VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Kristýna Mlčáková

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH SYSTÉMU PRO SPRÁVU ELEKTRONICKÝCH DOKUMENTŮ
DESIGN OF AN ELECTRONIC DOCUMENT MANAGEMENT SYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Kristýna Mlčáková**
AUTHOR

VEDOUCÍ PRÁCE — **JUDr. Pavel Loutocký, BA (Hons), Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Kristýna Mlčáková ***ID:*** 211323

Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Návrh systému pro správu elektronických dokumentů

POKYNY PRO VYPRACOVÁNÍ:

Práce by se měla zabývat základním návrhem systému, který by spravoval elektronické dokumenty, a to dostatečně důvěryhodným způsobem tak, aby mohly být takové dokumenty využity v rámci elektronického dokazování tak, aby nebyla zbytečně snižována důkazní spolehlivost elektronického dokumentu. Teoretická část se bude věnovat adekvátní analýze právní úpravy (jak soukromoprávní, tak veřejnoprávní), praktická část pak návrhem toho, jak by takový systém měl a mohl vypadat. Cílem práce je zanalyzovat dané prostředí a navrhnout možné přístupy k tomu, jak vhodně spravovat a ukládat elektronický dokument tak, aby byla zajištěna jeho dostatečná důkazní spolehlivost. Konkrétní výstup práce pak představuje návrh systému pro správu elektronických dokumentů respektující identifikované zákonné požadavky.

DOPORUČENÁ LITERATURA:

[1] Kapitola 5. POLČÁK, Radim, Matěj MYŠKA, Petr HOSTAŠ, František KASL, Tereza KYSELOVSKÁ, Tomáš LECHNER, Pavel LOUTOCKÝ, Jakub MÍŠEK, Jan TOMÍŠEK, Václav STUPKA a Miroslav UŘIČAŘ. Právo informačních technologií. Praha: Wolters Kluwer, 2018. 656 s. ISBN 978-80-7598-045-8.

[2] Komentářová literatura k § 562 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: JUDr. Pavel Loutocký, BA (Hons), Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

UPOZORNĚNÍ:
Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Bakalářská práce se věnuje problematice elektronických dokumentů, zejména pak oblasti jejich archivace. Závěrečná práce je složena ze dvou částí – teoretické a praktické. Významnou a nezbytnou součástí práce je analýza postavení elektronického dokumentu v českém právním prostředí. Analýza je obsažena v teoretické části práce. Na základě teoretických poznatků byla vytvořena aplikace pro správu elektronických dokumentů, které je věnována praktická část bakalářské práce. Samotná aplikace je úložištěm ve smyslu § 562 odst. 2 občanského zákoníku.

KLÍČOVÁ SLOVA

elektronický dokument, archivace, elektronický podpis, elektronické časové razítko, domněnka spolehlivosti, systém pro správu elektronických dokumentů

ABSTRACT

Bachelor's thesis deals with the problematics of the electronic documents, especially in the area of their archiving. The thesis consists of two parts – theoretical and practical. The analysis of the electronic document position in the Czech legal environment is a significant and essential part of the thesis. The analysis is included in the theoretical part of the thesis. Based on the theoretical knowledge, we created an application for the electronic document management system, which is the subject of the practical part of the bachelor's thesis. The application itself represents a repository in the accordance with § 562 paragraph 2 of the Civil Code.

KEYWORDS

electronic document, archiving, electronic signature, electronic time stamp, presumptiton of reliability, electronic document management system

Vysázeno pomocí balíčku `thesis` verze 4.03; `http://latex.feec.vutbr.cz`

MLČÁKOVÁ, Kristýna. *Návrh systému pro správu elektronických dokumentů*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2021, 56 s. Bakalářská práce. Vedoucí práce: JUDr. Pavel Loutocký, Ba (Hons) Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Kristýna Mlčáková
VUT ID autora:	211323
Typ práce:	Bakalářská práce
Akademický rok:	2020/21
Téma závěrečné práce:	Návrh systému pro správu elektronických dokumentů

Prohlašuji, že svou závěrečnou práci jsem vypracovala samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu bakalářské práce panu JUDr. Pavlu Loutockému, Ba (Hons), Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

S vývojem naší civilizace se stále více rozvíjí i oblast technologií. S postupujícím rozvojem se téměř vše přesouvá do elektronické sféry a dochází k stále většímu využívání elektronických služeb, které nám současné technologie umožňují. Spolu s rozvojem elektronizace se dokonce objevují snahy určité oblasti zcela převést do digitální sféry (např.: bankovnictví).[1]

Na pokročilý vývoj technologií muselo zareagovat i právo, které nebylo připraveno na přenesení určitých právních problémů do elektronické sféry a tehdejší právní úprava nezaručovala dostatečnou oporu právním jednáním vznikajícím elektronickou cestou.

Největším pokrokem v právní oblasti bylo přijetí nařízení eIDAS (nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES). Nařízení přineslo jistou nápovědu, jak se s nově vzniklými problémy vypořádat a zavedlo řadu dosud neužívaných institutů.

Mezi takovými instituty byl i elektronický dokument. Nařízení eIDAS však zavádí pouze definici tohoto pojmu, a tak otázky které nařízení neřeší musely být vyřešeny na „národní úrovni“.

Přijetí nařízení eIDAS mělo velký dopad na český právní řád. Přijetí nařízení vedlo ke zrušení zákona č. 227/2000 Sb., vzniku nového zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce a zákona č. 250/2017 Sb., o elektronické identifikaci. Oba zákony měly za cíl adaprovat právní řád České republiky na určitou část nařízení eIDAS – oblast služeb vytvářejících důvěru a část, která upravuje elektronickou identifikaci. Dále došlo k novelizaci mnoha právních předpisů.[2] [2]

Vzhledem k běžnému používání elektronických dokumentů v moderním světě je žádoucí, aby mohl být takový dokument využit jakožto důkazní prostředek. Elektronický dokument tedy musí být důvěryhodný. K zajištění důvěryhodnosti slouží opět instituty, které zavádí nařízení eIDAS. Tyto prvky lze souhrnně označit jako elektronické zabezpečovací prvky – konkrétně se jedná o elektronický podpis, elektronickou pečeť a elektronické časové razítko. Instituty, které zavádí nařízení eIDAS však nejsou jediné, otázku zajištění důvěryhodnosti řeší také občanský zákoník v § 562 odst. 2, kde nám zavádí domněnku spolehlivosti systému pro správu elektronických dokumentů. Má se za to, že dokumenty uložené v systému, který splní podmínky

[1] K tomu viz s. 213 [1].

[2] Vydáním změnového zákona č. 298/2016 Sb., který upravoval desítky dosavadních zákonů například zákon č. 499/2004 Sb o archivnictví a spisové službě, zákon č. 300/2008 Sb o elektronických úkonech a autorizované konverzi, atd.

stanovené v tomto ustanovení jsou důvěryhodné i bez využití elektronických zabezpečovacích prvků.

Problématická je taktéž oblast archivace elektronických dokumentů. V současné době nenastávají komplikace s ukládáním listinných dokumentů, na archivaci těchto dokumentů jsme totiž již zvyklí a víme, jak s dokumenty nakládat. Jsme schopni takovým dokumentům zajistit dostatečnou ochranu i potřebné důkazy o tom, že se jedná o originál potřebného dokumentu. V případě elektronických dokumentů však může být archivace o něco složitější.

Cílem bakalářské práce je na základě získaných informací popsat možnosti pro správu a nakládání s elektronickými dokumenty a následně navrhnout aplikaci pro správu elektronických dokumentů v rámci praktické části práce. Aplikace bude úložištěm ve smyslu § 562 odst. 2 občanského zákoníku.

1 Teoretická část bakalářské práce

Tato část práce se bude věnovat analýze postavení elektronického dokumentu v českém právním prostředí, zejména jejich archivaci. Zprvu vymezíme základní pojmy týkající se této problematiky. Nejdříve bude vydefinován pojem elektronického dokumentu, dále se zaměříme na jeho specifičnost oproti listinnému dokumentu.[1] Dále budou představeny elektronické zabezpečovací prvky, jelikož právě ony zajišťují autenticitu elektronického dokumentu. Poté se práce zaměří na archivaci elektronických dokumentů. V práci se budeme často odkazovat na relevantní právní předpisy.

1.1 Elektronický dokument

S rozvojem informační společnosti se stále ve větší míře používají elektronické formy dokumentů. Elektronické dokumenty jsou totiž základními nositeli fixovaného stavu určité informace v daném časovém okamžiku. Pro elektronickou formu dokumentu není statická podoba jeho stěžejní vlastností, neboť dokument může mít i dynamický obsah.(s. 213, [1])

Pro přesnější vymezení pojmu elektronický dokument, by bylo vhodné zprvu vymezit samotný pojem dokument. Nejprve je nutné konstatovat, že pojem dokument se v české právní praxi používá zřídka. Primárně je se tento pojem používá jako jednotka spisové služby.[2] Z tohoto důvodu lze přímou definici pojmu „dokument“ nalézt v zákoně č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (dále ArSSZ). Dokumentem se v režimu ustanovení § 2, písm. e) zmiňovaného zákona rozumí *„každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena“* [3].

Dokument jako takový má šest významných atributů:[3]

- **informační hodnota** - dokument je nositelem informace, která má určitou hodnotu
- **stálost** - dokument je neměnný, stálý
- **jazyk** - dokument je vyjádřen v určitém jazyce[4]

[1] V rámci této práce bude pod pojmem „listinný dokument“ chápán protějšek elektronického dokumentu, ačkoliv v kapitole 1.1.1 bude poukázáno, že i listinný dokument může mít elektronickou podobu.

[2] K tomu viz: s. 214 [1].

[3] Podle R. Polčáka lze za významné atributy dokumentu považovat i pouze první dva z uvedeného výčtu. Viz s. 186 a násl. [6].

[4] Nejedná se o nezbytný atribut. Dokument může být vyjádřen také např.: v symbolice

- **strukturovanost** - vnitřní struktura dokumentu je závislá na mnoha aspektech[5]
- **ucelenost** - s dokumentem je nakládáno jako s celkem
- **funkční zabarvení** (s. 37-38, [4])

Jak si lze povšimnout z výše uvedené definice pojmu dokument, jeho klíčovým prvkem je informace.[6] Podle způsobu, jakým je informace uložena jde buď o listinný, či o elektronický dokument. [7]

S pojmem elektronický dokument se setkáváme v 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 (dále nařízení eIDAS). Podle článku 3 nařízení eIDAS je elektronickým dokumentem *„jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka.“* [5]

Elektronický dokument má čistě elektronickou podobu a v mnoha ohledech určité specifické vlastnosti, kterými se odlišuje od analogových podob dokumentů.[8] Mezi základní oblasti, ve kterých jsou elektronické dokumenty specifické řadíme např.: jejich tvorbu, přístup k originálu, přístup k ochraně apod. Ovšem i přes specifičnost elektronického dokumentu mu nesmí být slovy článku 46 nařízení eIDAS *„upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu.“* [9] Elektronický a analogový dokument jsou tak dvě právně rovnocenné alternativy dokumentu. [10] (s. 40-44, [4])

V odborných článcích a publikacích se lze též setkat s pojmem „digitální dokument“. Digitální dokument je vnímán jako protějšek analogového dokumentu. V českém prostředí je tento pojem brán jako synonymum „elektronického dokumentu“ a proto bude s pojmy v této práci také tak nakládáno.[11]

V právní praxi však pojem dokumentu není příliš používaným pojmem, vyskytují se spíše pojmy jako „listina“ či „písemnost“.[12] V současné době ve vztahu k elek-

[5]Např.: na povaze dokumentu, na okolnostech vzniku apod.

[6]Definici informace je možné najít např. v § 3 odst. 3 zákona č. 106/1999 Sb. o svobodném přístupu k informacím: *„Informací se pro účely tohoto zákona rozumí jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního.“* [7]

[7]Ačkoliv listinný dokument může mít i elektronickou podobu, jak bude rozebráno v rámci kapitoly 1.1.1, v rámci této práce budeme pod pojmem listinný dokument uvažovat protějšek elektronického dokumentu – tedy dokument v „papírové podobě“.

[8]Ke srovnání vlastností elektronického dokumentu a listinného dokumentu (bude diskutováno dále) viz tabulka: [4], s. 43.

[9]Viz čl 46 [5].

[10]K tomu viz s. 88, [4]

[11]Pojem elektronického dokumentu se používá zejména ve vztahu k české legislativě [9].

