: Nejlepší prohlížeč PDF je ještě dokonalejší. *Adobe ČR: Řešení pro kreativce, marketing a správu dokumentů* [online]. [cit. 25.2.2022]. Dostupné z: https://www.adobe.com/cz/acrobat/pdf-reader.html

program jej nejprve vyzve k vyznačení oblasti pro grafické vyobrazení podpisu. Následně se zobrazí dialogové okno s dostupnými digitálními identifikátory. Uživatel z nabídky vybere svůj příslušný kvalifikovaný certifikát dislokovaný v systému Windows. Mimo jiné během tohoto kroku uživatel může nakonfigurovat nové digitální ID neboli certifikát pro podepisování dokumentů, které může vycházet z externího prostředku (např. čipová karta nebo token), datového souboru nebo může být přímo vytvořeno uživatelem. Pokud uživatel vytvoří vlastní digitální ID, nebude se jednat o kvalifikovaný certifikát, tudíž elektronický podpis bude pouze na úrovni zaručeného. Na základě výběru digitálního ID nám v dalším kroku aplikace předestře návrh vzhledu včetně grafického uspořádání jednotlivých údajů v původně označeném místě. Vizuální podobu podpisu je možné upravit například přidáním podpisové křivky, která by více mohla připomínat vlastnoruční podpis. Ačkoliv podepsání dokumentu zaručeným elektronickým podpisem zaručuje nemožnost činit změny nebo úpravy podepsaného dokumentu, program Acrobat Reader DC dále umožňuje zaškrtnutí pole „Zamknout dokument po podepsání“, což navíc oproti standardní vlastnosti zaručeného elektronického podpisu znemožní aplikování dalších elektronických podpisů jinými uživateli, přidávání poznámek a vyplňování předem určených formulářových polí.[74]

Potvrzením posledního kroku softwarový nástroj provede potřebné technické procesy, na základě nichž dojde k podepsání dokumentu. Následuje přidání vizuálního prvku elektronického podpisu, který zpravidla obsahuje jméno a příjmení podepisující osoby, systémový datum a čas podepsání a vodoznak loga softwaru Acrobat Reader DC. Dále může grafické znázornění elektronického podpisu zahrnovat například verzi programu, umístění podpisu nebo rozlišující název. Požadované prvky si uživatel může libovolně vybrat v rámci posledního kroku podpisu, avšak fixním údajem je skutečné jméno podepisující osoby uvedené v kvalifikovaném certifikátu. Ukázka možného vzhledu podepsaného elektronického dokumentu je vyobrazena na obrázku 14.

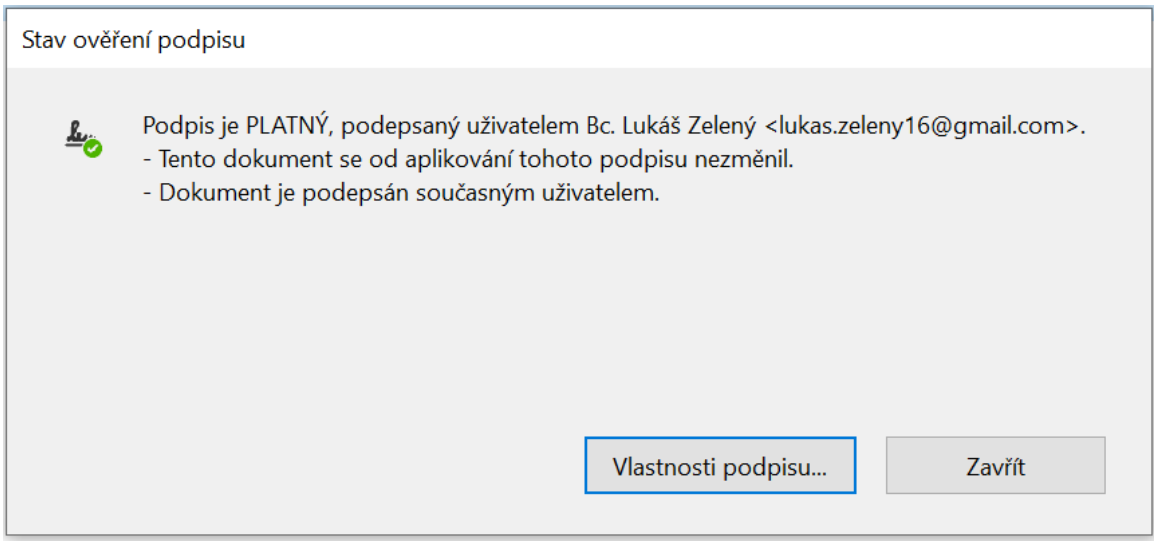
[74] Úprava podepsaného dokumentu PDF | Časté dotazy: Co když je dokument PDF po podepsání uzamčen?. *Adobe ČR: Řešení pro kreativce, marketing a správu dokumentů* [online]. [cit. 26.2.2022]. Dostupné z: https://helpx.adobe.com/cz/acrobat/kb/edit-signed-PDF.html



Obrázek 14 – Ukázka podepsaní dokumentu zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu

Další velmi důležitou funkcí aplikace Acrobat Reader DC je ověřování platnosti podpisu. Pokud je software ve výchozím nastavení, k ověřování elektronických podpisů dochází již během otevření dokumentu. Ověření je prováděno na základě informaci od zdroje důvěry, kterým je v tomto případě uložiště důvěryhodných certifikátů Windows, tudíž aplikace označila vytvořený podpis za platný. Přehled platnosti podpisu obsahuje další podrobné informace o tom, v čem je platnost podpisu spatřována. Jedná se primárně o informaci, že dokument se od aplikace podpisu nezměnil, díky čemuž je zajištěna integrita dat (viz obrázek 15). Dále přehled informuje, zdali je povolena alespoň částečná práce s dokumentem v podobě přidávání dalších elektronických podpisů, poznámek a vyplňování formulářů, nebo zdali je dokument uzamčen a nejsou možné žádné další změny. Platnost podpisu je také velmi úzce provázána s platnou identitou podepisující osoby, jejíž ověření probíhá na základě dat z kvalifikovaného certifikátu. V neposlední řadě přehled obsahuje informace o ověření podpisu, datu a času podepsání dokumentu. Nechybí ani upozornění, že uváděný datum a čas podpisu byl převzat z počítače autora, tudíž bez přidání časového razítka nelze garantovat validitu těchto informací. Mimo jiné zpráva o platnosti podpisu zahrnuje informace o autorovi, které potvrzují, že cesta od certifikátu autora podpisu k certifikátu vystavitele byla úspěšně vytvořena a certifikát autora je platný a nebyl doposud odvolán.

Jak již bylo nastíněno, aplikace Adobe Acrobat Reader DC umožňuje také přidávání časových razítek. Časová razítka bývají k dispozici u certifikačních autorit a jejich použití garantuje přesný datum a čas, a navíc prodlužují platnost zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu.



Obrázek 15 – Stav ověření platnosti vytvořeného elektronického podpisu

6. Komparace kvalifikovaných certifikátů

Následující kapitola praktické části práce nepřímo navazuje na kapitoly předcházející, ve kterých byla rozebírána problematika jednotlivých důvěryhodných certifikačních autorit, nabídek kvalifikovaných certifikátů a jejich využitelnosti.

Vzhledem k tomu, že v nabídkách kvalifikovaných certifikátů od dostupných poskytovatelů služeb vytvářejících důvěru můžeme spatřovat různé nuance, považuji za vhodné se v rámci praktické části práce zaměřit na komparaci kvalifikovaných certifikátů určeným fyzickým osobám. Na první pohled lze za největší odlišnost označit poměrně značné cenové rozdíly mezi jednotlivými nabídkami kvalifikovaných certifikátů od důvěryhodných certifikačních autorit.

Na základě elementární analýzy cenových nabídek jsem se rozhodl komparovat kvalifikované certifikáty od jedněch z největších poskytovatelů certifikačních služeb v České republice. První důvěryhodnou certifikační autoritou je společnost Česká pošta, s. p., která nabízí kvalifikovaný certifikát pro fyzické osoby za 396 Kč vč. DPH s platností na 385 dní.[75] Druhým poskytovatelem služeb vytvářejících důvěru je společnost První certifikační autorita, a. s., u níž vystavení kvalifikovaného certifikátu pro fyzickou osobu na jeden rok stojí 545 Kč vč. DPH.[76] I přes nižší pořizovací cenu můžeme mírnou výhodu společnosti Česká pošta, s. p. spatřovat ve větším množství kontaktních míst, a tím pádem lepší dostupnosti na území České republiky.

6.1 Předmět komparace

Komparace jednotlivých kvalifikovaných certifikátů bude primárně prováděna se zaměřením na technické parametry. Předmětem porovnávacího procesu bude kvalifikovaný certifikát vystavený společností První certifikační autorita, a. s. (I.CA) označený sérovým číslem 00b672b6, jehož vlastníkem je autor práce, a kvalifikovaný certifikát původem od společnosti Česká pošta, s. p. (PostSignum) se sériovým číslem 0156469f, jež byl pro účely této práce poskytnut

[75] Ceny za vydávané certifikáty: Kvalifikované certifikáty. *PostSignum* [online]. [cit. 26.2.2022]. Dostupné z: https://www.postsignum.cz/certifikaty.html

[76] Ceník - certifikáty: Certifikáty uložené ve Vašem PC. *I.CA* [online]. [cit. 26.2.2022]. Dostupné z: https://www.ica.cz/cenik-certifikaty

kolegyní Bc. Kristýnou Markovou. Pro účely této práce bude certifikát vydaný I.CA označován a prezentován jako první (číslo 1) a certifikát od PostSignum jako druhý (číslo 2).

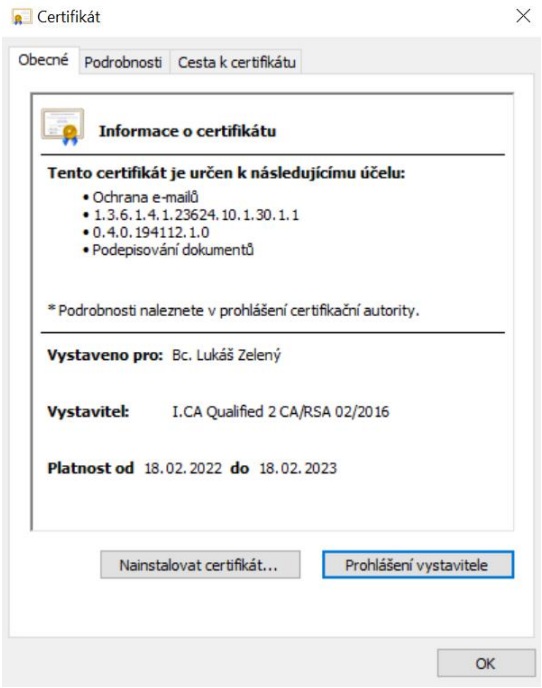
6.2 Porovnání certifikátu I.CA a PostSignum

Datové soubory kvalifikovaných certifikátů obsahují různé informace (viz kapitola 2.4), přičemž datová struktura certifikátů může být uložena v různých formátech. Pro operační systém Windows jsou typické soubory s příponou .cer, avšak data mohou být uložena také například ve standardním textovém formátu s příponou .txt. Informace obsažené v certifikátu jsou dislokovány v jednotlivých polích, které obsahují zpravidla obecné názvy parametrů, přičemž ke každému poli se váže konkrétní hodnota.