[12]K problematice listina vs. písemnost viz [1], s. 216–217.

tronickým dokumentům nemůže ani jedna z těchto forem být spojována s čistě listinnou formou. Písemný dokument může mít jak listinnou, tak elektronickou formu. V českém právním řádu není písemnost ani listina, na rozdíl od dokumentu, nijak definována a tím pádem nejsou kladeny specifické požadavky na jejich vlastnosti. Vymezení pojmů písemnost a listina je tedy právním obyčejem. (s. 216, [1], s. 286 a násl. [6])

Typickou vlastností písemnosti je, že je zaznamenána písmem – na hmotném nosiči, nebo v elektronické podobě. Nejdůležitější písemností , z pohledu práva, je taková písemnost, která zaznamenává projev lidské vůle. Je důležité si uvědomit, že písemná podoba právního jednání nemusí znamenat vazbu na listinnou podobu. V tomto smyslu se vyjádřil i Nejvyšší soud České republiky v první právní větě svého stanoviska Plsn 1/2015: *„V občanském soudním řízení lze učinit podání mimo jiné i písemně, tj. v listinné podobě, v elektronické podobě prostřednictvím veřejné datové sítě nebo telefaxem (§ 42 odst. 1 o. s. ř.).“* [8] Podobně se vyslovuje i občanský soudní řád v § 42 odst. 1 a občanský zákoník v §3026.[13] (s. 216, [1])

Pod pojmem listina lze rozumět časově stabilní fixaci písemnosti.[14] Opět pro listinu platí, že nemusí být pouze v listinné podobě.[15] Z právního hlediska lze rozlišit dvě varianty listiny – veřejnou a soukromou.[16]

Kromě pojmů „listina“ a „písemnost“ se lze setkat i s jinými výrazy, například ve výše uvedeném ustanovení § 2, písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů se hovoří o dokumentu v analogové a v digitální podobě (s. 28, [10]).

1.1.1 Srovnání elektronického a listinného dokumentu

Pro lepší pochopení základních problémů v oblasti využívání elektronických dokumentů je vhodné si uvědomit podobnosti ale zároveň i zásadní rozdíly mezi elektronickými a listinnými dokumenty.

Oba typy dokumentů mají informační hodnotu, kterou je třeba chránit, oba totiž

[13] Srov. § 42 odst. 1 o. s. ř. *„Podání je možno učinit písemně. Písemné podání se činí v listinné nebo elektronické podobě prostřednictvím veřejné datové sítě nebo telefaxem.“* Srov. § 3026 NOZ *„Nevylučuje-li to povaha písemnosti, platí ustanovení tohoto zákona o listině obdobně i pro jinou písemnost bez zřetele na její podobu.“*

[14] K tomu viz [1], s. 216.

[15] V rámci této práce však budeme dále používat pojem listinný dokument ve významu protějšku k elektronickému dokumentu, tedy jako dokument v „papírové podobě“.

[16] Veřejná listina má v současné době svou zákonnou definici v § 567 NOZ, ale vztahuje se k ní mnoho ustanovení i jiných zákonů např.: § 131 odst. 1 zákona č. 40/2009 Sb. K vlastnostem soukromé listiny viz § 565–566 NOZ.

nesou určité sdělení, tedy informaci. [17] Informace by měla být srozumitelná a čitelná – zajištění těchto dvou aspektů řadíme k základním rizikům archivace.

Srovnáním obou typů dokumentů dojdeme k závěru, že jak elektronický dokument, tak i analogový mají své výhody. U analogového dokumentu můžeme hovořit o snadné rozpoznatelnosti (jedinečnosti) originálu a fyzické hmatatelnosti. Elektronický dokument je výhodný ve své snadné dostupnosti, manipulaci, nezávislosti na nosiči a relativní stálosti kvality.

Základní rozdíly mezi listinnými a elektronickými dokumenty vycházejí z jejich fyzické podstaty (s. 11, [9]). Zásadní rozdíl je například v rozpoznávání originálu u daného dokumentu. Zatímco u listinného dokumentu je pořízení kopie poměrně složité a vzniklá kopie mívá zpravidla nižší kvalitu než originální dokument, je velmi snadné určit originál. U elektronických dokumentů je situace o něco složitější. Při vytváření kopie původního dokumentu se kvalita nesnižuje a tudíž vedle původního dokumentu nevzniká nová kopie, nýbrž další originál – fakticky totiž není rozdíl mezi originálem a kopií.(s. 28, [12])

S problematikou rozpoznávání originálu dokumentu souvisí i otázka pravosti dokumentů. Opět se jedná o poměrně jednoduchý proces v případě listinných dokumentů, neboť pokud nastane změna původní informace, jedná se o pozměnění či poškození nosiče. Pro elektronické dokumenty musely být v tomto ohledu vyvinuty speciální techniky zajišťující integritu a autentičnost informací obsažených v dokumentů. Tyto techniky zároveň přináší možnost ověření pravosti elektronického dokumentu. Typicky se jedná především o elektronický podpis, který bude rozebrán v kapitole 1.2.1.

Další oblastí, ve které lze pozorovat odlišnosti mezi listinnými a elektronickými dokumenty jsou důsledky v případě poškození nosiče. Jako příklad lze uvést USB flash disk, na který je možno uložit velké množství knih (v závislosti na velikosti paměti). Proto pokud dojde k poškození USB disku přijdeme tak o veškerá data na tomto nosiči uložená (v našem případě knihy), zatímco při poškození knihy v papírové podobě přijdeme pouze o jednu knihu. Elektronické dokumenty jsou tedy náchylnější na poškození či zničení nosiče než listinné dokumenty. Zároveň však je třeba upozornit, že při kopírování USB disku je proces kopírování výrazně snazší a rychlejší než fyzická výroba většího množství knih (s. 11, [9]).

Vzhledem k zaměření této práce zde ještě upozorním na odlišnosti v oblasti archivace elektronických a analogových dokumentů. Při archivaci analogových dokumentů se snažíme o uchování fyzikálních a chemických vlastností dokumentu – navíc archivace listinných dokumentů je oborem s dlouholetou tradicí (v řadech tisíců

[17] Zde je třeba si uvědomit rozdíl mezi informacemi a daty. Tyto pojmy bývají i v zákoně zaměňovány a jsou poněkud nepřesné. K problematice viz [11]. My nadále budeme pracovat spíše s pojmem informace.

let) a oproti archivaci digitálních dokumentů je ustálená. Při archivaci elektronických dokumentů jde zejména o zachování čitelnosti dat a skladovatelnosti virtuálních vlastností dokumentů (tab. s. 14, [13]). Ve srovnání s archivací listinných dokumentů je archivace elektronických dokumentů poměrně novým a dynamičtějším oborem.

Odlišnosti mezi elektronickými a listinnými dokumenty lze hledat zejména v oblasti rozpoznávání originálu, otázce pravosti dokument, možných ochranných prvcích, přístupu k ochraně atd. [18]

1.2 Nástroje zajišťující autenticitu elektronických dokumentů

V případech, kdy jsou elektronické dokumenty nositeli informace s důkazní hodnotou je třeba zajistit důkazním spolehlivost takovýchto dokumentů tzn. je nutné zajistit jejich autenticitu. *„Autentizační informace představuje nutnou formální náležitost právně relevantní písemnosti.“* (s. 186 a násl. [6])

K zajištění autenticity dokumentů slouží tzv. elektronické zabezpečovací prvky. Mezi tyto prvky řadíme elektronický podpis, elektronickou pečeť a elektronické časové razítko. Jde o nástroje analogické s prostředky kterými je zajištěna autenticita listinných dokumentů.[19] Připojením těchto atributů jsme schopni, za určitých podmínek, ověřit pravost dokumentu i po určité době.

Způsoby zajištění věrohodnosti elektronických dokumentů (tedy elektronické zabezpečovací prvky) upravuje nařízení eIDAS.[20] V prostředí českého právního řadu toto nařízení doplňuje zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále ZoSVD). ZoSVD mimo jiné zcela zrušil zákon č. 227/2000 Sb., o elektronickém podpisu.[21]ZoSVD doplňuje nařízení eIDAS o národní pravidla opatřování dokumentů elektronickými zabezpečovacími prostředky. Kromě ZoSVD nabyl účinnosti též změnový zákon 298/2016 Sb. – tímto změnovým zákonem se novelizovala řada dosavadních zákonů (zejména v oblasti elektronické identifikace).[22]

Momentálně se v České republice vyskytují tři certifikační autority. Tyto certifikační autority mají oprávnění vydávat elektronické zabezpečovací prvky. Přehled certifikačních autorit je uveden v tabulce 1.1.[23]

[18]Tuto problematiku shrnuje T. Lechner v tabulce na s. 43, [4]. Srov. [13], s. 14.

[19]V případě listinných dokumentů se setkáváme s vlastnoručním podpisem, razítkem a pečetí.

[20]Pro srovnání právní úpravy dle nařízení eIDAS a dřívější právní úpravy v české legislativě viz tab. s. 199–213 [22].

[21]Viz zrušovací ustanovení uvedená v § 20 odst. 1 [15].

[22]Počet takto novelizovaných předpisů je poměrně vysoký – k tomu viz [16].

[23]Informace v obrázku jsou dostupné z: [19].

Poskytovatelé certifikačních služeb	Kvalifikované služby	Zahájení vydávání
První certifikační autorita, a. s.	Vydávání kvalifikovaných certifikátů;	03/2002
	Vydávání kvalifikovaných systémových certifikátů;	02/2006
	Vydávání kvalifikovaných časových razítek.	02/2006
	Vydávání prostředků pro bezpečné vytváření el. podpisů.	01/2016
Česká pošta, s. p.	Vydávání kvalifikovaných certifikátů;	09/2005
	Vydávání kvalifikovaných systémových certifikátů;	04/2005
	Vydávání kvalifikovaných časových razítek.	07/2009
	Vydávání prostředků pro bezpečné vytváření el. podpisů.	06/2016
eIdentity, a. s.	Vydávání kvalifikovaných certifikátů;	08/2005
	Vydávání kvalifikovaných systémových certifikátů;	08/2005
	Vydávání kvalifikovaných časových razítek.	08/2010

Tab. 1.1: Přehled certifikačních autorit v České republice

1.2.1 Elektronický podpis

Chceme-li, aby *„elektronický dokument mohl obsahovat zaznamenání projevu vůle, musí existovat možnost, jak jej elektronicky podepsat.“* (s. 218, [1]) Tato skutečnost je však pouze obyčejovým právním pravidlem. Jak již bylo zmíněno výše, elektronický podpis je alternativou vlastnoručního podpisu pro elektronické dokumenty (s. 216, [1], s. 286 a násl. [6]).

Vlastnoruční podpis je typickým příkladem právního obyčeje v České republice. Ačkoliv je totiž velice často používaným instrumentem, není upraven v žádném psaném pramenu práva České republiky. Nejsou tedy stanoveny formální požadavky ani definice vlastnoručního podpisu. [24]

V tomto směru se elektronický podpis od svého listinného protějšku výrazně odlišuje, jelikož elektronický podpis je přesně popsán v nařízení eIDAS.[25]. Nařízení rozlišuje tři druhy (resp. stupně) elektronického podpisu: elektronický podpis, zaručený elektronický podpis a kvalifikovaný elektronický podpis. Tyto tři stupně elektronického podpisu jsou explicitně zmíněny v nařízení eIDAS, ale např. zákon č.297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce zmiňuje navíc uznávaný podpis a pod tímto pojmem zákon rozumí *„zaručený podpis založený na kvalifikovaném certifikátu pro elektronické podpisy a kvalifikovaný elektronický podpis.“*[26]

Prvním stupněm a zároveň nejnižší úrovní je elektronický podpis bez přívlastku

[24] K tomu viz s. 186 a násl. [6].

[25] Definice jednotlivých úrovní elektronického podpisu je uvedena v čl. 3 odst. 10-12 a dále je elektronickému podpisu věnován oddíl 4.

[26] Viz § 6 odst. 2 zákona č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce.[15]

(někdy též jednoduchý elektronický podpis). Jeho definici vymezuje ustanovení čl. 3 odst. 10) nařízení eIDAS: *„data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání.“* Tento stupeň ovšem není dostatečně důvěryhodný a nemůže tedy být postaven na roveň vlastnoručnímu podpisu. Někteří autoři se dokonce domnívají, že bychom tento stupeň vůbec neměli považovat za elektronický podpis.[27] Zákon tak však činí a nevylučuje tento druh elektronického podpisu ani jako důkaz projevu vůle podepisující osoby při určitých typech právního jednání – zejména pro soukromoprávní oblast.[28] (s. 233, [1], § 7 [15], s. 30, [10])

Další úrovní elektronického podpisu je zaručený elektronický podpis, v případě tohoto stupně je zapotřebí technické zabezpečení důvěryhodnosti. V článku 26 nařízení eIDAS jsou stanoveny čtyři požadavky, které podpis musí splňovat:

a) je jednoznačně spojen s podepisující osobou
b) umožňuje identifikaci této osoby
c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou
d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.[29] (čl. 26, [5])

Z citovaného ustanovení písm. c) vyplývá, že elektronický podpis nesmí vznikat automatizovaně, pokud podepisující osoba přímo nevyjádří svobodnou vůli podpis vytvořit.

Třetí úrovní je zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronické podpisy. Na rozdíl od předchozí úrovně již zaručuje důvěryhodnost i v údajích uvedených v certifikátu přiloženém k podpisu. Jak již bylo zmíněno výše, nařízení eIDAS s touto úrovní nepracuje, avšak je třeba ji samostatně uvažovat, jelikož české předpisy s ní pracují. Účinky vlastnoručního podpisu třetí úrovni přiznává zákon č. 297/2016 Sb. pro případy, kdy se kvalifikovaným podpisem podepisují elektronické dokumenty kterými se právně jedná vůči orgánům veřejné moci (s. 235, [1], § 6 [15]).

Nejvyšší míru důvěrnosti zaručuje kvalifikovaný elektronický podpis: *„zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy“*.[30] Kvalifikované prostředky zajišťují značnou míru důvěrnosti dat, proto musí splňovat požadavky na kvalifikované prostředky pro vytváření elektronických podpisů, které jsou stanoveny v příloze II nařízení eIDAS, a technické normy. Tech-

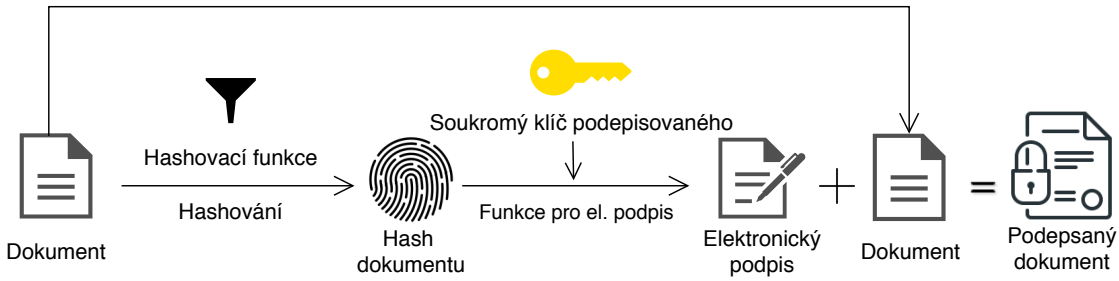
[27] Viz [10], s. 30.
[28] Viz § 7 zákona č. 297/2016 Sb.
[29] K technické stránce řešení elektronického podpisu: [10]
[30] Viz článek 3 odst. 12 [5].

nické upřesnění je pak obsaženo v prováděcím rozhodnutí Komise (EU) 2016/650 [17]. Jedná se o jedinou úroveň elektronického podpisu které samotné nařízení eIDAS přiznává účinky vlastnoručního podpisu, ačkoli připouští, že i jiné úrovně mohou mít právní účinky (s. 236, [1]).

ZoSVD stanovuje, které subjekty musí využít kvalifikovaný podpis v případě, že právně jednají. Jedná se o stát a územní samosprávné celky, právnickou osobu zřízenou zákonem nebo právnickou osobu zřízenou nebo založenou státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem.[31] Dále pak mezi takové subjekty řadíme i jinou (tj. fyzickou) osobu, která právně jedná při výkonu své působnosti.[32]

Princip kvalifikovaného elektronického podpisu

Vytváření elektronického podpisu probíhá ve dvou krocích. Nejprve se vytvoří hash (otisk) dokumentu. K vytvoření otisku se využije hashovací funkce, v dnešní době se doporučuje používat minimálně funkci SHA-2 (s. 70, [10]). [33] Získaný hash se pomocí soukromého klíče podepisující osoby zašifruje a tím vznikne elektronický podpis který se přidá k původnímu dokumentu. Proces podepisování elektronického dokumentu je znázorněn na obrázku 1.1:[34]



Obr. 1.1: Podepisování elektronického dokumentu

Ověřování elektronického podpisu probíhá taktéž ve dvou krocích, které probíhají paralelně. Z původního (originálního) dokumentu se vytvoří hash, k jehož vytvoření se použije stejná hashovací funkce jako při vytváření elektronického podpisu. Současně se dešifruje elektronický podpis za použití veřejného klíče podepisované osoby. Tímto způsobem získáme původní hash dokumentu. [35] V závěrečné fázi procesu se

[31] Právnickou osobou se slovy zákona rozumí *„organizovaný útvar, o kterém zákon stanoví, že má právní osobnost, nebo jehož právní osobnost zákon uzná.“* Viz § 20 odst. 1 věta první [20].

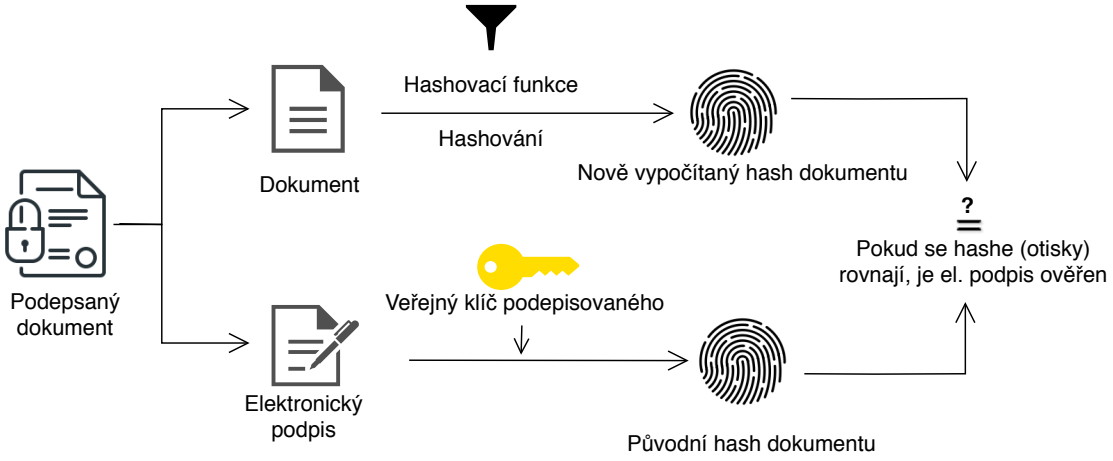
[32] Viz § 6 odst. 1 [15].

[33] K hashovacím funkcím viz [21].

[34] Obrázek inspirován [14].

[35] Použití veřejného a soukromého klíče napovídá, že se bude jednat o asymetrický algoritmus, konkrétně se jedná o RSA a DSA.

oba hashe porovnají. Pokud hashe odpovídají (tj. jsou stejné), je elektronický podpis úspěšně ověřen. V opačném případě je podpis neplatný. Ověření elektronického dokumentu je znázorněno na obrázku 1.2.[36]



Obr. 1.2: Ověření elektronického podpisu

1.2.2 Elektronická pečeť

Dalším elektronickým zabezpečovacím prvkem je elektronická pečeť. Pod pojmem elektronické pečeti rozumíme dle ustanovení čl. 3 odst. 25 nařízení eIDAS *„data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu“*. (čl. 5 odst 25 [5]) Na rozdíl od elektronického podpisu se tedy tímto zabezpečovacím prvkem neprokazuje vůle pečetící osoby a proto elektronická pečeť je typicky vytvářena automatizovaným procesem. U elektronické pečeti rozlišujeme opět čtyři úrovně pojmově shodné s úrovněmi u elektronického podpisu – základní úroveň (odpovídá uvedené definici), zaručená elektronická pečeť, zaručená elektronická pečeť založena na kvalifikovaném certifikátu pro elektronické pečetě a kvalifikovaná elektronická pečeť.

Stejně jako pro zaručený elektronický podpis jsou i pro zaručenou elektronickou pečeť stanoveny konkrétní požadavky, které musí splňovat. Tyto požadavky jsou obsaženy ve článku 36 nařízení eIDAS a jejich přesné znění je:

a) je jednoznačně spojena s pečetící osobou
b) umožňuje identifikaci této osoby
c) je vytvořena pomocí dat pro vytváření elektronických pečetí, která může pečetící osoba s vysokou úrovní důvěry použít pod svou výhradní kontrolou
d) je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat. (čl. 36 [5])

[36] Obrázek inspirován [14].

Z citovaného ustanovení vidíme, že se velmi podobá požadavkům, které jsou stanoveny pro zaručený elektronický podpis. První dva požadavky jsou dokonce téměř totožné, je zde však zásadní rozdíl. Zatímco podepisující osobou může být jen a pouze fyzická osoba, pečetící osobou může být zase pouze právnická osoba.

Největší rozdíl oproti elektronickému podpisu je dán ve třetím požadavku, jelikož elektronická pečeť neslouží k vyjádření vůle osoby, může být na rozdíl od elektronického podpisu vytvářena automatizovaným procesem, který ovšem musí být zabezpečen na procesní úrovni. (s. 238, [1])

Čtvrtý požadavek je opět shodný s požadavkem pro zaručený elektronický podpis a tudíž tato shodnost se projeví v uplatnění obdobných technologií jak v případě podepisování, tak pečetění.

„Kvalifikovaná elektronická pečeť jako nejvyšší úroveň elektronické pečetě je spojena s presumpcí integrity dat a správnosti původu těchto dat.“ (s. 239, [1]) Dle článku 3 odst. 27 nařízení eIDAS rozumíme pod pojmem kvalifikované elektronické pečetě: *„zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.“* (čl. 3 odst 27 [5])

Elektronickou pečetí může právnická osoba označit pouze dokument, jehož je sama původcem, tím se elektronická pečeť liší od elektronické značky. [37] Při srovnání elektronické pečeti a elektronického podpisu lze konstatovat hlavní rozdíl mezi těmito prvky, a to že podepisovat mohou pouze fyzické osoby a pečetit mohou pouze právnické osoby. Je třeba mít na paměti, že elektronická pečeť tedy není elektronickým podpisem ve smyslu podpisu – nevyjadřuje, že by se pečetící osoba před připojením pečetě s pečetěným textem seznámila. (s. 48–49, [23]).

1.2.3 Elektronické časové razítko

Trojici základních zabezpečovacích prvků uzavírá elektronické časové razítko, které prokazuje, že konkrétní dokument existoval v určitém okamžiku.[38] Stejně tak může časové razítko prokazovat existenci podpisu či pečetě v určitém čase, a to pokud je spojen právě s elektronickým podpisem či pečetí. Tento aspekt časového razítka má velký význam zejména při procesu ověřování platnosti zabezpečovacích prvků. Ve srovnání s předchozími zabezpečovacími prvky má časové razítko pouze dvě úrovně – základní a kvalifikované elektronické časové razítko.

[37] Ke srovnání elektronické pečeti a elektronické značky viz s. 45–50, [23].