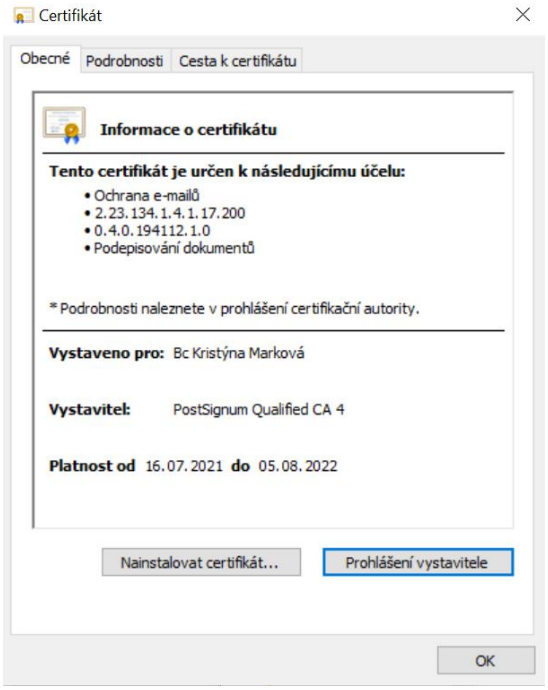
Obecné informace o certifikátu

Po otevření obou souborů s certifikáty se zobrazí titulní strana se základními informacemi o certifikátu. V prvním oddílu informačního listu certifikátu je stručný výčet účelu daného certifikátu. V případě certifikátu od I.CA a PostSignum je účel shodný, jelikož oba certifikáty jsou primárně určeny k podepisování dokumentů a ochraně e-mailových zpráv. Další informací obsaženou v obecných informacích o certifikátů je jméno a příjmení (případně titul) osoby, pro kterou je certifikát vystaven. V tomto případě se informace logicky liší, jelikož první komparovaný certifikát byl vystaven pro jinou fyzickou osobu než certifikát druhý. Odlišnost lze očekávat také v dalším poli, kde se nachází vystavitel certifikátu. První certifikát vystavila kvalifikovaná certifikační autorita I.CA Qualified 2 CA/RSA 02/2016 spadající pod společnost První certifikační autorita, a. s. Vystavitelem druhého certifikátu je certifikační autorita se zaměřením na kvalifikované certifikáty PostSignum Qualified CA 4, jíž tvoří společnost Česká pošta, s. p. Poslední informací obsaženou v úvodním přehledu certifikátu je interval platnosti daného certifikátu. Časová platnost obou certifikátů se nemůže shodovat jednak z důvodu rozdílných termínů vystavení certifikátu a dále také kvůli odlišené době platnosti. Certifikační autorita PostSignum vystavuje certifikáty na 385 dní, kdyžto platnost kvalifikovaného certifikátu I.CA je pouze 365 dní od vystavení.

Oddíl obecných informací o certifikátu zachycený na obrázcích 16 a 17 obsahuje zpravidla takové informace, které jsou důležité k ověření platnosti. Pokud vystavitel je zařazen mezi kvalifikovaného poskytovatele služeb vytvářejících důvěru, a zároveň je interval data platnosti v souladu s datem v den ověření, lze certifikát označit za platný a důvěryhodný.



Obrázek 17 – Obecné informace o prvním certifikátu



Obrázek 16 – Obecné informace o druhém certifikátu

Podrobné informace o certifikátu

V další sekci informací o certifikátu se nachází jednotlivé podrobnosti rozdělené do polí a k nim přiřazených hodnot. Hodnota „V3“ uvedená v poli „Verze“, která označuje použitou verzi standardu X.509, což je kryptografický formát pro certifikáty založené na infrastruktuře veřejného klíče, je pro oba certifikáty shodná.[77]

Velmi důležitým identifikátorem certifikátu je jeho sériové číslo přidělené certifikační autoritou v rámci procesu vystavení. Hodnota sériového čísla bývá uváděna v dekadickém nebo hexadecimálním tvaru. Vzhledem k tomu, že se jedná o unikátní označení každého certifikátu, shoda hodnot prvního a druhého

[77] What Is an X.509 Certificate?. *SSL.com* [online]. 23 September 2019 [cit. 26.2.2022]. Dostupné z: https://www.ssl.com/faqs/what-is-an-x-509-certificate/#

certifikátu není možná. Sériové číslo certifikátu č. 1 je 00b672b6 a sériové číslo certifikátu č. 2 je 0156469f.

Z pohledu síly šifrování si můžeme všimnout významného rozdílu v hodnotách pole označeného jako „Algoritmus podpisu“. První certifikát je vybaven podpisovým algoritmem typu sha512RSA a druhý certifikát disponuje algoritmus podpisu sha256RSA. SHA (Secure Hash Algorithm) je rozšířená hashovací funkce, která přiřadí vstupním datům číselný řetězec o pevné délce. Rozdíl mezi těmito algoritmy je především v počtu výstupních znaků, síle hashování a rychlosti podepisování.[78]

Dále se v souboru nachází podrobnosti o vystaviteli certifikátu. Kromě základní informace o certifikační autoritě, která byla obsažena již v sekci s obecnými informacemi, je zde uvedena také firma společnosti včetně právní formy, NTRCZ, jakožto identifikátor subjektu, a země. V případě prvního certifikátu je uváděn jako vystavitel I.CA Qualified 2 CA/RSA 02/2016, firma První certifikační autorita, a. s. s identifikačním číslem NTRCZ-26439395 v zemi CZ. Pole druhého certifikátu obsahuje PostSignum Qualified CA 4, Česká pošta, s. p., identifikační číslo NTRCZ- 47114983 a zemi CZ.

Oddíl podrobností dále rozšiřuje informace o časové platnosti obou certifikátů, které byly již předestřeny v obecné informační části certifikátu. Vzhledem k tomu, že doba začátku a konce platnosti certifikátu je stanovena na sekundy přesně a obecná část obsahuje pouze datum platnosti bez příslušných časových údajů, je třeba využívat podrobných údajů. Certifikáty v oblasti platnosti obsahují dvě pole. První pole s názvem „Platnost od“ se týká začátku platnosti a v případě prvního certifikátu je svázáno s hodnotou pátek 18. února 2022 10:11:13. Jedná se o přesný datum a čas vystavení certifikátu vydavatelem. Druhý certifikát byl vystaven v pátek 16. července 2021 9:15:01. Navazující pole „Platnost do“ naopak určuje konec platnosti daného certifikátu. Konec platnosti prvního certifikátu je stanovena přesně na jeden rok od vystavení, tj. sobota 18. února 2023 10:11:13. Platnost druhého certifikátu díky navýšení

[78] NOHE, Patrick. Re-Hashed: The Difference Between SHA-1, SHA-2 and SHA-256 Hash Algorithms. *Hashed Out by The SSL Store* [online]. 9 November 2018 [cit. 27.2.2022]. Dostupné z: https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/

platnosti na 385 dní končí v pátek 5. srpna 2022 9:15:01, jelikož certifikační autorita PostSignum přidává 20 dní k standardní roční platnosti jako bonus.

Další pole obsahuje velmi důležité informace o subjektu, tj. osobě, která certifikát vlastní. Informace v obou certifikátech se neliší pouze hodnotami jednotlivých parametrů, ale také typem dat, které obsahují. Subjektem prvního certifikátu je autor práce, přičemž pole obsahuje jméno, příjmení, titul a další doplňující osobní údaje, mezi které patří adresa trvalého pobytu (včetně kraje a země) nebo číslo dokladu totožnosti. V případě druhého certifikátu nejsou odlišené jen samotné osobní údaje, ale také jednotlivé parametry. Pole standardně obsahuje jméno a příjmení subjektu, avšak chybí adresa trvalého pobytu a číslo dokladu totožnosti. Naopak oproti prvnímu certifikátu je zde navíc název organizace, za kterou fyzická osoba vystupuje, a IČO společnosti. Na základě těchto informací lze odhadnout, že první certifikát byl vydán výhradně pro osobní účely fyzické osoby, kdežto druhý certifikát zřejmě bude využíván pro fyzickou osobu v zaměstnaneckém či jiném poměru k uvedené organizaci nebo instituci.

Jeden z velmi důležitých technických parametrů označený jako „Veřejný klíč“, jehož hodnota má vliv na sílu a rychlost šifrování, nalezneme v dalším poli. Oba certifikáty používají velmi rozšířený šifrovací algoritmus typu RSA, jež je vhodný jak pro šifrování, tak i pro podepisování.[79] První certifikát využívá algoritmus RSA s délkou klíče 4096 bitů, který je oproti algoritmu RSA s délkou klíče 2048 druhého certifikátu méně využívaný, avšak lze jej považovat za silnější. Naopak nevýhodou je však vyšší nároky na využití procesoru a delší doba procesu šifrování. Pro účely standardního elektronického podepisování však aktuálně dostačuje klíč o délce 2048, ale s rostoucím vývojem výkonnosti jednotlivých zařízení není vyloučena změna standardu a přechod výhradně na klíče o větší délce.[80]

[79] Algoritmus RSA. *Expedited Security* [online]. [cit. 27.2.2022]. Dostupné z: https://www.algoritmy.net/article/4033/RSA

[80] So you're making an RSA key for an HTTPS certificate. What key size do you use?: Or: why you probably don't want a 4096 bit RSA cert. *Expedited Security: Security as a Service for Heroku, AWS and Google Cloud Applications* [online]. 12 July 2021 [cit. 27.2.2022]. Dostupné z: https://expeditedsecurity.com/blog/measuring-ssl-rsa-keys/

Ačkoliv velká část osobních údajů a identifikátorů fyzické osoby již byla v předchozích polích uvedena, stále zbývá představit důležitý parametr pro oblast elektronické komunikace, kterým je e-mailová adresa vlastníka certifikátu. E-mailová adresa, která se ke konkrétnímu certifikátu váže, je uvedena v poli „Alternativní název předmětu“. Hodnota pole dále může zahrnovat identifikátor MPSV, jakožto jedinečný identifikátor osoby před orgány státní správy, který na žádost přiděluje certifikační autorita. Z přehledu je patrné, že první certifikát má identifikátor MPSV přidělen a je tedy připraven na komunikaci se státní správou, kdežto druhý certifikát tento identifikátor přidělený nemá, tudíž jeho využitelnost při úkonech vůči orgánům státní správy může být omezena. Identifikátor představuje řetězec znaků, přičemž jednotlivé části mají různý význam. První část před rovnítkem představuje identifikátor objektu přidělený MPSV pro jednoznačnou identifikaci Identifikátoru klienta (je shodný pro všechny IK MPSV) a část za rovníkem označuje binární řetězec IK MPSV.[81]