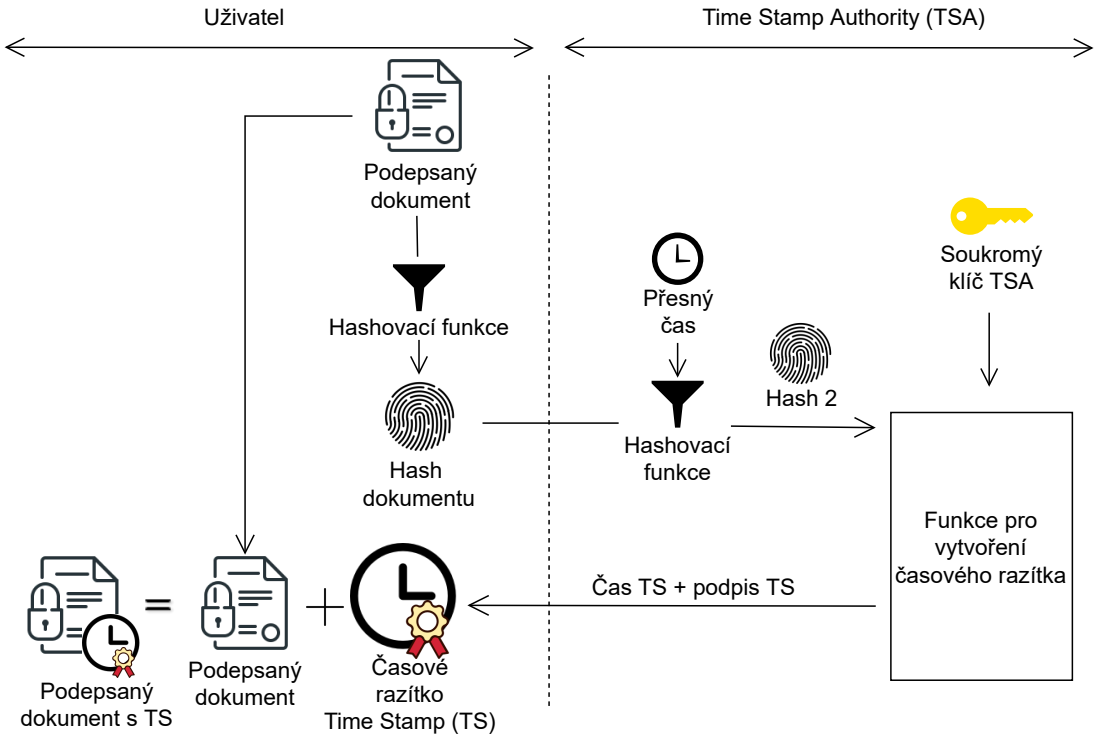
[38] Jak je patrné z definice časového razítka obsažené v čl. 3 odst. 33 [5] – pod pojmem elektronické časové razítko rozumíme: *„data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku;“*

V případě kvalifikovaného časového razítka je potřeba, stejně jak tomu bylo v případě podpisu a pečeti, splnit požadavky přesně definované v čl. 42 nařízení eIDAS, konkrétně:

a) spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat
b) je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem
c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou. (s. 239–240, [1], čl. 42 [5])

Princip kvalifikovaného elektronického časového razítka

Tvorba elektronického časového razítka probíhá na dvou stranách – na straně uživatele a straně TSA (Time Stamp Authority).[39] TSA garantuje svým podpisem čas vytvoření časového razítka. Proces vytvoření elektronického časového razítka je znázorněn na obrázku 1.3:[40]



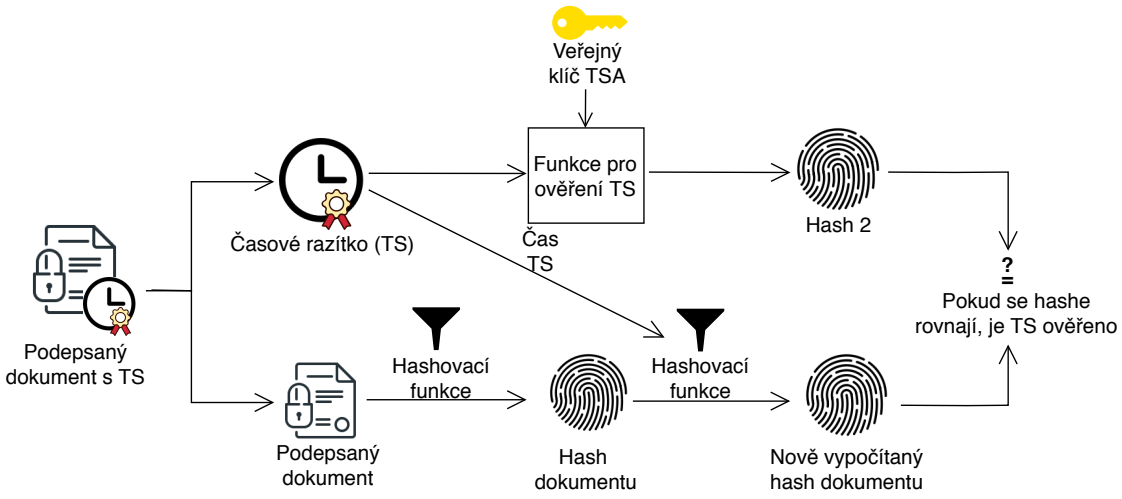
Obr. 1.3: Vytvoření časového razítka

[39] Vydávání časových razítek je jednou ze služeb certifikačních autorit (akreditavaných poskytovatelů certifikačních služeb) – viz tabulka 1.1.

[40] Obrázek inspirován [18].

Nejdříve uživatel podepíše dokument, pomocí vlastního páru klíčů, elektronickým podpisem, poté je pomocí hashovací funkce vytvořen hash dokumentu. Otisk dokumentu je poslán TSA. TSA k otisku přidá přesný čas a poté je otisk spolu s přesným časovým údajem zahashován. K nově vzniklému hashi se opět přidá přesný čas a poté je podepsán soukromým klíčem, tím vzniká certifikát s atributy časového razítka. Následně TSA posílá časové razítko zpět žadateli, který jej přiloží k dokumentu.[18]

Proces ověření časového razítka probíhá totožně jako proces ověřování elektronického podpisu, který je popsán v kapitole 1.2.1, proto nebude podrobněji rozebírán. Ověřování časového razítka není třeba provádět na straně TSA – je pouze potřeba mít k dispozici certifikát, kterým je časové razítko podepsáno. Ověření časového razítka je znázorněno na obrázku 1.4:[41] Pro pořizování časových razítek musí uživatel použít speciální aplikaci k tomuto účelu určenou – tu lze získat od TSA.



Obr. 1.4: Ověření časového razítka

Stejně jako předešlé elektronické zabezpečovací prvky i elektronické časové razítko má omezenou platnost.[42] Pokud je třeba zajistit důvěryhodnost elektronického dokumentu po delší časový interval, než po jaký je časové razítko platné, je nutné časové razítko tzv. přerazítkovat novým časovým razítkem. Žádný z elektronických zabezpečovacích prvků není imunní vůči tzv. kolizním dokumentům. Může se jednat o dva dokumenty, které jsou odlišné ale mají stejný hash (s. 71, [10]).[43]

[41] Informace v obrázku jsou dostupné z: [19].

[42] Platnost elektronických zabezpečovacích prvků se odvozuje od platnosti certifikátu na kterých jsou tyto prvky založeny – pro potřeby archivace jsou přípustné pouze kvalifikované certifikáty vydané kvalifikovaným a akreditovaným poskytovatelem certifikačních služeb.

[43] K problematice kolizních dokumentů více s. 71-73 [10]

1.3 Archivace elektronických dokumentů

Jak jsme již zmínili v předchozích kapitolách elektronický dokument je typický svou specifičností oproti listinnému dokumentu. Proto se také uplatňuje rozdílný přístup při nakládání s listinnými dokumenty a při nakládání s elektronickými dokumenty.[44] Kvůli odlišnostmi mezi elektronickými a listinnými dokumenty, tak existuje v oblasti týkající se elektronických dokumentů řada specifik. Specifika v oblasti archivace budou diskutována dále.

1.3.1 Specifika uchovávání elektronických dokumentů

Při archivaci elektronického dokumentu se snažíme o zachování informace obsažené v tomto dokumentu, bez ohledu na její fyzické umístění. Proto abychom mohli s elektronickými dokumenty dále nakládat, musí být jejich uchovávání spojeno i se zajištěním věrohodnosti původu dokumentu, čitelnosti dokumentu a také musí být zamezeno možnosti změnit obsah uchovávaného dokumentu.[45] K ochraně elektronických dokumentů konkrétně před paděláním se vyjadřuje T. Lechner, který provádí srovnání přístupu k ochraně elektronických dokumentů s ochranou bankovek.[46] T. Lechner v tomto srovnání naráží zejména na skutečnost, že tak jako nepřestáváme používat bankovky, ačkoliv jsou známy případy jejich padělání (tedy ochrana bankovek není stoprocentní), není možné bránit používání elektronických dokumentů pouze protože není zajištěna jejich dokonalá ochrana (s. 103, [4]).

Archivace elektronických dokumentů je tedy spojena s řadou rizik. Mezi ty nejvýznamnější řadíme: (s. 264, [1])

- rizika spojená s datovými formáty
- rizika spojená s technickým nosičem
- rizika spojená s omezenou platností elektronických zabezpečovacích prvků

Obecně výrazným problémem je problém zastarávání, ať už se to týká datových formátů, technických nosičů nebo elektronických zabezpečovacích prvků.

Kromě zastarávání formátů řadíme mezi rizika spojená s datovými formáty také otázky proprietárnosti a otevřenosti dokumentace datového formátu, podpora formátu a jeho robustnost. Užívání proprietárních formátů, může být poněkud problematické a to hlavně z důvodu ochrany těchto formátů – jsou totiž chráněny právy

[44] Zejména se jedná o rozdílný přístup v oblasti ukládání, ochraně a archivaci (uchovávání) [1].

[45] Viz § 3 odst. 5 ArSSZ: *„V případě dokumentů v digitální podobě se jejich uchováváním rozumí rovněž zajištění věrohodnosti původu dokumentů, neporušitelnosti jejich obsahu a čitelnosti, tvorba a správa metadat náležejících k těmto dokumentům v souladu s tímto zákonem a připojení údajů prokazujících existenci dokumentu v čase. Tyto vlastnosti musí být zachovány do doby provedení výběru archiválií.“* [3]

[46] K tomu viz s.103 [4].

duševního vlastnictví, a proto je jejich používání omezeno. Avšak některé proprietární formáty jsou doporučovány právními předpisy pro ukládání elektronických dokumentů. Jedná se především o formáty s otevřenou dokumentací, která je podložena konkrétními ISO standardy (s. 264, [1]).

Pravděpodobně nejčastěji využívaným je datový formát PDF/A (Portable Document Format/Archieve) je určen pro statické textové dokumenty a statické kombinované (textové a obrazové) dokumenty. Jak již s názvu formátu vyplývá, norma byla určena právě pro dlouhodobou archivaci elektronických dokumentů. Nejenom že tato norma odpovídá potřebám dlouhodobé archivace dokumentů, navíc odpovídá i potřebám na zachování nezávislosti, a to nezávislosti na hardwaru, na operačním systému a na konkrétní aplikaci. (s. 49–51 a 108–109, [4]) V současné době existuje verze PDF/A-4, která je standardizována normou 19005-4.[24] Jaké formáty použít pro konkrétní typy dokumentů nám stanovuje § 23 vyhlášky č. 259/2012 Sb. [25]. Další formáty jsou shrnuty v tabulce 1.2.[47] [25]

Textové dokumenty statické a kombinované	**Obrazové dokumenty**		**Zvukové dokumenty**	**Databáze**	**Účetní záznamy**	**Metadata**
	statické	**dynamické**				
PDF/A	PNG TIF/TIFF JPEG/JFIF	MPEG-2 MPEG-1 GIF	MP2 MP3 WAV	XML a popis jeho struktury nebo DTD	ISDOC	XML

Tab. 1.2: Použití datových formátů pro konkrétní typy dokumentů

„Rizika spojená s technickým nosičem se snižují s různými způsoby archivace a duplicitních uložení.“ (s. 265, [1]) Elektronické dokumenty mohou být uloženy na různých typech datových nosičů (tzn. technických nosičích dat). V případě elektronických dokumentů je důležité si uvědomit, že obsažená informace je důležitější než nosič samotný. *„Problematika datových nosičů spadá do technologické roviny adaptace elektronických dokumentů, přičemž mezi největší problémy, patří degradace digitálních nosičů a zastarávání technologií.“* (s. 56 [4]) Srovnání různých typů datových nosičů provádí L. Cubr, který srovnává i aspekty vhodnosti jejich použití. [48] Je nutné volit datový nosič s přihlédnutím k účelu elektronických dokumentů na něm uložených. Obecně při rozhodování, jaký datový nosič použít se budeme řídit zejména dobou uložení, četností přístupu a počtem uchovávaných dokumentů, přičemž klíčovým faktorem je právě doba, po kterou chceme dokumenty archivovat. (s. 264–265, [1],s. 101–109, [4])

Rizika spojená se ztrátou ověřitelnosti elektronických zabezpečovacích prvků jsou způsobena omezenou dobou platnosti elektronických zabezpečovacích prostředků –

[47] Doplnění k informacím v tabulce – u položek MPEG-2 a MPEG-1 je datovým formátem formát, který podporuje uložení komprimovaných dat podle těchto standardů. V případě databáze je pak nutno k XML formátu přidat i popis jeho struktury pomocí schématu XML nebo DTD.

[48] Viz s. 48 [12]

typicky se jedná o jeden rok. Pouze pokud se jedná o certifikáty připojené k elektronickým časovým razítkům je doba jejich platnosti delší. Zásadním problémem v této oblasti je, že žádné čistě technické řešení nedokáže plně zabezpečit elektronické dokumenty, proto je třeba využít řešení kombinované – to v sobě propojuje technické a procesní opatření (s. 265, [1]).[49]

U problematiky dlouhodobého ukládání elektronických dokumentů se setkáváme s pojmem „důvěryhodný repozitář“. Důvěryhodný repozitář je určen pro dlouhodobé zajišťování důvěryhodnosti, použitelnosti a dostupnosti uložených a uchovávaných dat. Zmíněné principy využívá národní digitální archiv, jenž je vystaven na standardním modelu OAIS. Jedná se o referenční model pro otevřený archivační informační systém, který stojí na ISO standardu ISO 14721.[50] (s. 268, [1])

V současné době je k dispozici ohromné množství technických řešení datových úložišť. Konkrétní řešení je závislé na velikosti a z velké části také na ekonomické situaci konkrétní organizace. Proto je třeba před samotnou realizací provést dobrou analýzu procesu nakládání s digitálními dokumenty. Zejména je nutné věnovat pozornost rizikům a zajistit dostatečnou fyzickou a kybernetickou bezpečnost. Stejně tak je dobré pravidelně provádět bezpečnostní audit – ten totiž může odhalit nové hrozby či nefunkčnost krizových scénářů. Fyzická bezpečnost musí řešit především otázky zálohování dat, technických závad buď na datovém nosiči nebo úložišti. Předejít těmto rizikům je možné využitím cloudového úložiště (s. 37, [13])

1.3.2 Metoda přerazítkování

V současné době je upřednostňovaným technickým řešením archivace elektronických dokumentů připojení kvalifikovaného elektronického časového razítka. [51] Časové razítko prokazuje existenci elektronického dokumentu i elektronických zabezpečovacích prostředků v určitém čase (uvedeném na razítku) a následnou neměnnost tohoto stavu.

Čistě technický přístup k řešení této problematiky spočívá v tzv. „přerazítkovávání“. Tímto způsobem se vytváří „řetězec důvěry“. Časové razítko má omezenou platnost, potřebujeme-li zajistit důvěryhodnost dokumentu po delší časový úsek, než po jaký je časové razítko platné, je nutné před vypršením tohoto razítka provést přerazítkování novým razítkem. Připojování je pravidelné a opakované. Postupně se řetězec rozvijí do podoby, kdy poslední časové razítko prokazuje platnost předchozího a to zase prokazuje platnost předchozího stavu – ani toto řešení není však zcela

[49] Viz čl. 19 odst. 1 nařízení eIDAS.

[50] K tomu viz [26].

[51] Ve spojení s archivací používáme pouze nejvyšší úroveň časového razítka – kvalifikované časové razítko.

spolehlivé.[52]

Navíc toto řešení není úplně nejelegantnější. Vezměme si ukázkový příklad, kdy potřebujeme zajistit věrohodnost dokumentu po dobu dvaceti let. Nejprve bude třeba, aby vlastník dokumentu dokument podepsal elektronickým podpisem a podpis opatřil časovým razítkem. V průběhu archivace onoho dokumentu se pak bude muset hlídat, do kdy je časové razítko platné a před vypršením jeho platnosti bude nutné provést přerazítkování novým razítkem. Pokud počítáme se situací, kdy je časové razítko platné po dobu pěti let, bude po dvaceti letech dokument obsahovat již čtyři časová razítka. Navíc pro potřeby archivace je často nutné ukládat dokumenty na dobu delší než je v ukázkovém příkladu.

Tento přístup je reakcí na dřívější ustanovení ArSSZ[53] , které zakládalo právní domněnku pravosti elektronických dokumentů, v případě že byly podepsány uznávaným elektronickým podpisem a v době podpisu navíc opatřeny kvalifikovaným časovým razítkem, nehledělo se však již na to zda certifikát, na kterém bylo razítko založeno je platný. Ustanovení tak v tomto znění působilo dojmem, že není třeba zajišťovat validitu elektronických dokumentů. [54]

Ověřování platnosti elektronických zabezpečovacích prvků se dle nařízení eIDAS vztahuje k okamžiku vytvoření konkrétního zabezpečovacího prvku.[55] Z hlediska prokazatelnosti může být ovšem určení tohoto okamžiku poněkud problematické. Za účelem dlouhodobého udržení ověřitelnosti elektronických zabezpečovacích prvků nabízí nařízení eIDAS možnost realizace služby vytvářející důvěru.[56] Služba vytvářející důvěru by spočívala v postupech a technologiích, které jsou způsobilé zajistit důvěryhodnost kvalifikovaného elektronického podpisu, a to po uplynutí jeho technické platnosti.

K pojmu technické platnosti není v nařízení eIDAS obsažena žádná bližší specifikace, ale je to poprvé co toto nařízení připouští, že elektronický podpis může pozbýt určité platnosti, resp. nepozbývá platnosti, ale snižuje se kvalita jeho ověřitelnosti. Z hlediska aplikovaných technologií může dojít k vypršení platnosti certifikátů, prolomení bezpečnosti použitých kryptografických algoritmů, což vede ke snížení důvěryhodností těchto algoritmů. *„Opatření, která lze aplikovat pro snížení rizika snížení důkazní spolehlivosti elektronických dokumentů z důvodu omezené technické platnosti elektronického podpisu, musí být vždy ve spojitosti procesních i technických kroků.“* (s. 267, [1])

[52] K tomu viz s. 266 [1].

[53] Jednalo se konkrétně o §69a odst. 5 ArSSZ – ustanovení bylo zrušeno v souvislosti se změnovým zákonem 298/2016 Sb. a podrobněji bude probráno dále.

[54] K tomu viz s. 266 [1] a s. 103–108 [4].

[55] K tomu viz čl. 32-34 nařízení eIDAS – pokud se jedná o elektronickou pečeť, použijí se přiměřeně zmíněná ustanovení dle čl. 40.

[56] V režimu čl. 34 odst. 1 nařízení eIDAS.

1.3.3 Vyvratitelná domněnka pravosti

Vyvratitelnou domněnku pravosti (nebo také presumpci pravosti) vnášelo do právního řádu ustanovení § 69a odst. 5 ArSSZ (ve znění platném od 1.července 2012):[57] *„**Neprokáže-li se opak**, dokument v digitální podobě se považuje za pravý, byl-li podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, a následně za doby platnosti uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, nebo uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, opatřen kvalifikovaným časovým razítkem. To platí i pro dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.“* [58] (§ 69a odst. 5 [3] ve znění platném od 1. července 2012)

Jak si lze povšimnout, ustanovení má podobu implikace: pokud dojde k naplnění předpokladů (byl-li dokument podepsán, resp. opatřen značkou), vyplývá z nich určitý důsledek (dokument se považuje za pravý). (s. 161, [10]) První část ustanovení tedy formuluje vyvratitelnou domněnku a dále následují podmínky, za kterých nastává presumpce pravosti dokumentu, a to:

- dokument je opatřen uznávaným elektronickým podpisem založeném na kvalifikovaném certifikátu (nebo označen stejnou úrovní elektronické značky),
- dokument je podepsán či označen oprávněnou osobou,
- dokument je opatřen kvalifikovaným časovým razítkem.

V souvislosti s tímto ustanovením se vyvinulo mylné přesvědčení, že při splnění podmínek stanovených ve výše citovaném znění není třeba se o elektronické dokumenty dále starat a zajišťovat jejich důvěryhodnost (s. 104–107, [4]). V praxi ustanovení vedlo k situaci, kdy se platnost dokumentů odvozovala od technické platnosti a elektronické dokumenty se opatřovaly jediným časovým razítkem na libovolně dlouhou dobu. Zastánci tohoto přístupu se tak domnívali, že praxe přerazítkovávání již není nutná. [27]

Kontroverzní ustanovení tak vneslo do právního systému řadu nepřesných formulací a mylných závěrů a není tedy překvapením, že bylo zrušeno změnovým zákonem č. 298/2016 Sb.[59] Zrušení dlouho diskutovaného ustanovení tak vedlo ke konečnému závěru, že o elektronické dokumenty je třeba se aktivně starat a využívat praxe pře-

[57] Vyvratitelná domněnka znamená, že uvedené platí, dokud se neprokáže opak (tzn. připouští se důkaz *a contrario*, tedy důkazu opaku). „[P]ouhá, třebas i závažná pochybnost o tom, zda existuje skutečnost, které svědčí právní domněnka, nestačí k tomu, aby tato skutečnost nebyla považována za prokázanou.“[29] V ustanovení je vyvratitelná domněnka zvýrazněna.

[58] Zde je namístě upozornit, že pojmy *uznávaný podpis* a *elektronická značka* měli jinou právní definici než je tomu dnes. K definici pojmů v režimu tohoto ustanovení viz § 11 odst. 3–4 [30].

[59] Citované ustanovení podrobně rozebírá T. Lechner, viz s. 104-107 [4].

razítkovávání. Ovšem i zde lze uplatnit výjimku stanovenou v zákoně č. 89/2012 Sb., občanský zákoník (dále NOZ). Pro konkrétní dokument je totiž možné využít domněnky spolehlivosti, která je určena parametry bezpečného úložiště ve smyslu § 562 odst. 2 NOZ, kterému se budeme blíže věnovat v následující kapitole.

1.3.4 Parametry bezpečného úložiště ve smyslu § 562 odst. 2 občanského zákoníku

Jiný přístup k archivaci elektronických dokumentů, než zmiňované přerazítkování či již zrušené ustanovení diskutované výše, představuje § 562 odst. 2 NOZ. Ustanovení nám zakládá vyvratitelnou domněnku spolehlivosti elektronických dokumentů obsažených v elektronickém systému, který splňuje podmínky stanovené tímto ustanovením. Zároveň nám ustanovení § 562 odst. 2 NOZ poskytuje návod řešení problému archivace elektronických dokumentů a to bez použití elektronických zabezpečovacích prostředků. Z těchto důvodů, a také proto, že základní myšlenka samotné aplikace, která má být výstupem praktické části této práce, bude postavena na tomto ustanovení, zde blíže představím § 562 odst. 2 NOZ.

Přesné znění § 562 odst. 2 NOZ je následující: *„**Má se za to**, že záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám. Byl-li záznam pořízen při provozu závodu a dovolá-li se jej druhá strana k svému prospěchu, **má se za to**, že záznam je spolehlivý.“* [60]

Výraz spolehlivost souvisí s vedením záznamů o nějakých skutečnostech bez ohledu na jejich povahu (účetnictví) – konkrétně v NOZ je pojem „spolehlivost“ používán v ustanoveních, kde se mluví o vedení záznamů (konkrétně § 119, § 1414 a § 1547) [28]. Pro upřesnění významu tohoto pojmu je možné se inspirovat ustanovením § 19 odst. 7 ve spojení s § 7 odst. 1 zákona č. 563/1991 Sb., o účetnictví – požadavky na spolehlivou informaci lze shrnout jako požadavek na úplnost informace, včasnost informace, srozumitelnost a požadavek, aby podávala věrný a poctivý obraz předmětu účetnictví.[61]

Pokud se zaměříme pouze na první větu daného znění, vidíme, že zde máme v první části opět obsaženou vyvratitelnou domněnku, kterou nám nyní indikují slova „má se za to“ – první (zvýrazněná) část ustanovení.[62] Tentokrát ovšem nejde o vyvratitelnou domněnku pravosti elektronického dokumentu, která byla diskutována dříve (viz kapitola 1.3.3), nýbrž o vyvratitelnou domněnku spolehlivosti záznamů údajů o právních jednáních obsažených v elektronickém systému.

[60] § 562 odst. 2 [20].

[61] Tak, aby mohla osoba na základě těchto informací činit rozhodnutí.

[62] Jedná se o typickou formulaci v případě vyvratitelné domněnky.

Druhá část první věty zmiňovaného ustanovení stanovuje podmínky (resp. požadavky) spolehlivosti záznamů údajů o právních jednáních v elektronickém systému. Mezi tyto požadavky řadíme:

- požadavek na systematické provádění záznamů,
- požadavek na posloupné provádění záznamů,
- požadavek na dostatečné zabezpečení záznamů vůči změnám.

Předpoklad systematičnosti a posloupnosti vznáší požadavek, aby záznamy byly prováděny chronologicky – podle časové posloupnosti právních jednání (tedy vždy v jejich časové následnosti) a zároveň aby systém zamezil dodatečným změnám v posloupnosti záznamů. Dalším požadavkem je náležitá ochrana prováděných záznamů proti neoprávněným zásahům. Důsledkem takového zásahu by mohla být jakákoliv změna záznamu, tedy včetně změny v posloupnosti záznamu. Jakákoliv taková změna je nepřípustná a vedla by k nenaplnění požadavku na dostatečnou ochranu záznamů v elektronickém systému.[28]

Vyvratitelnou domněnku máme obsaženou i ve druhé větě. Opět se jedná o vyvratitelnou domněnku spolehlivosti záznamů tentokrát ovšem ve spojení s provozem závodu.[63] Podmínky pro splnění vyvratitelné domněnky v tomto případě jsou následující:

- záznam byl pořízen při provozu závodu,
- druhá strana se dovolává tohoto záznamu, a to ke svému prospěchu.