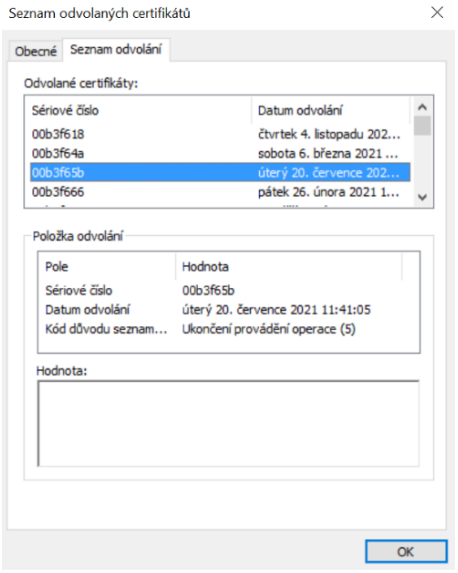
Podrobnosti dále zahrnují pole „Zásady certifikátu“, ve kterém se mimo jiné nachází prohlášení vystavitele. Nalezneme zde identifikátory jednotlivých zásad, ID kvalifikátoru zásad a samotný kvalifikátor. V případě prvního certifikátu se jedná zejména o certifikační prováděcí směrnici (CPS), přičemž kvalifikátorem je odkaz na hlavní stránku internetových stránek vystavitele, tedy www.ica.cz. Druhý certifikát také uvádí v rámci ID kvalifikátoru zásad certifikační prováděcí směrnici s odkazem na web www.postsignum.cz. Kromě zmíněných kvalifikátorů v certifikátu nachází také oznámení pro uživatele ve shodném znění „Tento kvalifikovaný certifikát pro elektronický podpis byl vydán v souladu s nařízením EU c. 910/2014.This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014.“ Jedná se o důležitou informaci, která je mimo jiné prezentována jako prohlášení vystavitele, jež garantuje splnění podmínek úrovně kvalifikovaného certifikátu dle nařízení EU.

Významnou roli hraje také pole „Přístup k informacím autority“, které pro oba certifikáty zahrnuje odkaz na umístění protokolu OCSP (Online Certificate

[81] Jak zjistím, zda můj kvalifikovaný certifikát obsahuje Identifikátor MPSV?. *EPodpora aplikací Daňového portálu - Finanční správa* [online]. [cit. 27.2.2022]. Dostupné z: https://epodpora.mfcr.cz/cs/seznam-okruhu/certifikaty-elektronicky-podpis/jak-zjistim-zda-muj-kvalifikovany-certif-4439

Status Protocol). Jedná se internetový protokol, jehož účelem je ověření stavu, resp. platnosti certifikátů. Uživatel má možnost zejména v důsledku nežádoucí události (např. odcizení soukromého klíče) zneplatnit svůj certifikát u certifikační autority. Aby se protistrana, respektive celá veřejnost o takovém zneplatnění dozvěděla, používají se OCSP protokoly, které fungují na bázi dotazu, který odešle zařízení uživatele a navazující odpovědi ze strany serveru. Jedná se o rychlejší a méně náročné procesy, jelikož množství data obsažené v komunikaci klienta a serveru je podstatně menší, než u metody CRL, která je starší alternativou fungující na odlišeném systému zveřejňování celých seznamů zneplatněných certifikátů vydaných certifikační autoritou, což samozřejmě z dlouhodobého hlediska znamená větší náročnost na objem přenášených dat. OCSP protokol prvního certifikátu se nachází na adrese ocsp.ica.cz/2qca16_rsa. Druhý certifikát má OCSP protokol dislokován na adrese ocsp.postsignum.cz/OCSP/QCA4/.

Jak již bylo zmíněno dříve, s problematikou zneplatněných certifikátů souvisí také CRL seznamy, které se v datové struktuře certifikátu také nachází, a to konkrétně v poli s distribučními místy CRL. První i druhý certifikát zahrnuje odkazy na soubory se seznamy zneplatněných certifikátů umístěné na serverech obou certifikačních autorit. Seznam obsahuje sériové číslo každého odvolaného certifikátu, přesný datum a čas odvolání a v některých případech také důvod odvolání. Mezi nejčastější důvody patří „Ukončení provádění operace (5)“ a „Nahrazeno (4)“ viz obrázek 18.



Obrázek 18 – Ukázka seznamu CRL

V neposlední řadě certifikáty zahrnují informaci o reálné použitelnosti daného certifikátu, resp. klíče. V poli „Použití rozšířeného klíče“ se u obou certifikátu nachází shodné informace o využitelnosti z hlediska zabezpečení e-mailu (1.3.6.1.5.5.7.3.4) a podepisování dokumentů (1.3.6.1.4.1.311.10.3.12). Problematika možného použití souvisí také s polem „Použití klíče“, ve kterém má první certifikát uvedeny hodnoty „Digitální podpis, Neodvolatelnost, Šifrování klíče (e0)“, v čemž lze spatřovat odlišnost oproti hodnotě stejného pole u druhého certifikátu „Digitální podpis, Neodvolatelnost (c0).“ Neodvolatelnost (Non Repudiation) certifikátu slouží ověření pravosti na základě garance nemožnosti autora zříct se odpovědnosti. Použití certifikátu za účelem „Šifrování klíče“ (Key Encipherment), což je parametr, který má první certifikát oproti druhému navíc, značí možnost zašifrovat symetrický klíč určený k zašifrování dat veřejným klíčem z certifikátu. V takových případech se jedná o kombinaci symetrické a asymetrické kryptografie.[82]

Certifikáty mimo jiné také zahrnují své jedinečné kryptografické otisky, které slouží k ověření platnosti a zajištění integrity proti nežádoucí změně datové struktury.

Tabulka 2 – Vybrané informace o komparovaných certifikátech

Pole	**Hodnota (1. certifikát)**	**Hodnota (2. certifikát)**
Verze	V3	V3
Sériové číslo	00b672b6	0156469f
Algoritmus podpisu	sha512RSA	sha256RSA
Podpisový algoritmus hash	sha512	sha256
Vystavitel	SERIALNUMBER = NTRCZ-26439395 O = První certifikační autorita, a.s. CN = I.CA Qualified 2 CA/RSA 02/2016 C = CZ	CN = PostSignum Qualified CA 4 O = Česká pošta, s.p. 2.5.4.97 = NTRCZ-47114983 C = CZ
Platnost od	pátek 18. února 2022 10:11:13	pátek 16. července 2021 9:15:01
Platnost do	sobota 18. února 2023 10:11:13	pátek 5. srpna 2022 9:15:01

[82] Key usage extensions and extended key usage. *HCL SOFTWARE* [online]. [cit. 28.2.2022]. Dostupné z: https://help.hcltechsw.com/domino/10.0.1/conf_keyusageextensionsandextendedkeyusage_r.html

Subjekt	SERIALNUMBER = ICA - 10628554 SN = Zelený G = Lukáš PostalCode = 25244 STREET = *(neuvedeno z osobních důvodů)* C = CZ S = Středočeský L = Psáry SERIALNUMBER = IDCCZ-*(neuvedeno z osobních důvodů)* CN = Bc. Lukáš Zelený	SERIALNUMBER = P804760 G = Kristýna SN = Marková CN = Bc Kristýna Marková OU = 0091 O = *(neuvedeno z osobních důvodů)* 2.5.4.97 = NTRCZ-*(neuvedeno z osobních důvodů)* C = CZ
Veřejný klíč	RSA (4096 Bits)	RSA (2048 Bits)
Přístup k informacím autority	[1]Přístup k informacím autority Přístupová metoda=Vystavitel certifikátu autority (1.3.6.1.5.5.7.48.2) Alternativní název: URL=http://q.ica.cz/2qca16_rsa.cer [2]Přístup k informacím autority Přístupová metoda=Protokol OCSP (1.3.6.1.5.5.7.48.1) Alternativní název: URL=http://ocsp.ica.cz/2qca16_rsa	[1]Přístup k informacím autority Přístupová metoda=Vystavitel certifikátu autority (1.3.6.1.5.5.7.48.2) Alternativní název: URL=http://crt.postsignum.cz/crt/psqualifiedca4.crt [2]Přístup k informacím autority Přístupová metoda=Protokol OCSP (1.3.6.1.5.5.7.48.1) Alternativní název: URL=http://ocsp.postsignum.cz/OCSP/QCA4/
Zásady certifikátu	[1]Certifikační zásady: Identifikátor zásad=1.3.6.1.4.1.23624.10.1.30.1.1 [1,1]Informace o kvalifikátoru zásad: ID kvalifikátoru zásad=CPS Kvalifikátor: http://www.ica.cz [1,2]Informace o kvalifikátoru zásad: ID kvalifikátoru zásad=Uživatelské oznámení Kvalifikátor: Text oznámení=Tento kvalifikovany certifikat pro elektronicky podpis byl vydan v	[1]Certifikační zásady: Identifikátor zásad=2.23.134.1.4.1.17.200 [1,1]Informace o kvalifikátoru zásad: ID kvalifikátoru zásad=Uživatelské oznámení Kvalifikátor: Text oznámení=Tento kvalifikovany certifikat pro elektronicky podpis byl vydan v souladu s narizenim EU c. 910/2014.This is a qualified certificate for electronic signature

	souladu s narizenim EU c. 910/2014.This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014. [2]Certifikační zásady: Identifikátor zásad=0.4.0.194112.1.0	according to Regulation (EU) No 910/2014. [1,2]Informace o kvalifikátoru zásad: ID kvalifikátoru zásad=CPS Kvalifikátor: http://www.postsignum.cz [2]Certifikační zásady: Identifikátor zásad=0.4.0.194112.1.0
Distribuční místa seznamu	[1]Distribuční místo CRL Název distribučního místa: Jméno a příjmení: URL=http://qcrldp1.ica.cz/2qca16_rsa.crl [2]Distribuční místo CRL Název distribučního místa: Jméno a příjmení: URL=http://qcrldp2.ica.cz/2qca16_rsa.crl [3]Distribuční místo CRL Název distribučního místa: Jméno a příjmení: URL=http://qcrldp3.ica.cz/2qca16_rsa.crl	[1]Distribuční místo CRL Název distribučního místa: Jméno a příjmení: URL=http://crl.postsignum.cz/crl/psqualifiedca4.crl [2]Distribuční místo CRL Název distribučního místa: Jméno a příjmení: URL=http://crl2.postsignum.cz/crl/psqualifiedca4.crl [3]Distribuční místo CRL Název distribučního místa: Jméno a příjmení: URL=http://crl.postsignum.eu/crl/psqualifiedca4.crl
Použití rozšířeného klíče	Zabezpečení e-mailu (1.3.6.1.5.5.7.3.4) Podepisování dokumentů (1.3.6.1.4.1.311.10.3.12)	Zabezpečení e-mailu (1.3.6.1.5.5.7.3.4) Podepisování dokumentů (1.3.6.1.4.1.311.10.3.12)
Použití klíče	Digitální podpis, Neodvolatelnost, Šifrování klíče (e0)	Digitální podpis, Neodvolatelnost (c0)
Kryptografický otisk	651672d0bc23a0674ba1ceaeab827abb1c0ada5f	bbe2a4422b749f111807be0138e58a003ca87fed