Oproti první větě je tedy v případě, že záznam údajů byl pořízen při provozu závodu, potom dojde-li k tomu, že se druhá strana dovolá záznamu údajů o právním jednání ke svému prospěchu,[64] platí presumpce spolehlivosti záznamu, ovšem bez nutnosti splnění podmínek obsažených v první větě § 562 odst. 2 (systematičnost a posloupnost v provádění záznamů a dostatečná ochrana záznamů). [28]

Dané ustanovení bude mít zásadní dopad na problematiku dokazování, jelikož subjekt, který záznamy údajů o právních jednáních vede, bude muset prokázat, že se jedná o přístup systematický, posloupný a že daný systém je chráněn proti změnám. Pokud tyto předpoklady ale splní, nebude muset prokazovat uvedené záznamy a soud je bude považovat za spolehlivé, neboť skutečnost, které svědčí vyvratitelná právní domněnka není předmětem procesního dokazování. [31, 32]

Dle M. Zuklínové toto ustanovení vybočuje z mezí obvyklého obsahu zákona (tj. občanského zákoníku), a to proto že úprava dané problematiky spadá spíše do dikce veřejného práva [28].[65]

[63] Obchodní závod je v režimu § 502 NOZ *„organizovaný soubor jmění, který podnikatel vytvořil a který z jeho vůle slouží k provozování jeho činnosti. Má se za to, že závod tvoří vše, co zpravidla slouží k jeho provozu.“* – §562 [20].

[64] Tím rozumíme, že tato strana hledá svůj prospěch a domnívá se, že v záznamu nalezne potřebný důkaz o právním jednání, jeho obsahu, apod. [28]

[65] Dalším takovým ustanovením je podle M. Zuklínové ustanovení o veřejných a soukromých

1.4 Národní digitální archiv

Problematickou se stává zejména dlouhodobá archivace a to zejména z technického hlediska – především problémy s technickým pokrokem v jehož důsledku dochází k zastarávání formátů, nosiče apod. Navíc roste zájem veřejnosti o poskytování informací vzdáleným přístupem. Z těchto důvodů byl zahájen projekt Národní digitální archiv (NDA), který spadá pod Národní archiv.

Národní archiv je ústředním orgánem České republiky, jeho základním úkolem je uchování a zpřístupnění informací pro současné a budoucí potřeby společnosti. Zatímco uchovávání informací v listinné podobě se opírá o mnohaleté zkušenosti, situace s elektronickými dokumenty je zcela jiná. V posledních letech se uplatňuje trend elektronizace státní správy. Se zvyšujícím se podílem elektronicky vedených agend se zvyšuje potřeba dlouhodobého zabezpečení těchto informací [33].

V současné době neexistuje v České republice žádný institut pro zajišťující dlouhodobou archivaci digitálních informací vzniklých elektronicky či digitalizovaných z analogové formy. Cílem tohoto projektu je vybudování servisního pracoviště, který by zajišťoval následující:

- dlouhodobé uchování archiválií vybraných veřejnými archivy [66]
- provoz archivního portálu
- zpřístupnění dokumentů
- podporu institucí (původců) a archivů při skartačním řízení
- podpora při zpracování digitálních archiválií
- bezpečné uložení digitálních reprodukcí tradičních archiválií [33, 34]

Projekt NDA je součástí efektivní veřejné správy[67], která si klade za cíl přiblížit občanům veřejné služby a zajistit maximální dostupnost a kvalitu těchto služeb. Myšlenka NDA je taková, že by uživatelé přistupovali k uloženým archiváliím přes archivní portál. Archivní portál uživatelům zpřístupní uchovávané archiválie a zpracuje o nich potřebné údaje. Portál bude propojen se současnými informačními systémy archivů a veřejné správy a dále by měl být napojen na ostatní paměťové instituce (muzea, knihovny), přičemž se do budoucna počítá s propojením až na mezinárodní úrovni.

Právě kvůli potřebě bezpečného ukládání digitálních dokumentů vzniklo Pracoviště pro dlouhodobé uchovávání a zpřístupňování dokumentů v digitální podobě. Úkolem tohoto pracoviště je stanovení způsobu nakládání s digitálními dokumenty tak, aby bylo dosaženo jejich dostupnosti, čitelnosti a důvěryhodnosti s odstupem času. O možnostech digitální archivace se v České republice vedou úvahy již mnoho

listinách – viz § 565 a 569 [20].

[66] K pojmu archiválie viz § 2 písm. f) ArSSZ.

[67] Smart Administration

let – konkrétní podobu dostaly až v usnesení vlády č. 11 ze 7. ledna 2004. Vláda tak uložila místopředsedovi vlády a ministru vnitra zpracovat ve spolupráci s ministrem informatiky projekt dlouhodobého uchovávání a zpřístupňování dokumentů v digitální podobě. [33]

V předkládací zprávě bylo opět upozorněno na nutnost archivace digitálních dokumentů, neboť pokud nebude problematika archivace těchto dokumentů vyřešena, hrozí ztráta informací ukládaných digitálně. Dále je zde stanovena povinnost Ministerstva vnitra vytvořit podmínky pro činnost odborného týmu, ten bude tvořit základ pracoviště (digitálního archivu) zaměřeného právě na dlouhodobé uchovávání digitálních archiválií. Pracoviště vznikne při Státním ústředním archivu v Praze a na základě zkušeností z provozu by postupně mohla vznikat regionální pracoviště. Předkládací zpráva dále vznesla předpoklad zpracování podkladů pro zadání projektu dlouhodobého uchování digitálních archiválií a to do roku 2004, podklady měl zpracovávat tým odborníků – hardwarový a softwarový odborník, archivář a operátor. Na základě těchto podkladů měl být vybudován digitální archiv. [35].

V roce 2005 byl tedy ustaven tým pro přípravu digitálního archivu, který vypracoval zadávací dokumentaci v průběhu roku 2006. Národní archiv následně vyhlásil výběrové řízení na zpracovatele tohoto projektu a vítěz výběrového řízení poté vypracoval technologický projekt Pracoviště pro dlouhodobé uchovávání a zpřístupňování dokumentů v digitální podobě.[68] Digitalizace archiválií přináší mnoho výhod pro různé cílové skupiny. Výhody jsou shrnuty v tabulce 1.3. [69]

Původci archiválií	Možnost dlouhodobého uložení digitálních dokumentů bezpečným způsobem Použitelnost dokumentů jako důkazního materiálu Snadné a rychlé vyhledávání dokumentů Efektivní využívání dokumentů pro svou činnost
Veřejné archivy	Možnost garantovaného uložení digitálních archiválií a jejich reprodukcí Efektivní práce s elektronickými archiváliemi
Veřejnost	Bezplatný přístup k digitálním archiváliím či reprodukcím pomocí internetu

Tab. 1.3: Výhody digitalizace archiválií

1.4.1 Technické řešení Národního digitálního archivu

Navrhované řešení NDA je postaveno na standardu OAIS (Open Archival Information System)[70] a splňuje znaky důvěryhodného repozitáře – dlouhodobě zajišťuje

[68] Součástí dokumentu je spoustu nákresů a návrhů možného řešení archivu. Nákresy jsou v rámci kapitoly představeny a popsány.

[69] Poznámka k tabulce: bezpečným způsobem rozumíme takový způsob, který zajišťuje důvěryhodnost dokumentu v čase. Tabulka zpracována na základě informací uvedených v [33].

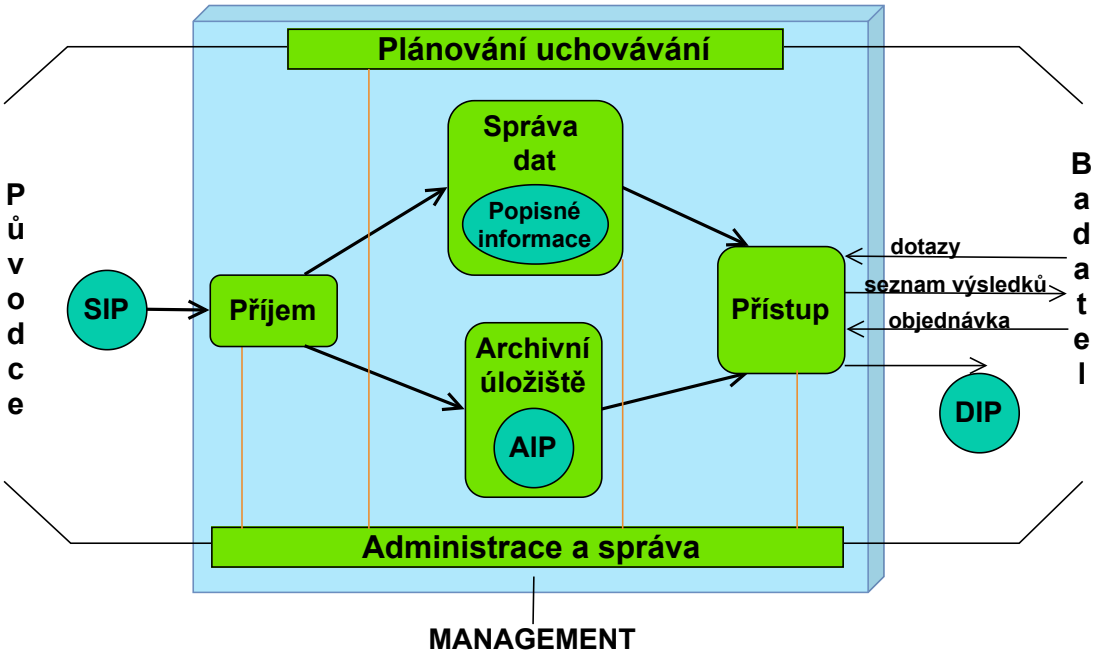
[70] Jedná se o ISO 14721:2003.

důvěryhodnost, použitelnost a dostupnost uložených a uchovávaných dat.[71] OAIS je konceptuální model dlouhodobého archivu. Popisuje základní komponenty dlouhodobého archivu, související funkce a vazby. Zároveň je také informačním modelem. OAIS vymezuje základní koncepci archivu pro ukládání elektronických dokumentů a v současné době je na něm založena většina archivů tohoto typu. Mezi základní funkce, které by měl archiv zajišťovat, podle tohoto standardu, patří zejména příjem, správa dat, archivní uložení atd. [37]

Elektronický dokument a všechny popisné informace (metadata) jsou zabaleny do balíčku s jednotnou strukturou. [72] Standard OAIS rozlišuje tři typy balíčků:

- **Submission Information Package (dále SIP)** – jde o balíčky přijímané od původců
- **Archival Information Package (dále AIP)** – jedná se o archivní balíčky, které zahrnují ukládaný obsah a příslušné popisné informace pro uchovávání (tzv. metadata)
- **Dissemination Information Package (dále DIP)** – tyto balíčky jsou vytvořené na základě badatelského dotazu

Nákres základního modelu OAIS a jeho funkčních celků je na obrázku 1.5.[73] [33]

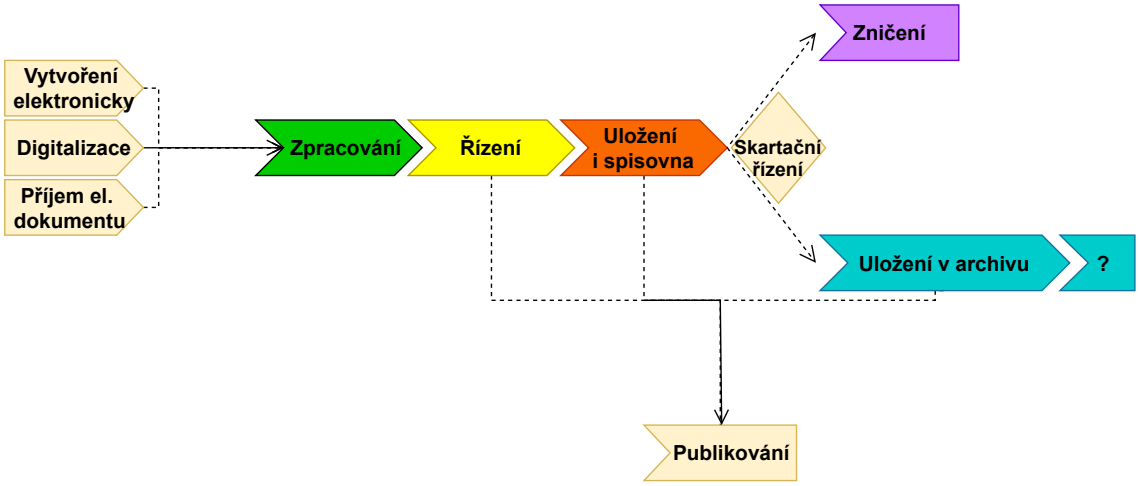


Obr. 1.5: Základní model OAIS

Elektronický dokument, který bude potřeba archivovat (tedy bude označen za archiválii), bude nejdříve převeden na straně původce dokumentu do podoby vhodné