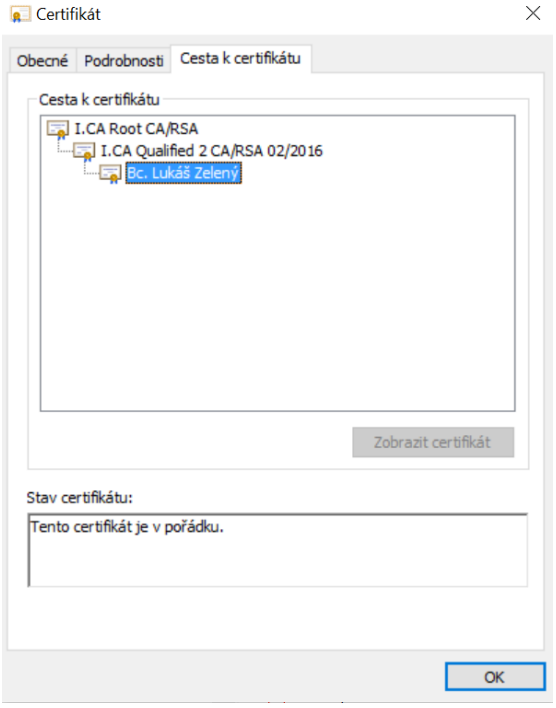
Cesta k certifikátu

Posledním oddílem informační struktury certifikátu je grafické znázornění hierarchické struktury certifikátů. Obecně u kvalifikovaných certifikátů se zpravidla jedná o provázanost základního (kořenového certifikátu) certifikační autority

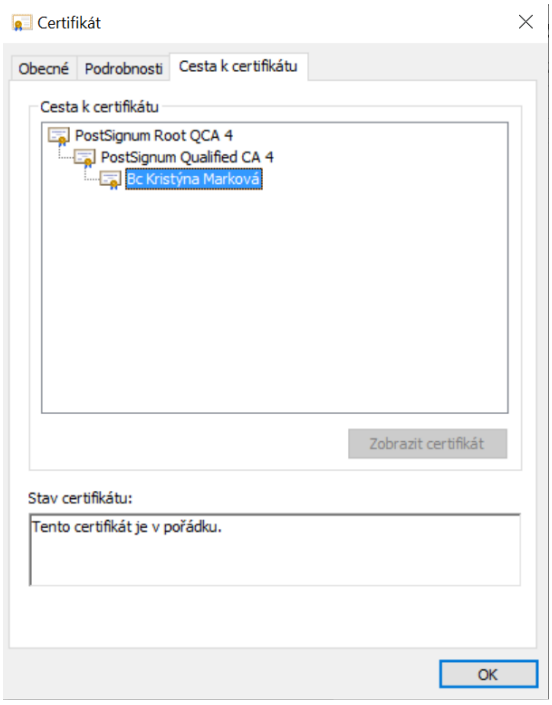
s koncovým osobním certifikátem konkrétního uživatele. V rámci systému uspořádání certifikátů platí vzájemná důvěryhodnost mezi navázanými certifikáty.

Kořenovým certifikátem v případě prvního porovnávaného certifikátu je I.CA Root CA/RSA, který je zároveň vystavitelem pro podřazený certifikát I.CA Qualified 2 CA/RSA 02/2016 sloužící k vystavování kvalifikovaných certifikátů. Poslední v hierarchické struktuře je certifikát vystavený pro konkrétní fyzickou osobu tj. Bc. Lukáše Zeleného (viz obrázek 20).

Druhý komparovaný certifikát má kořenovou autoritu PostSignum Root QCA 4. Navazující certifikát vlastník certifikátu PostSignum Qualified CA 4 vystupuje jako vystavitel pro koncového vlastníka kvalifikovaného certifikátu, tedy Bc. Kristýnu Markovou (viz obrázek 19).



Obrázek 19 – Cesta k prvnímu certifikátu

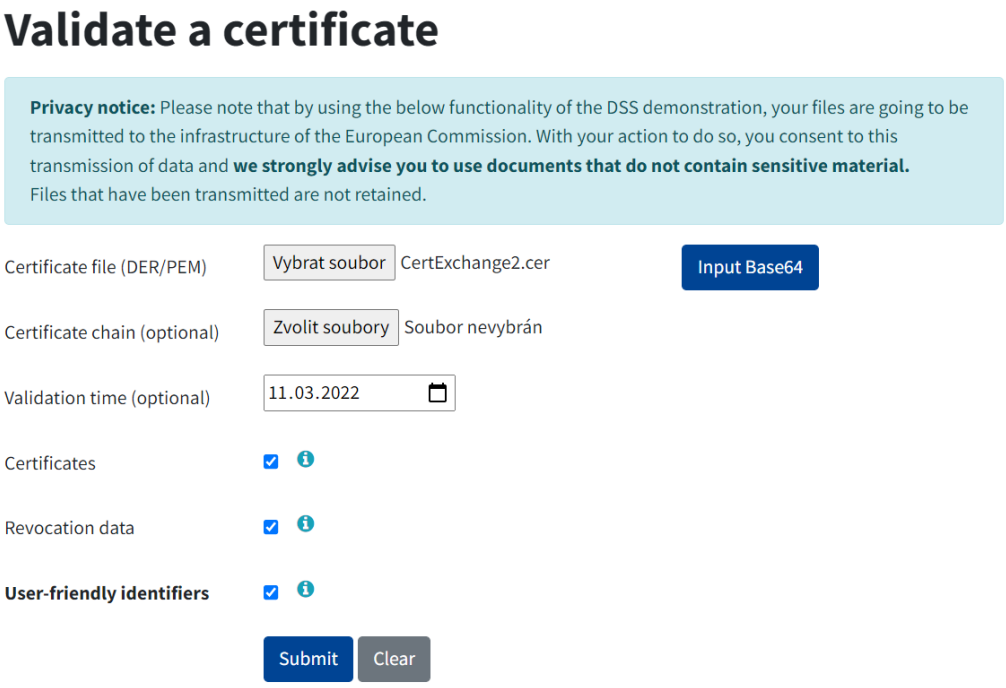


Obrázek 20 – Cesta k druhému certifikátu

7. Analýza certifikátu pomocí on-line nástroje

Předchozí kapitoly ukazují, že schopností ověřit platnost certifikátu zaručeného elektronického podpisu disponuje značná část softwarových nástrojů, které s elektronickými podpisy pracují. Ačkoliv se má za to, že vývojáři aplikací jsou solidní a dělají vše pro to, aby jejich nástroje nevykazovaly žádné významné bezpečnostní riziko, jelikož je to zpravidla především v zájmu softwarových společností, z uživatelského pohledu není vždy možné zajistit nebo ověřit dostatečnou úroveň zabezpečení nebo nežádoucí úpravy daného softwaru. Mimo jiné v kyberprostoru se mohou vyskytovat aplikace, které se tváří jako nástroj pro práci s elektronickými podpisy, avšak jejich reálná funkčnost může být záměrně zkreslena nebo zmanipulována.

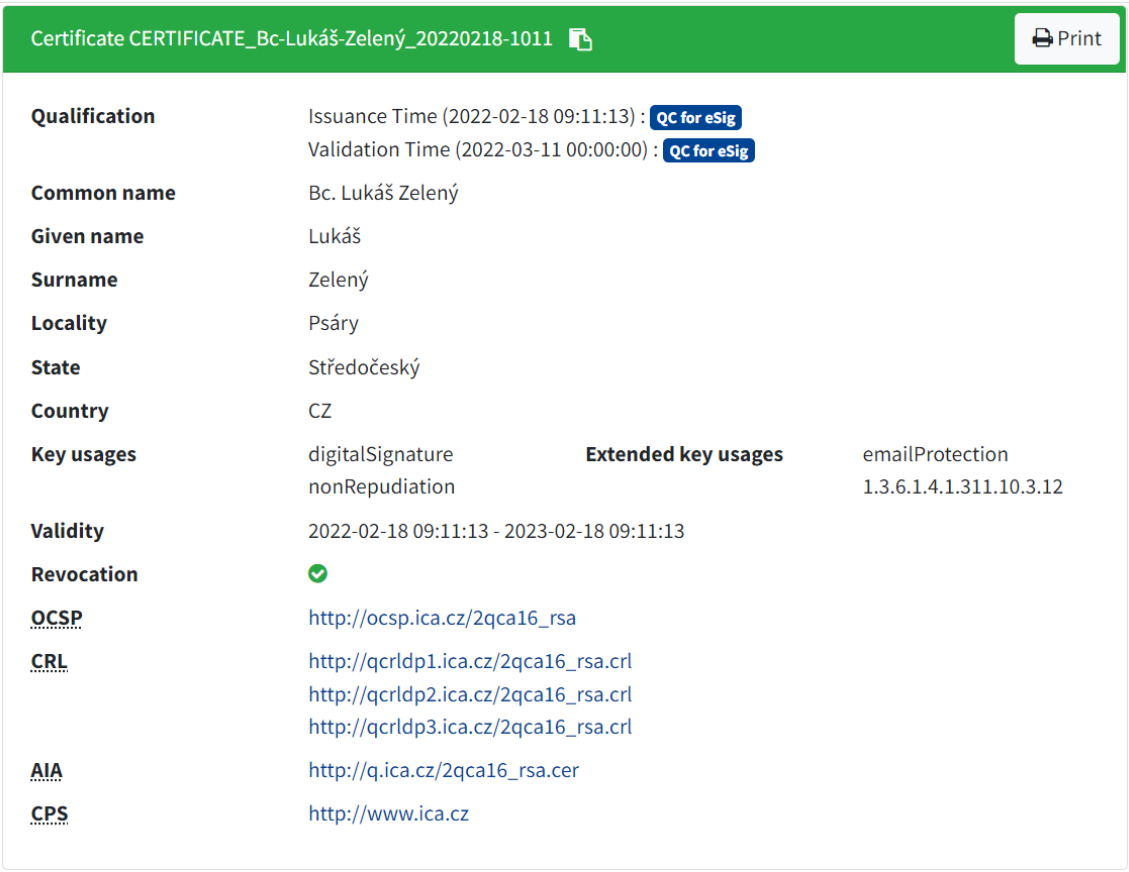
Nejen z výše uvedených důvodů existuje on-line nástroj DSS Demonstration WebApp umístěný v souvislosti s nařízením eIDAS přímo na internetových stránkách Evropské komise (ec.europa.eu/cefdigital/DSS/webapp-demo/home). Rozhraní aplikace je vybaveno množstvím funkcí, které souvisí s elektronickým podepisování souborů, mezi niž se řadí například ověření certifikátu, přidání časového razítka, ověření časového razítka, nebo za předpokladu instalace rozšíření NexU také přímo elektronické podepisování dokumentů.



Obrázek 21 – Rozhraní DSS Demonstration WebApp

Jak je patrné z obrázku 21, pro účely demonstrace funkčnosti nástroje DSS Demonstration WebApp a ověření platnosti kvalifikovaného certifikátu jsem zvolil certifikát, který byl označený jako první porovnávaný certifikát v předchozí kapitole. Soubor s kvalifikovaným certifikátem je nejprve třeba nahrát na server ve formátu DER/PEM. Požadovaný formát certifikátu je možné získat například exportem certifikátu v rámci operačního systému Windows nebo stažením z oficiálního uložiště certifikační autority.

Webová aplikace na základě vstupního souboru provede analýzu dat obsažených v certifikátu a následně zobrazí výsledky ověření. Po vyhodnocení jsou výsledky rozděleny do tří oblastí: jednoduchého přehledu, detailního přehledu a diagnostického stromu.

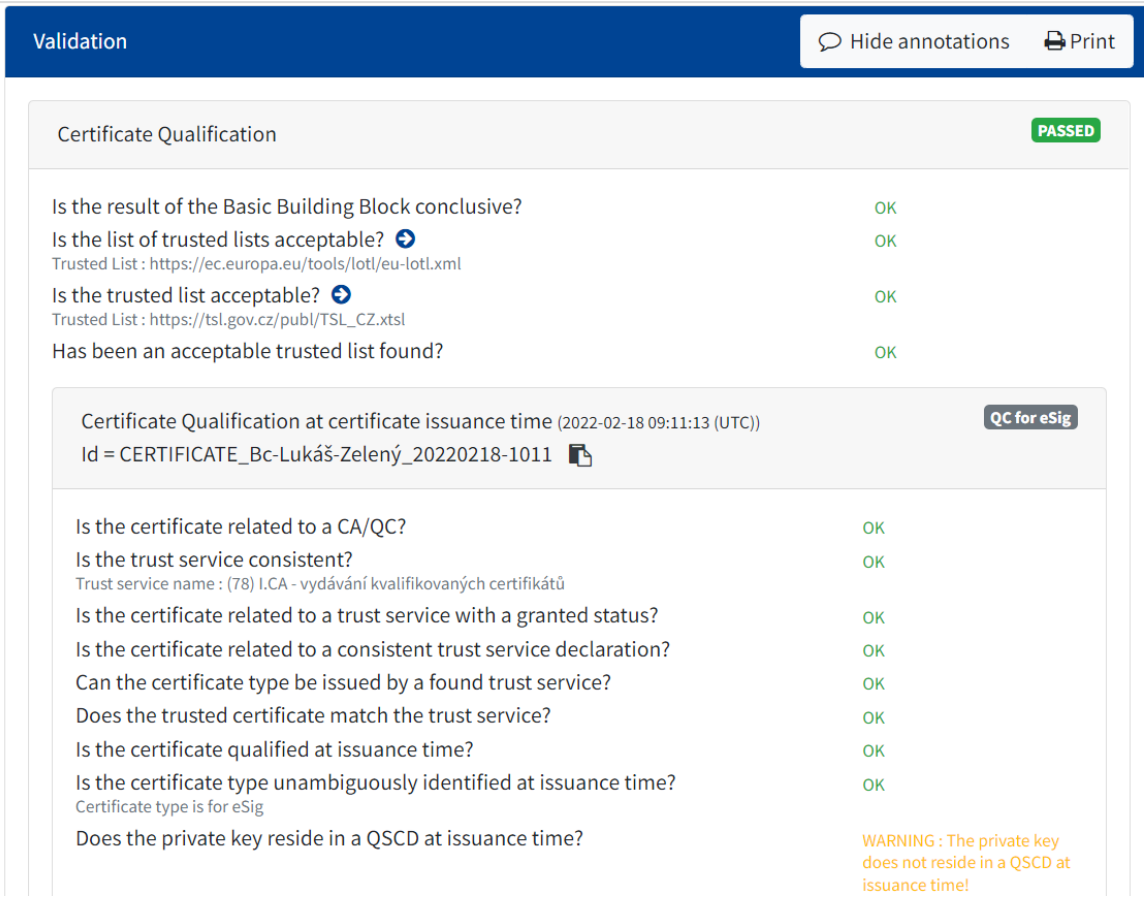


Obrázek 22 – Jednoduchý přehled výsledků on-line analýzy

Jednoduchý přehled zachycený na obrázku 22 obsahuje základní informace o osobním kvalifikovaném certifikátu a dalších navazujících certifikátech včetně kořenového certifikátu v rámci dané hierarchické struktury. Mezi informacemi nechybí základní údaje o vlastníkovi certifikátu (jméno, příjmení, země), časová platnost certifikátu nebo jeho využitelnost. Dále v reportu najdeme

odkazy na OCSP protokol a CRL seznamy. Důležitá je také hodnota „QC for eSig“ v poli „Qualification“, která verifikuje úroveň kvalifikovaného certifikátu za účelem elektronického podepisování. Informace zachycené v jednoduchém přehledu webové aplikace jsou oproti informacím obsaženým v samotném certifikátu značně zredukovány, avšak s originálními hodnotami plně korespondují.

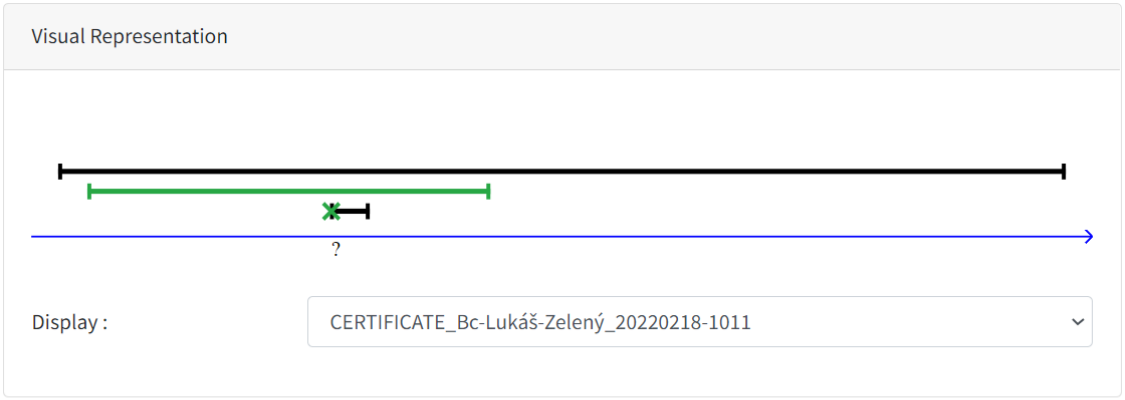
Dalším výstupem, který on-line nástroj uživateli připraví, je detailní přehled obsahující výsledky ověření platnosti certifikátu (viz obrázek 23). Jedná se o formu kontrolního seznamu, kdy program předdefinované otázky uspořádané do jednotlivých bloků na základě procesu validace označí odpovídající hodnotou „OK“ nebo „NOT OK“. Případně se uživatel může setkat s hodnotami „WARNING“ nebo „IGNORED“ s příslušnými komentáři vysvětlujícími důvody k udělení takového statusu.



Obrázek 23 – Úryvek detailního přehledu výsledků on-line nástroje

Na základě analýzy nahraného certifikátu byla drtivá většina hodnot kontrolního seznamu hodnocena pozitivně, čímž došlo verifikaci platnosti a úrovně kvalifikovaného certifikátu. Mezi základní parametry, které nástroj posuzoval,

patřila konzistentnost základní datové struktury certifikátu, platnost oficiálního seznamu důvěryhodných poskytovatelů služeb v EU, jež má nástroj k dispozici ve formátu XML (dostupný z ec.europa.eu/tools/lotl/eu-lotl.xml), platnost seznamu kvalifikovaných poskytovatelů služeb vytvářejících důvěru v ČR (dostupný z tsl.gov.cz/publ/TSL_CZ.xtsl) včetně kontroly začlenění analyzovaného certifikátu do uvedených seznamů. Nástroj dále posuzoval, zdali certifikát ke dni ověření nebyl revokován (včetně důvěryhodnosti revokačního zdroje), nebo zdali není certifikát podepsán sebou samotným, což by znamenalo ztrátu důvěryhodnosti. I přes převažující míru pozitivních výsledků aplikace označila za mírný nedostatek uložiště soukromého klíče, který se v době validace nenacházel na kvalifikovaném prostředku, nýbrž v uložišti počítače. Ačkoliv se jedná o hodnotu pouze na úrovni „WARNING“, kvalifikovaný prostředek by z bezpečnostního hlediska výrazně posilnil postavení kvalifikovaného certifikátu a umožnil elektronicky podepisovat soubory na nevyšší úrovni kvalifikovaných elektronických podpisů.




```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DiagnosticData xmlns="http://dss.esig.europa.eu/validation/diagnostic">
    <ValidationDate>2022-03-11T00:00:00Z</ValidationDate>
    <UsedCertificates>
        <Certificate Id="CERTIFICATE_I-CA-Qualified-2-CA-RSA-02-2016_20160211-1317">
            <SubjectDistinguishedName Format="CANONICAL">2.5.4.5=#130e4e5452435a2d3236343339333935,o=první
            <SubjectDistinguishedName Format="RFC2253">2.5.4.5=#130e4e5452435a2d3236343339333935,O=První ce
            <IssuerDistinguishedName Format="CANONICAL">2.5.4.5=#130e4e5452435a2d3236343339333935,cn=i.ca r
            <IssuerDistinguishedName Format="RFC2253">2.5.4.5=#130e4e5452435a2d3236343339333935,CN=I.CA Roo
            <SerialNumber>100001006</SerialNumber>
            <SubjectSerialNumber>NTRCZ-26439395</SubjectSerialNumber>
            <CommonName>I.CA Qualified 2 CA/RSA 02/2016</CommonName>
            <CountryName>CZ</CountryName>
            <OrganizationName>První certifikační autorita, a.s.</OrganizationName>
            <AuthorityInformationAccessUrls>
                <aiaUrl>http://r.ica.cz/rca15 rsa.cer</aiaUrl>
```

Obrázek 24 – Úryvek výsledků prezentovaných v podobě diagnostického stromu

Třetí, a zároveň poslední, částí výsledků analýzy je diagnostický strom, jehož ukázka je zachycena na obrázku 24, který obsahuje vizuální prezentaci časových platností jednotlivých certifikátů z hierarchické struktury včetně zaznačení okamžiku validace. Dále zde najdeme souhrn diagnostických dat ve formátu XML, které lze využít například jako doklad o nezávislém ověření.