[71] K tomu viz s. 268 [1]
[72] K problematice balíčků viz s. 94–97 [36].
[73] Veškeré obrázky této kapitoly jsou inspirovány [36].

pro předání do archivu – tedy bude vytvořen balíček typu SIP. Součástí balíčku budou také příslušná metadata, která budou pořizována během celého životního cyklu dokumentu. Životní cyklus dokumentu je naznačen na obrázku 1.6. [74]



Obr. 1.6: Životní cyklus elektronického dokumentu

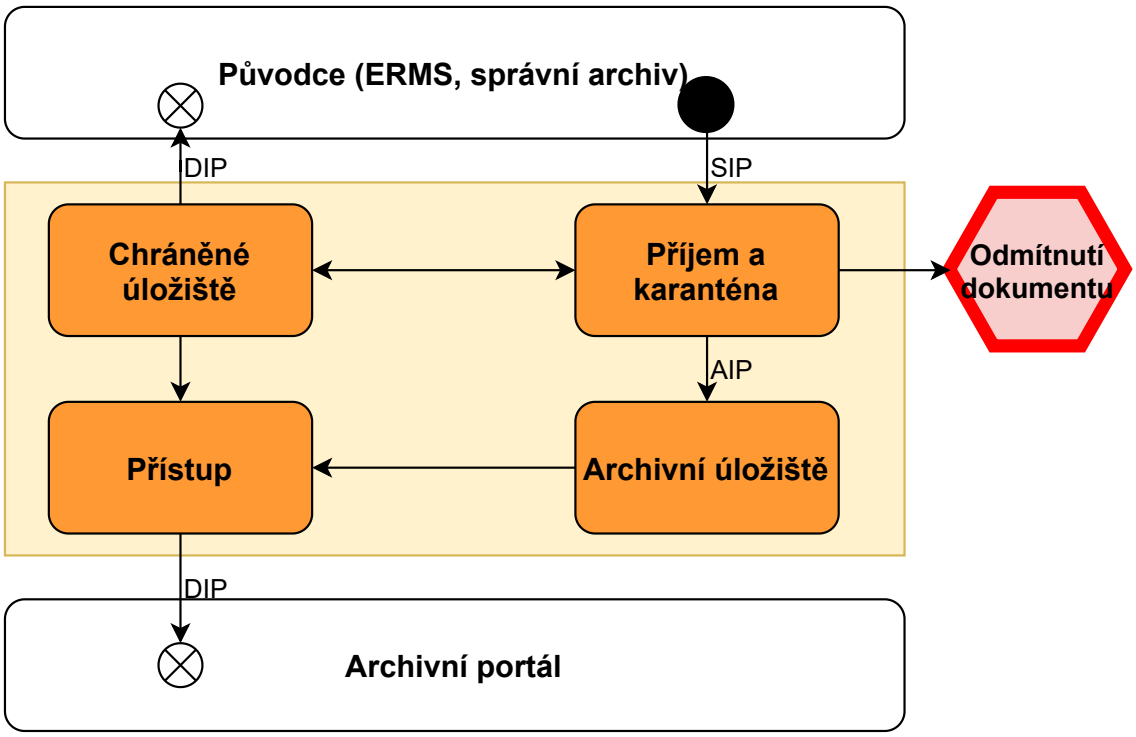
Zaslaný balíček bude nejdříve umístěn do karantény, kde bude zkontrolováno, že soubory neobsahují škodlivý kód – kontrola proběhne dvakrát s časovým odstupem třiceti dní. V případě že dokument bude v tomto ohledu nezávadný, proběhne další kontrola balíčku – ta bude zaměřena především na formát souborů a rozsah vyplnění metadat. Dokument bude odmítnut, pokud bude obsahovat škodlivý kód nebo nebude ve vhodném formátu či nebude obsahovat požadovaná metadata. V případě odmítnutí dokumentu bude původce o této skutečnosti informován.

Přijatý balíček bude nadále zpracováván. V rámci procesu zpracování bude balíček doplněn o metadata podporující procesy řízení uchovávání a zpřístupňování, následně bude dokumentu přidělen jednoznačný identifikátor v rámci digitálního archivu. Proces zpracování povede k vytvoření balíčku AIP (tedy archivního informačního balíčku). Balíček AIP bude uložen do archivního úložiště s řízeným přístupem.

Jelikož v průběhu prací na technologickém projektu bylo třeba vyřešit otázku dokumentů, které sice nejsou digitálními archiváliemi, ale které by bylo dobré taktéž uchovat, byl do schématu archivu zařazen i mezisklad digitálních dokumentů (*chráněné úložiště*). Sem mohou být uloženy balíčky, které původce poslal do archivu, ale nesplňují předepsaná kritéria popsána výše. Takový balíček bude možno tedy vrátit původci nebo jej zde uložit v úložišti a původce ho ve spolupráci s archivem opraví. Stejně tak mohou být v úložišti uchovány dokumenty s dlouhými skartačními lhůtami nebo zde mohou být uchovávány digitální obrazy klasických archiválií.

[74] Viz s. 19 [36].

[33, 36] Na obrázku 1.7 je znázorněno základní navržené schéma digitálního archivu, které bylo popsáno výše.



Obr. 1.7: Schéma digitálního archivu

Důležitou podmínkou archivního úložiště je, že každý dokument musí být opatřen alespoň základními metadaty[75] jako např.: původce, systémový identifikátor souboru, datum vzniku, název, obsah apod.

Archiv bude také umožňovat zpřístupnění uložených dokumentů. Uživatel zadá svůj požadavek do webového portálu NDA, který mu požadovaný dokument následně zpřístupní. Modul *přístup* žádost zpracuje a vytvoří balíček DIP, který bude uživateli (badateli) opět prostřednictvím webového portálu NDA zobrazen. Obsah balíčku DIP pak bude závislý na požadavku uživatele – balíček bude moci obsahovat seznam přístupných dokumentů včetně jejich náhledů nebo konkrétní dokument s jeho metadaty. Stejně tak může být uživateli zobrazena informace o omezení přístupnosti dokumentu apod. [33]

Jak jsme již dříve v této práci zmínili, při uchovávání elektronického dokumentu musíme zajistit vlastní zachování dokumentu (tedy uložení dat) i čitelnost dokumentu. Zachování dokumentu je v projektu NDA řešeno tak, že dokument bude v archivu zajištěn uložením na dvou geograficky oddělených místech.

[75] Tedy nebude možné ukládat nepopsané dokumenty.

NDA se zároveň zabývá otázkou zajištění čitelnosti dokumentů. NDA bude využívat pro zajištění dlouhodobé čitelnosti dokumentů metodu migrace. Metoda migrace spočívá v přizpůsobení dat prostředí, tzn. že dokumenty uložené ve formátech, které nebude možné interpretovat budou převedeny do vhodnějšího formátu.[76] Z pohledu životního cyklu se nabízí tři okamžiky pro provedení migrace – migrace na vstupu, dávková migrace a migrace při přístupu. [77]

NDA musí mít pro každý formát dokumentu přebíraného do archivu vypracovanou strategii uchovávání, pokud neexistuje tato strategie digitální archiv nemůže přijmout daný dokument. V technologickém projektu jsou formáty rozděleny do tří skupin podle jejich životnosti:

- **preferované formáty** – vhodné pro dlouhodobé uchovávání, budou tedy přebírány do archivu bez migrace
- **akceptované** – méně vhodné pro dlouhodobé uchovávání, není je však nutné v okamžiku předání migrovat
- **neakceptované** –nejpozději při předání do archivu jsou migrovány ideálně na preferovaný formát

„Nejvhodnějším okamžikem pro převod dokumentu do preferovaného formátu se jeví okamžik jeho vyřízení (uzavření) u původce.“ [33]

V rámci NDA je také nutné zajistit autenticitu dokumentů, tedy, že dokument nebyl v průběhu uložení změněn a že migrací dokumentu nedošlo ke ztrátě dat. Principem zachování autenticity dokumentů v rámci NDA je fyzické a procesní zajištění uložených dokumentů vůči změnám a transparentní, dokumentovaný způsob migrace [36]. Tento princip vyžaduje certifikaci digitálního archivu třetí stranou jako důvěryhodné úložiště, tedy že splňuje požadavky takového úložiště jak po stránce fyzické bezpečnosti, tak i po stránce procesní. Jednou z navrhovaných možností je posouzení archivu Národním bezpečnostním úřadem. [33]

Při dlouhodobém uchovávání digitálních dokumentů je třeba vedle samotného dokumentu uchovávat i další informace – metadata. Metadata nám poskytují informace např. o formátu dokumentu, o manipulaci s dokumentem apod. Jelikož NDA je postaven na protokolu OAIS budou veškerá metadata spolu s dokumentem součástí AIP balíčku. Rozlišujeme tři skupiny metadat – popisná, konzervační (neboli uchovávací) a strukturální. [78]

Popisná metadata jsou určena pro vyjádření obsahu digitálních dokumentů, často jsou proto používána k vyhledávání nebo k zařazení objektu a zjištění základních údajů o něm – typicky se jedná například o název, autora, původce atd. Mohou vznikat po celou dobu života elektronického dokumentu ale typicky vznikají ve fázi

[76] K dalším metodám zajištění dlouhodobé čitelnosti viz [36] str. 48 a násl.
[77] Viz s. 46 [36].
[78] K tomu viz s. 34 [36].

příjmu a zpracování u původce a během archivního zpracování dokumentu. Klíčovou fází je pro vznik popisných metadat zejména fáze příjmu a zpracování u původce, jelikož metadata, která nebudou zachycena v této fázi bude velmi těžké (až nemožné) doplnit později. Popisná metadata, která je potřeba zaznamenat se v současnosti běžně evidují[79] nebo je automaticky generuje systém správy dokumentů (ERMS).[80] Popisná metadata vycházejí z doporučení Moreq2 vypracovaného organizací DLM fórum. [33]

Konzervační metadata jsou určena pro podporu a uchovávání archivačních aktivit. Jejich obsahem jsou údaje o formátu dokumentu dále technické údaje o uložených digitálních objektech a informace o činnostech nebo změnách provedených s digitálním obsahem apod. Taktéž vznikají po celou dobu života dokumentu zejména však v digitálním archivu právě proto, že digitální archiválie budou po větší část svého životního cyklu uloženy v digitálním archivu. Informace o formátu dokumentu je zásadní pro volbu okamžiku a způsobu migrace, stejně tak informace o změnách dokumentu je stěžejní informací tentokrát však při zajišťování autenticity dokumentu. Podobně jako u popisných metadat se bude u konzervačních metadat vycházet z Národního standardu pro elektronické systémy spisové služby.

Poslední skupinu metadat tvoří strukturální metadata. Účelem strukturálních metadat je sdružení všech částí informačního balíčku do jednoho logického celku. Popisují souvislosti mezi jednotlivými částmi. Dokument bude v archivu uložen spolu se souvisejícími metadaty v rámci AIP balíčku – metadata se mohou vztahovat k celému archivnímu balíčku nebo pouze k určitému objektu. A právě závislosti a vztahy jednotlivých částí popisují strukturální metadata. [36]

[79] Například pořadové číslo, spisový znak apod.
[80] Například datum přijetí.

2 Praktická část bakalářské práce

Cílem teoretické části práce bylo zanalyzovat postavení elektronického dokumentu v českém právním prostředí, přiblížit problematiku archivace elektronických dokumentů a představit možné způsoby archivace.

V rámci praktické části bude popsáno řešení samotné aplikace pro správu elektronických dokumentů, vycházející z poznatků získaných v teoretické části bakalářské práce, které jsou propojeny a vhodně implementovány tak, aby splňovaly zákonné požadavky. Z možností archivace dokumentů, které byly popsány v rámci kapitoly 1.3 byl pro potřeby praktické části zvolen systém, jehož základní myšlenka vychází z § 562. odst. 2 NOZ.