8. Vyhodnocení praktické části a vlastní návrhy

8.1 Vyhodnocení komparace kvalifikovaných certifikátů

Ačkoliv kvalifikované certifikáty pro zaručené elektronické podpisy od dostupných poskytovatelů služeb vytvářejících důvěru na první pohled vykazují množství shodných znaků, stejně jako jiné produkty na trhu mají také své odlišnosti. Rozdíly v technických parametrech certifikátů zpravidla na běžné uživatele nemají zásadní dopady. Velká část poptávajících se tedy dle mého názoru řídí především cenou a dalšími aspekty, které zajišťují pohodlnou a rychlou možnost vystavení kvalifikovaného certifikátu.

Vzhledem k tomu, že oba komparované certifikáty pochází od různých vystavitelů a jsou určeny pro rozdílné osoby, není relevantní zaměřit se na porovnávání osobních údajů zúčastněných subjektů a vystavitelů, jelikož je zcela zřejmé, že zde shoda panovat nebude. V rámci vyhodnocení považuji za vhodné zaměřit se primárně na technické parametry určující kvalitu a sílu zabezpečení a další kritéria na základě pohledu běžného uživatele.

Z hlediska bezpečnosti můžeme velký rozdíl mezi oběma certifikáty spatřovat v použitém podpisovém algoritmu. Algoritmus sha512 produkuje výstup o délce 512 bitů, což je dvojnásobek oproti algoritmu sha256. Z hlediska hashovacích funkcí je zásadním znakem nedostatečné síly tzv. kolize neboli shoda dvou výstupů na základě rozdílných vstupů. Případy kolize se v minulosti vyskytly u starších funkcí generace SHA-0 a SHA-1. Vzhledem k tomu, že algoritmy SHA-256 a SHA-512 patří do skupiny SHA-2, u níž zatím k problémům s kolizemi nedošlo, můžeme oba tyto algoritmy označit za bezpečné, avšak s ohledem na zvyšování výkonnosti zařízení může mít silnější funkce sha512 do budoucna mírnou výhodu.[83]

S problematikou podpisových algoritmů souvisí také rychlost samotných výpočtů. Funkce SHA-256 vyžaduje zpravidla nižší výkon zařízení a méně paměti než SHA-512, avšak může být až o třetinu rychlejší pouze při hashovaní kratších

[83] RHODES, Delton. SHA-512 Hashing Algorithm Overview. *Komodo Platform Blockchain - Home of AtomicDEX and KMD Coin* [online]. Dec 28, 2020 [cit. 28.2.2022]. Dostupné z: https://komodoplatform.com/en/academy/sha-512/

vstupů. Naopak hashování vstupů delších znamená na základě provedených testů vyšší rychlost algoritmu SHA-512.[84]

První certifikační autorita, a. s. dává žadatelům na výběr, zdali chtějí vystavit certifikát s podpisovým algoritmem sha512 a veřejným klíčem RSA (4096 bitů), nebo raději využijí více rozšířeného algoritmu sha256 a veřejného klíče RSA (2048 bitů). Varianta silnějšího podpisového algoritmu byla z mé strany konzultována také s technickou podporou certifikační autority, přičemž se mi dostalo upozornění na teoretickou možnost nižší kompatibility silnější funkce. Dle slov pracovníka CA je reálná úroveň zabezpečení v praxi téměř shodná, pro běžného uživatele naprosto dostačující.

Dalším, z mého pohledu podstatným, rozdílem mezi porovnávanými certifikáty je odlišná doba platnosti. Ačkoliv se jedná o kvalifikované certifikáty určené pro zaručený (popř. kvalifikovaný) elektronický podpis od certifikačních autorit se stejnou úrovní akreditace, doba platnosti prvního certifikátu je o 20 dní kratší než platnost druhého certifikátu, a zároveň cena prvního certifikátu o 149 Kč vyšší než cena certifikátu druhého, a to i přes to, že jejich využitelnost a úroveň zabezpečení je velmi podobná. Ačkoliv je třeba respektovat, že cenotvorba a další podmínky jsou plně v kompetenci prodejce, nesoulad mezi cenami kvalifikovaných certifikátů od jednotlivých certifikačních autorit a dobou jejich platnosti pohledem běžného zákazníka vnímám jako jistou nevýhodu nabídky kvalifikovaných certifikátů od společnosti První certifikační autorita, a. s.

Oba certifikáty také obsahují poměrně výrazně odlišné typy hodnot v poli s informacemi o subjektu, které pro získání a ověření důležitých údajů o podepisující osobně mají zásadní roli. Vzhledem k tomu, že vystavitel certifikátu ověřuje totožnost žadatele před vydáním certifikátu, má se za to, že osobní údaje uvedené v takovém poli jsou v době vystavení validní. Z hlediska účelnosti certifikátu v oblasti přesné identifikace podepisující osoby lze považovat za vhodnější první certifikát, jelikož obsahuje veškeré podstatné náležitosti identifikace osoby jako je jméno, příjmení, adresa trvalého pobytu a číslo

[84] LATINOV, Lyudmil. MD5, SHA-1, SHA-256 and SHA-512 speed performance: Post summary: Speed performance comparison of MD5, SHA-1, SHA-256 and SHA-512 cryptographic hash functions in Java. *Automation Rhapsody* [online]. 18. 01. 2022 [cit. 28.2.2022]. Dostupné z: https://automationrhapsody.com/md5-sha-1-sha-256-sha-512-speed-performance/

občanského průkazu, které se u druhého certifikátu nevyskytují. Druhý certifikát naopak obsahuje navíc informace o zainteresované společnosti. Na první pohled je tedy zřejmé, první certifikát je na základě uvedených osobních údajů ryze osobní povahy, kdyžto druhý byl vystaven sice také pro konkrétní fyzickou osobu, avšak primárně k pracovním účelům.

S problematikou identifikace osob vůči orgánům státní správy se pojí také další důležitý unikátní údaj, kterým je identifikátor MPSV, jímž disponuje pouze první certifikát. Údaje o subjektu se v certifikátech objevují primárně na základě informací uvedených v žádosti o certifikát. Velká část těchto osobních údajů s výjimkou jména a příjmení není CA přímo vyžadována (např. adresa trvalého bydliště), jelikož se může jednat o citlivé osobní údaje, které se stávají uvedením v certifikátu prakticky veřejné, tudíž snáze dohledatelné a zneužitelné. Protiargumentem může být však domněnka, že tyto osobní údaje výrazně přispívají důvěryhodnosti kvalifikovaného certifikátu a navazujícího elektronického podpisu nejen v rámci komunikace s veřejnoprávními institucemi, ale také mezi subjekty soukromoprávními.

8.2 Vyhodnocení analýzy certifikátu pomocí on-line nástroje

Vzhledem k tomu, že webová aplikace DSS Demonstration WebApp je umístěna přímo na internetových stránkách Evropské komise, jakožto jednoho z nejvýše postavených orgánů EU, samotná důvěryhodnost nástroje je do značné míry garantována již samotným provozovatelem domény.

Jelikož kvalifikované certifikáty jsou za určitých podmínek využitelné k elektronickému podepisování dokumentů a zpráv v rámci komunikace napříč veřejnoprávními a soukromoprávními subjekty v celé Evropské unii, považuji za žádoucí mít k dispozici volně dostupný on-line nástroj pro nezávislou validaci certifikátů s přehlednou interpretací výsledků.

Výsledky ověření platnosti certifikátu pomocí DSS Demonstration WebApp dle mého názoru reflektují vlastnosti certifikátu deklarované certifikační autoritou, dále jednotlivé výstupy ověření platnosti certifikátu pomocí komerčních softwarů (např. Acrobat Adobe Reader) a v neposlední řadě také osobní analýzy, kterou jsem zpracoval za účelem komparace kvalifikovaných certifikátů. Report

jednoznačně deklaruje možnost využití certifikátu pro účely elektronického podepisování.

S ohledem na aktuální dispozice analyzovaného kvalifikovaného certifikátu je možné jej použít pouze k vytvoření zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, nikoliv však jako kvalifikovaný elektronický podpis, k němuž je navíc zapotřebí uložení soukromého klíče na kvalifikovaném prostředku, což je na základě reportu spatřováno jako určitý nedostatek.

8.3 Vyhodnocení hypotéz

Na základě poznatků získaných během zpracování diplomové práce došlo k ověření platnosti jednotlivých hypotéz. První hypotéza prohlašuje, že kvalifikované certifikáty od různých certifikačních autorit nabízí shodnou úroveň bezpečnosti. Druhá hypotéza tvrdí, že zaručený elektronický podpis je vhodným nástrojem k zabezpečení dokumentu proti nežádoucím úpravám.

Vzhledem k tomu, že jednotlivé technické parametry zajišťující zabezpečení kvalifikovaných certifikátů (např. Algoritmus podpisu) jsou na základě ověření výsledků během komparace jednotlivých certifikátů odlišené, nemůže být totožná ani úroveň bezpečnosti kvalifikovaných certifikátů. V praxi při běžném používání se úroveň zabezpečení příliš neliší, avšak i přes to první hypotéza byla vyvrácena.

Aplikace zaručeného elektronického podpisu na dokument díky používaným kryptografickým metodám (především hashovaní) zajišťuje integritu dat obsažených v dokumentu. Jakákoliv změna učiněná v podepsaném dokumentu znamená odlišný výstupní hash. Výsledný nesoulad hashů je vyhodnocen jako porušení integrity dat. Na základě analýzy technické procedury zaručeného elektronického podpisu byla hypotéza potvrzena.

8.4 Vlastní návrhy

I přes to, že oblast digitalizace veřejného i soukromého sektoru prošla v posledních letech velkým rozmachem a určitá odvětví IT mimo jiné díky globální pandemii COVID-19 zažily exponenciální růst (např. sektor e-commerce), problematiku elektronického podpisu lze označit za relativní konstantní, jelikož její

základy, které jsou i v dnešní době z velké části stále platné, byly vytvořeny již před několika desítkami let. S rostoucím trendem rozvoje informačních technologií však expanduje také zájem o elektronickou komunikaci nejen mezi fyzickými a právnickými osobami v soukromém sektoru, ale také s orgány státní správy, samosprávy a jinými veřejnoprávními institucemi.

Dle mého názoru byla právě koronavirová pandemie jedním z největších „katalyzátorů“ zájmu o elektronickou komunikaci, jelikož úřední hodiny podatelen byly výrazně zkráceny, což citelně omezilo možnost osobního podání dokumentů. Do popředí se tedy více dostávaly alternativní služby, prostřednictvím kterých je možné osobní doručovaní písemností nahradit. Vzhledem k tomu, že návštěva poboček poskytovatelů poštovních služeb představovala relativně vysoké zdravotní riziko, logickou náhradou byly varianty elektronické komunikace.

Ačkoliv problematika datových schránek byla nastíněna již v teoretické části práce, z hlediska její souvislosti s elektronickými podpisy považuji za vhodné provázat obě oblasti konkrétními doporučeními. Princip fungování elektronického podepisování a informačního systému datových schránek je určitých sférách velmi odlišný, jelikož elektronický podpis se zaměřuje na zabezpečení a zajištění integrity dokumentu, ale dále neřeší proces jeho bezpečného transferu k příjemci, kdežto datové schránky zajišťují zabezpečený přenos dat mezi odesílatelem a příjemcem, avšak nedochází k aplikaci žádné kryptografické metody, která by integritu dokumentu zaručila. Za účelem zajištění vyšší úrovně bezpečnosti tedy doporučuji uživatelům využívat kombinaci informačního systému datových schránek, jakožto jednoduchého, rychlého a bezpečného prostředku komunikace, a zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu (popř. kvalifikovaného elektronického podpisu), díky čemuž dokument získá garanci neměnnosti.

Z mého pohledu spatřuji obrovský potenciál využitelnosti elektronického podpisu v elektronických občanských průkazech s integrovanými čipy, které jsou již řadu let v oběhu a na základě průběžné obměny budou zanedlouho k dispozici většině občanů České republiky. Jelikož elektronické občanské průkazy vydávané od roku 2018 jsou kvalifikovanými prostředky ve smyslu příslušného nařízení EU, občané je mohou využívat pro vytváření kvalifikovaných elektronických podpisů. Uživatelům díky tomu odpadnou náklady na pořízení čipových karet nebo USB

tokenů, a zároveň se výrazně usnadní celý proces, jelikož v takovém případě postačí pouze kvalifikovaný certifikát a čtečka čipových karet splňující požadavky nařízení eIDAS. Dle mého názoru není tato možnost ze strany státu dostatečně prezentována, a to i přes to, že se jedná o jeden z důležitých kroků směrem k digitalizaci státní správy. Osobně bych se také navrhoval projednat možnosti přímé implementace kvalifikovaných certifikátu na elektronické občanské průkazy s tím, že pozici kvalifikované certifikační autority by zajišťovala státní instituce (např. Správa základních registrů, která nyní již roli certifikační autority pro určité skupiny osob zastává). Tímto krokem by se výrazně usnadnil proces, který předchází vytváření kvalifikovaného elektronického podpisu, jelikož uživatelům by scházela pouze zmiňovaná čtečka čipových karet, za pomocí které by mohli elektronický podpis aplikovat.

Dále z hlediska zvýšení povědomí o možnostech využívání kvalifikovaných certifikátů pro zaručené elektronické podpisy bych navrhoval zajistit větší marketingovou propagaci, která by nejen fyzickým osobám a OSVČ, ale také právnickým osobám dokázala objasnit výhody využívání elektronického podepisování a přesvědčila je využívat taková řešení při svých činnostech. Dle mého názoru by na takové propagaci měl mít zájem primárně stát, jelikož využívání informačních a digitálních technologií v dlouhodobém horizontu šetří čas i finance. Konkrétně bych navrhoval například předkládat informační sdělení ve formě letáku občanovi v rámci procesu žádosti o vydání občanského průkazu, na kterém by byly jednoznačně prezentovány možnosti využití integrovaného čipu k elektronickému podpisování včetně dalších výhod, mezi které patří především využitelnost kvalifikovaného podpisu v členských státech EU.

Míra zájmu o kvalifikované certifikáty může být částečně ovlivněna také kvalitou procesu žádosti. Dle mého názoru by celý proces měl být co nejjednodušší. Při tvorbě formulářů by se certifikační autority měly zaměřit především na přehlednost a srozumitelnost obsahu. Z osobní zkušenosti mohu proces žádosti u společnosti První certifikační autorita, a. s. až na malé drobnosti ohodnotit kladně. Požadavky byly interpretovány stručně a výstižně. Žádost o vydání kvalifikovaného certifikátu u společnosti Česká pošta, s. p. je podle mě méně uživatelsky přívětivá. Negativně hodnotím především požadavek ze strany certifikační autority na stažení a vyplnění Smlouvy o poskytování certifikačních

služeb a Údajů pro vydávání certifikátu (formát PDF), vytištění a následně osobní doručení dokumentů na některou z poboček Czech Point za účelem vydání žádosti. Tento postup je dle mého názoru v přímém rozporu se snahou o digitalizaci, přičemž předání všech potřebných údajů by bylo možné vyřešit jednoduše prostřednictvím webových formulářů.

V neposlední řadě vnímám jako ne příliš příznivé poměrně značné cenové rozdíly kvalifikovaných certifikátů u jednotlivých certifikačních autorit. Cenotvorbu certifikačních autorit plně respektuji, avšak dle mého názoru by bylo vhodné zvážit například zavedení bonusových programů pro dlouhodobé spolupráce, které by v delším časovém horizontu snížily náklady zákazníkovi a potenciálně zvýšily zájem o řešení v podobě elektronického podepisování.

Účelem nastínění vlastních návrhů není snaha o masivní budování povědomí o elektronickém podepisování a vyzdvihování pozitivních stránek na úkor jiných obdobných nástrojů, ale spíše snaha o postupný a přirozený přechod do digitálního prostředí i pro běžné uživatele, kteří si nejsou jisti vhodným způsobem elektronické komunikace. Dle mého názoru problematika elektronického podpisu není příliš mezi veřejností rozšířena, což vnímám do jisté míry jako příležitost, protože funkce elektronického podpisu by mohly usnadnit každodenní činnosti spoustě uživatelů.

ZÁVĚR

Digitalizaci veřejného i soukromého sektoru lze označit za kontinuální proces, jemuž naše společnost čelí již několik desítek let. Některé sféry přechází do digitálního prostředí snáze a rychleji a jiné naopak čelí množství legislativních, finančních, technických a jiných překážek a nástrah, se kterými je třeba nejprve se vypořádat, aby proces mohl pokračovat dále k úspěšnému naplnění stanoveného cíle. Typickým příkladem obrovské expanze oblasti v on-line prostředí je internetové obchodování, které především v posledních letech zažívá značný rozmach umocněný především celosvětovou koronavirovou pandemií a technologickým pokrokem.

S postupným přesunem služeb do virtuálního prostředí, modernizací a zvyšováním dostupnosti techniky dochází k zintenzivnění rizika nežádoucího chování kybernetických útočníků. Vzhledem k rychlému vývoji informačních a komunikačních technologií je nezbytně nutné udržovat na dostatečné úrovni také systémy ochrany a zabezpečení. Kyberprostor je místem skrývajícím nové hrozby, což mimo jiné dokládá také aktuální situace mezi Ukrajinou a Ruskou federací. Tyto země jsou kromě válečného konfliktu zapojeny také do kybernetické války, která svými dopady může způsobit rozsáhlé materiální, finanční nebo i jiné závažnější škody.

Veškeré hrozby a rizika plynoucí z digitalizace dat je třeba v maximální možné míře eliminovat. Ochrana před nežádoucími vlivy není pouze v kompetenci hlavních představitelů a odpovědných osob z centrální úrovně, ale funkčnost celého systému informační bezpečnosti vychází již od samotných uživatelů, kteří musí k úkonům vždy přistupovat zodpovědně a obezřetně. Z hlediska zvýšení bezpečnosti a důvěryhodnosti elektronické komunikace je využíván mimo jiné také elektronických podpis.

Diplomová práce se zaměřuje na problematiku elektronického podpisu, která především v oblasti elektronické komunikace se státní správou hraje významnou roli. Cílem práce bylo vytvoření souboru relevantních poznatků o problematice elektronického podpisu se zaměřením na jednotlivé úrovně důvěryhodnosti, související nástroje, technické principy a metody zabezpečení a v neposlední řadě také vhodné alternativy s následnou aplikací v rámci praktické

části práce v podobě elektronického podepsání dokumentu, komparace dvou kvalifikovaných certifikátů a analýzou platnosti certifikátu za použití nezávislého on-line nástroje.

Vyšší formy elektronického podpisu jsou velmi výhodným prvkem elektronické komunikace, jelikož zajišťují integritu podepsaného dokumentu, což dává protistraně garanci neměnnosti dat od okamžiku podepsání až do ověření, a zároveň jsou jejich certifikáty vystaveny důvěryhodnou certifikační autoritou, která zajišťuje ověření totožnosti podepisující osoby při vystavení certifikátu. Elektronický podpis však není komplexní nástroj, který by řešil zabezpečení samotné komunikace, tudíž je vhodné jej využívat v kombinaci s bezpečným prostředkem pro přenos dat mezi klientem a serverem.

Všichni uživatelé, kteří přichází do styku nejen s elektronickým podpisem, ale také s jinými formami elektronické komunikace, by měli získat alespoň základní povědomí o případných rizicích, která se při elektronickém podepisování a následné komunikaci mohou vyskytnout. Základním předpokladem pro bezpečné využívání elektronického podpisu je důkladné ověřování platnosti podpisových certifikátů, spolehlivé uložiště privátního klíče, využívání šifrovaných komunikačních kanálů a v neposlední řadě také vhodný výběr aplikace pro práci s elektronickými podpisy.

SEZNAM POUŽITÉ LITERATURY

Monografie

[1] BUDIŠ, Petr, Ludwig GRAMLICH a Bohumír ŠTĚDROŇ. *Sichere elektronische Kommunikation: Rechtliche, wirtschaftliche und technische Perspektiven*. Chemnitz: GUC - Verlag der Gesellschaft für Unternehmensrechnung und Controlling, 2009. ISBN 978-3-934235-77-9.

[2] BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi*. Olomouc: ANAG, 2008. ISBN 978-80-7263-465-1.

[3] DONÁT, Josef, Martin MAISNER a Robert PIFFL. *Nařízení eIDAS: komentář.* Praha: C.H. Beck, 2017. ISBN 978-80-7400-633-3.

[4] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[5] DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* 2., aktualiz. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2619-6.

[6] HUSEBY, Sverre H. *Zranitelný kód*. Brno: Computer Press, 2006. ISBN 80-251-1180-6.

[7] KMENT, Vojtěch. *Elektronické právní jednání: Analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU, České republiky a Německa*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-814-8.

[8] MATYÁŠ, Vašek. *Autentizace uživatelů a autorizace elektronických transakcí: příručka manažera = User authentication and electronic transaction authorization : manager's handbook*. Praha: Tate International, 2007. ISBN 978-80-86813-14-1.

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

[10] STALLINGS, William. *Cryptography and network security: principles and practice*. 5th ed. Boston: Prentice Hall, c2011. ISBN 978-0-13-705632-3.

[11] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: CP Books, 2005. ISBN 80-251-0417-6.

Časopisecké články

[12] PETERKA, Jiří. Elektronický podpis v praxi (1): uznávaný, nebo jen zaručený?. *Computerworld*. 2012, roč. 23, č. 3, s. 30. ISSN 1210-9924.

Zákonná úprava a interní akty řízení

[13] 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 dne 1. 7. 2016*

[14] Zákon č. 227/2000 Sb., *o elektronickém podpisu a o změně některých dalších zákonů* v posledním znění

[15] Zákon č. 250/2017 Sb., *o elektronické identifikaci* v posledním znění

[16] Zákon č. 297/2016 Sb., *o službách vytvářejících důvěru pro elektronické transakce* v posledním znění

[17] Zákon č. 300/2008 Sb., *o elektronických úkonech a autorizované konverzi dokumentů* v posledním znění

[18] Zákon č. 499/2004 Sb., *o archivnictví a spisové službě a o změně některých zákonů* v posledním znění

Webové stránky a elektronické zdroje

[19] *Adobe ČR: Řešení pro kreativce, marketing a správu dokumentů* [online]. [cit. 25.2.2022]. Dostupné z: https://www.adobe.com/cz/

[20] Algoritmus RSA. *Expedited Security* [online]. [cit. 27.2.2022]. Dostupné z: https://www.algoritmy.net/article/4033/RSA

[21] BLÜMELOVÁ, Kristina Kadlas. Nařízení eIDAS je základem spolehlivé elektronické identifikace a služeb vytvářejících důvěru. *Technický týdeník* [online]. 25. 10. 2021 [cit. 6.2.2022]. Dostupné z: https://www.technickytydenik.cz/rubriky/ict/narizeni-eidas-je-zakladem-spolehlive-elektronicke-identifikace-a-sluzeb-vytvarejicich-duveru_54320.html

[22] BRUNCLÍK, Zdeněk. Listinná, nebo elektronická agenda?. *Moderní obec* [online]. [cit. 9.1.2022]. Dostupné z: https://www.moderniobec.cz/listinna-nebo-elektronicka-agenda/

[23] Časová razítka. *Česká pošta* [online]. [cit. 29.1.2022]. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/casova-razitka

[24] *Datové schránky* [online]. [cit. 12.2.2022]. Dostupné z: https://www.datoveschranky.info/

[25] *Digitální Podpis* [online]. [cit. 6.2.2022]. Dostupné z: https://www.digitalni-podpis.cz/

[26] DOLEČEK, Marek. Využívejte elektronické podpisy a elektronickou identitu. Poradíme, jak na to. *BusinessInfo.cz* [online]. 28. 11. 2021 [cit. 21.1.2022]. Dostupné z: https://www.businessinfo.cz/navody/elektronicke-podpisy-elektronicka-identita-ppbi/2/#zaruceny-elektronicky-podpis-zalozeny-na-nekvalifikovanem-certifikatu

[27] DURČÁK, Pavel. Symetrické a asymetrické šifrování. *NaPočítači.cz* [online]. 18. 9. 2018 [cit. 29.1.2022]. Dostupné z: https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/

[28] *EARCHIVACE.CZ* [online]. [cit. 29.1.2022]. Dostupné z: http://www.earchivace.cz/

[29] *Elektronický Podpis* [online]. [cit. 6.2.2022]. Dostupné z: https://www.elektronickypodpis.cz/

[30] HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *EPRAVO.CZ: Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. 22. 1. 2020 [cit. 16.1.2022]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

[31] *I.CA* [online]. [cit. 19.2.2022]. Dostupné z: https://www.ica.cz/

[32] Jak zjistím, zda můj kvalifikovaný certifikát obsahuje Identifikátor MPSV?. *EPodpora aplikací Daňového portálu - Finanční správa* [online]. [cit. 27.2.2022]. Dostupné z: https://epodpora.mfcr.cz/cs/seznam-

okruhu/certifikaty-elektronicky-podpis/jak-zjistim-zda-muj-kvalifikovany-certif-4439

[33] Kapitola 6 – Šifrování a elektronický podpis. *Univerzita Tomáše Bati ve Zlíně* [online]. [cit. 30.1.2022]. Dostupné z: https://www.utb.cz/cvt/bezpecnost-sifrovani-elektronicky-podpis/

[34] Key usage extensions and extended key usage. *HCL SOFTWARE* [online]. [cit. 28.2.2022]. Dostupné z: https://help.hcltechsw.com/domino/10.0.1/conf_keyusageextensionsandextendedkeyusage_r.html

[35] KOLÁŘ, Milan. FOTO Jaromír Jágr a hokejové kluby jeho života. *Aktuálně.cz* [online]. 24. 7. 2013 [cit. 14.3.2022]. Dostupné z: https://sport.aktualne.cz/hokej/foto-jaromir-jagr-a-hokejove-kluby-jeho-zivota/r~c3196d5aef9111e2b9470025900fea04/

[36] Konverze. *Czech POINT* [online]. [cit. 9.1.2022]. Dostupné z: https://www.czechpoint.cz/public/verejnost/autorizovana-konverze/

[37] KORBEL, František a Dalibor KOVÁŘ. Nařízení eIDAS konečně adaptováno do českého práva, zákon o elektronickém podpisu končí. *Právní prostor* [online]. 13. 10. 2016 [cit. 23.1.2022]. Dostupné z: https://www.pravniprostor.cz/clanky/procesni-pravo/narizeni-eidas-konecne-adaptovano-do-ceskeho-prava-zakon-o-elektronickem-podpisu-konci

[38] LATINOV, Lyudmil. MD5, SHA-1, SHA-256 and SHA-512 speed performance: Post summary: Speed performance comparison of MD5, SHA-1, SHA-256 and SHA-512 cryptographic hash functions in Java. *Automation Rhapsody* [online]. 18. 01. 2022 [cit. 28.8.2022]. Dostupné z: https://automationrhapsody.com/md5-sha-1-sha-256-sha-512-speed-performance/

[39] *Lupa.cz: server o českém internetu* [online]. [cit. 29.1.2022]. Dostupné z: https://www.lupa.cz/

[40] *Magazín Egovernment* [online]. [cit. 13.2.2022]. Dostupné z: https://www.egovernment.cz/

[41] *Ministerstvo vnitra České republiky* [online]. [cit. 12.2.2022]. Dostupné z: https://www.mvcr.cz/

[42] NAVARA, David. Elektronický podpis prostý. *INOXI: Správa firemních IT & ICT sítí* [online]. 2. 4. 2021 [cit. 16.1.2022]. Dostupné z: https://www.elektronicky-podpis.info/pojmy/elektronicky-podpis-prosty.dot

[43] NOHE, Patrick. Re-Hashed: The Difference Between SHA-1, SHA-2 and SHA-256 Hash Algorithms. *Hashed Out by The SSL Store* [online]. 9 November 2018 [cit. 27.2.2022]. Dostupné z: https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/

[44] O projektu: Jeden z největších digitalizačních projektů českého bankovního sektoru. *Bankovní identita* [online]. [cit. 13.2.2022]. Dostupné z: https://bankovni-identita.cz/o-projektu/

[45] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra. *Advokátní deník* [online]. 4. 5. 2020 [cit. 15.1.2022]. Dostupné z: https://advokatnidenik.cz/2020/05/04/podepisovani-soukromych-listin-vcera-dnes-a-zitra/

[46] *PostSignum* [online]. [cit. 26.2.2022]. Dostupné z: https://www.postsignum.cz/

[47] PRŮŠA, Jiří. Nařízení eIDAS přehledně a srozumitelně: v deseti otázkách a odpovědích. *CZ.NIC: SPRÁVCE DOMÉNY CZ* [online]. [cit. 12.3.2022]. Dostupné z: https://www.nic.cz/files/nic/doc/ITSystems_eIDAS_092016.pdf

[48] RHODES, Delton. SHA-512 Hashing Algorithm Overview. *Komodo Platform Blockchain - Home of AtomicDEX and KMD Coin* [online]. Dec 28, 2020 [cit. 28.2.2022]. Dostupné z: https://komodoplatform.com/en/academy/sha-512/

[49] So you're making an RSA key for an HTTPS certificate. What key size do you use?: Or: why you probably don't want a 4096 bit RSA cert. *Expedited Security: Security as a Service for Heroku, AWS and Google Cloud Applications* [online]. 12 July 2021 [cit. 27.2.2022]. Dostupné z: https://expeditedsecurity.com/blog/measuring-ssl-rsa-keys/

[50] VODIČKA, Milan. Elektronický doklad - kam s ním a jak? *Daně, účetnictví, právo, práce a mzdy pro profesionály* [online]. 4. 4. 2018 [cit. 9.1.2022]. Dostupné z: https://www.du.cz/33/elektronicky-doklad-kam-s-nim-a-jak-

uniqueidmRRWSbk196FNf8-jVUh4Ese1lEiNjoMQoi3ehGYe2PDmmVIyNELpDA/

[51] VRÁNA, Ivo. Elektronická pečeť dle eIDAS – jak a co vlastně pečetit?. *Nástroje pro multifaktorovou autentizaci a PKI infrastrukturu – ProID* [online]. [cit. 23.1.2022]. Dostupné z: https://proid.cz/elektronicka-pecet-dle-eidas-jak-a-co-vlastne-pecetit/

[52] VRBA, Roman. *Metodický pokyn k elektronickým podpisům a pečetím pro veřejnoprávní původce* [online]. 12. 4. 2019 [cit. 29.1.2022]. Dostupné z: https://www.mvcr.cz/soubor/metodicky-material-k-problematice-peceteni-zsvd.aspx

[53] Vyznejte se v elektronické archivaci III: Princip elektronického podpisu. *EDIZONE: Informační portál* [online]. 17. 03. 2016 [cit. 6.2.2022]. Dostupné z: https://www.edizone.cz/technologie-a-trh/vyznejte-se-v-elektronicke-archivaci-iii-princip-elektronickeho-podpisu/

[54] What is a Qualified Electronic Signature (QES) and its characteristics. *Electronic IDentification - IDentity Verification Solutions* [online]. 19. 4. 2021 [cit. 22.1.2022]. Dostupné z: https://www.electronicid.eu/en/blog/post/qualified-electronic-signature/en

[55] What Is an X.509 Certificate?. *SSL.com* [online]. 23 September 2019 [cit. 26.2.2022]. Dostupné z: https://www.ssl.com/faqs/what-is-an-x-509-certificate/#

SEZNAM ZKRATEK

AdES	Advanced Electronic Signature
AdESQC	Advanced Electronic Signature based on a Qualified Certificate
CA	Certification Authority
CPS	Certifikační prováděcí směrnice
CRL	Certificate revocation list
ČR	Česká republika
DPH	Daň z přidané hodnoty
eIDAS	electronic IDentification, Authentication and trust Services
EU	Evropská unie
IČO	Identifikační číslo osoby
IT	Informační technologie
MPSV	Ministerstvo práce a sociálních věcí
OCSP	Online Certificate Status Protocol
OP	Občanský průkaz
OSVČ	Osoba samostatně výdělečně činná
QES	Qualified Electronic Signature
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TS	Time Stamp
TSA	Time Stamping Authority
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ A TABULEK

Seznam obrázků

Seznam tabulek