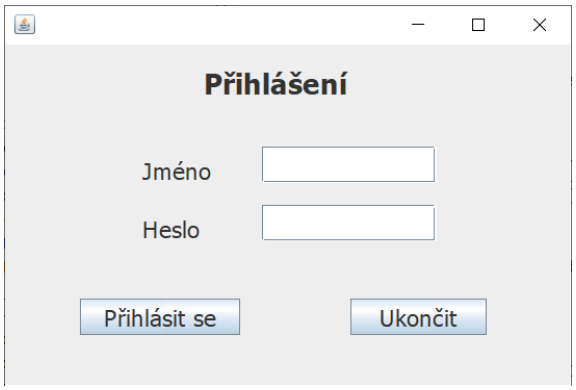
Jedná se tedy o systém, který splňuje podmínky stanovené v § 562. odst. 2 NOZ, a tím naplňuje vyvratitelnou domněnku spolehlivosti. Nejdůležitější částí tohoto systému tak bude implementace logů, které budou zaznamenávat posloupnost událostí, které v systému nastanou. Občanský zákoník v tomto ustanovení však nezmiňuje nic o formátech takto uložených dokumentů. Podle tohoto ustanovení by tedy v takovém systému mohly být archivovány i soubory ve formátech, které nejsou vhodné z hlediska dlouhodobé archivace, neboť nezaručují dlouhodobou čitelnost dokumentů. Z tohoto důvodu je systém doplněn o možnost převodu formátu a tato myšlenka vychází z metody migrace, která je součástí návrhu technického řešení NDA, který byl popsán v kapitole 1.4.1.

2.1 Popis aplikace

Aplikace je tvořena dvěma okny – oknem pro přihlášení uživatele a oknem pro práci s úložištěm. Při spuštění aplikace se zobrazí okno pro přihlášení. V okně pro přihlášení je třeba zadat identifikaci uživatele a heslo pro přístup do aplikace. Hlavní okno aplikace pro práci s úložištěm se otevře po vložení správných přihlašovacích údajů[1] a po stisknutí tlačítka „Přihlásit se“. V okně pro přihlášení může uživatel také aplikaci zcela ukončit kliknutím na tlačítko „Ukončit“. V případě, že zvolí tuto možnost, bude systémem dotázán, zda si opravdu přeje aplikaci ukončit a na základě jeho volby bude aplikace ukončena nebo bude uživatel navrácen zpět do okna pro přihlášení. Veškerá přihlášení, resp. pokus o přihlášení či ukončení aplikace jsou monitorovány a jsou zapsány jako samostatné události do logovacího souboru `logy.txt`.

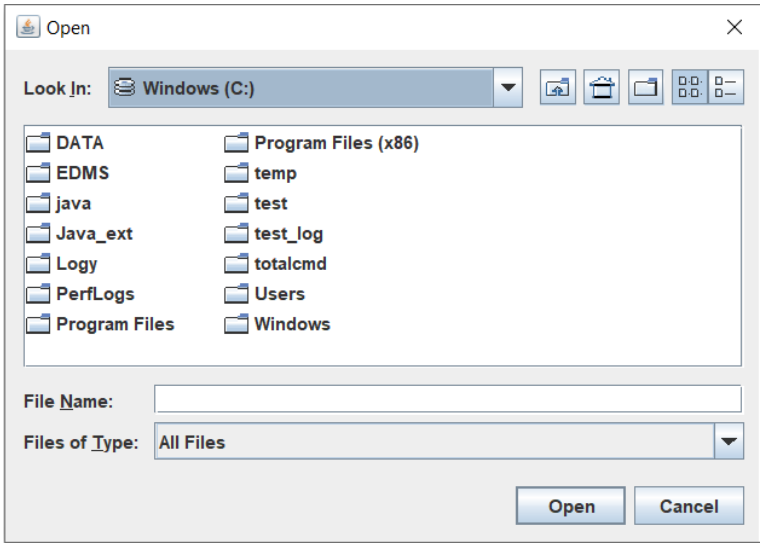
Hlavní okno aplikace umožňuje práci se soubory v úložišti. Konkrétně je možné provést operace – nahrání nového souboru do úložiště, výmaz souboru z úložiště

[1] V našem případě je přihlašovací jméno admin a heslo taktéž admin.



Obr. 2.1: Ukázka okna „Přihlášení“

a převedení vybraných formátů do vhodného formátu z hlediska dlouhodobé archivace.[2] V levé části okna pro práci se soubory je seznam souborů umístěných v adresáři. Pro jednotlivé operace jsou vytvořena tlačítka, po jejichž stisknutí se konkrétní operace provede. Při stisknutí tlačítka „Nahrát do úložiště“ se otevře nové okno se strukturou adresářů, ve kterém je možné zvolit soubor, který bude nahrán do úložiště. Z okna pro práci s úložištěm je taktéž možné ukončit celou aplikaci stisknutím tlačítka „Ukončení aplikace“.



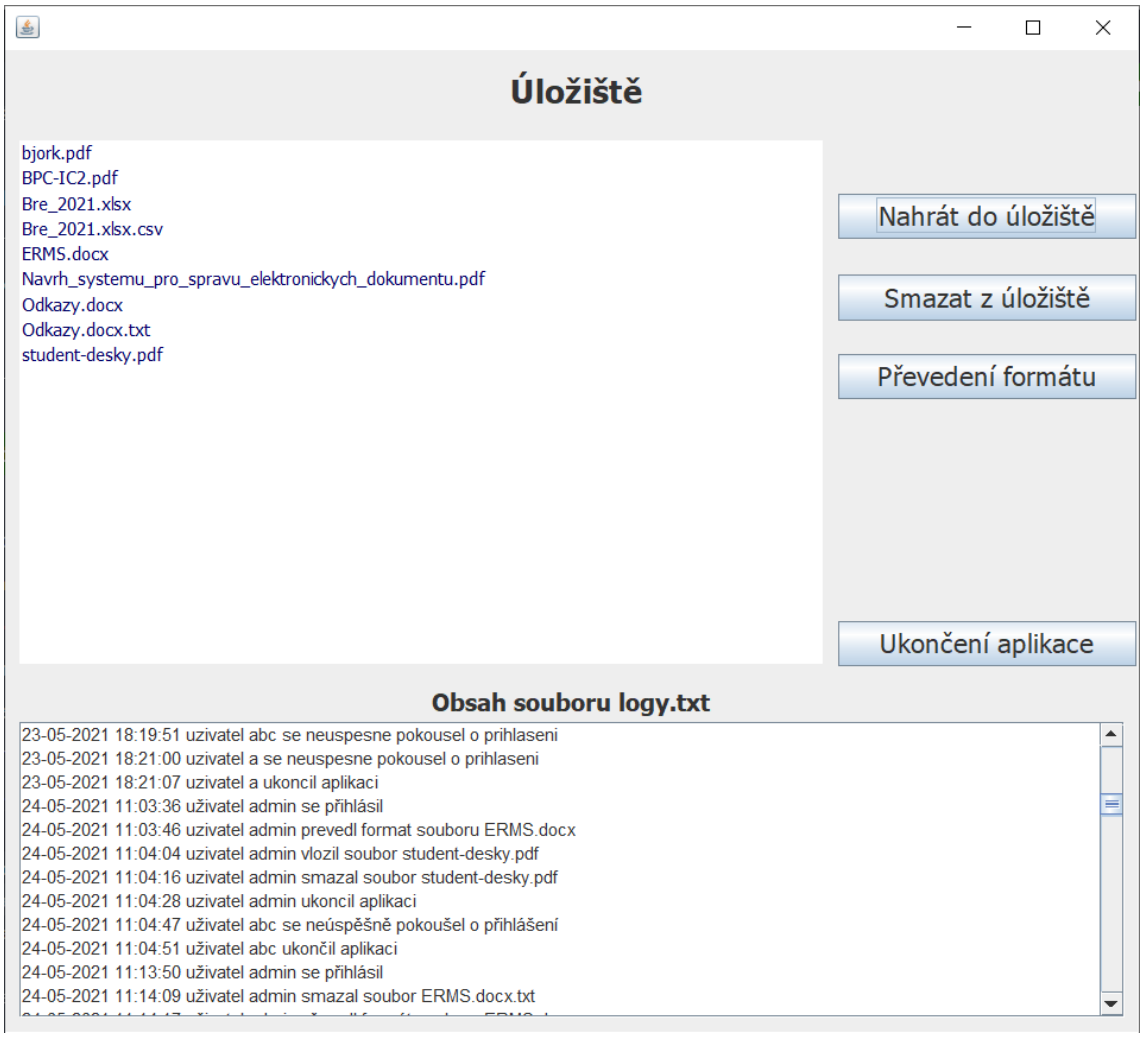
Obr. 2.2: Ukázka okna „Adresářová struktura“

Úložiště je vybraný adresář umístěný na lokálním disku. Uživatelem provedené aktivity v tomto adresáři[3] případně v jeho podadresářích jsou aplikací monitorovány

[2] Jedná se o převedení formátu .docx na .txt a .xlsx na .csv.

[3] Konkrétně jsou monitorovány operace typu vytvoření souboru resp. nahrání souboru, výmaz souboru, modifikace souboru a změna formátu.

a zaznamenávány jako samostatné události do logovacího souboru `logy.txt`. Monitorovány jsou operace provedené prostřednictvím aplikace, ale také jsou monitorovány jakékoliv změny souborů uložených v daném úložišti libovolnou jinou aplikací.[4] V dolní části okna pro práci s úložištěm je zobrazen obsah souboru `logy.txt`, který je při provedení určité operace aktualizován.



Obr. 2.3: Ukázka okna „Úložiště“

Záznamy v souboru `logy.txt` obsahují časové razítko, identifikaci uživatele, který operaci provedl, popis operace a případně i identifikaci souboru, u kterého byla provedena daná operace. Soubor se záznamy logů je šifrován pomocí AES a je tak vytvořen soubor `logy.crp` – přípona `.crp` značí, že se jedná o šifrovaný dokument. Při spuštění aplikace je soubor s logy dešifrován, aby bylo možné do něj

[4]Jinou aplikací se rozumí např. průzkumník souborů v OS Windows nebo např. Total Commander, atd.

dál zapisovat a při ukončení je opět zašifrován. Pro demonstrativní účely je však v adresáři s logy umístěn i soubor `logy.txt`.

Výpis 2.1: Ukázka výpisu souboru logy.txt.

```
24-05-2021 11:13:50 uživatel admin se přihlásil
24-05-2021 11:14:09 uživatel admin smazal soubor
                    ERMS.docx.txt
24-05-2021 11:14:17 uživatel admin převedl formát z .docx
                    na .txt souboru ERMS.docx
24-05-2021 11:14:31 uživatel admin vložil soubor
                    student-desky.pdf
24-05-2021 11:14:41 uživatel admin ukončil aplikaci
24-05-2021 11:14:57 uživatel 123 se neúspěšně pokoušel
                    o přihlášení
24-05-2021 11:15:00 uživatel 123 ukončil aplikaci
------------------------------------------------------------
26-05-2021 22:05:06 uživatel admin vytvořil soubor
                    C:\EDMS\student-desky.pdf, vytvořeno WD
26-05-2021 22:05:09 uživatel admin upravil soubor
                    C:\EDMS\student-desky.pdf, vytvořeno WD
26-05-2021 22:05:13 uživatel admin smazal soubor
                    C:\EDMS\student-desky.pdf, vytvořeno WD
```

Na ukázce výpisu jsou odděleny logy, které jsou zcela implementovány námi a logy, které jsou vytvářeny třídou `WatchDir`.[5] Tato metoda byla implementována, neboť `WatchDir` nesleduje pouze změny provedené přímo v aplikaci, ale sleduje i změny provedené tzv. z venčí, tedy např. v průzkumníku souborů. Navíc logy vytvářené třídou `WatchDir` jsou schopny zachytit i operaci úpravy dokumentu, což námi implementované logy nesvedou. Oba druhy záznamů jsou vkládány do souboru `logy.txt`. Za účelem rozlišení záznamů je do výpisu doplněna fráze „vytvořeno WD“, jedná–li se o log vytvořený `WatchDirem`. Podrobnější rozebrání obou metod bude provedeno v kap. 2.2.3.

2.2 Technické řešení aplikace

Pro realizaci aplikace byl zvolen objektově orientovaný programovací jazyk `Java`. Pro vývoj aplikace bylo použito vývojové prostředí `Eclipse IDE for Java Developers` ve verzi `2021-03`.

[5] Zkráceně WD, jak je možno vidět na výpisu.

Program je tvořen dvěma vlákny, samotná aplikace běží v jednom vlákně, zatímco ve druhém běží metody třídy `WatchDir3` pro monitorování událostí. Obě vlákna běží paralelně.

V rámci implementace naší aplikace bylo vytvořeno šest tříd:

- **BP_login** – okno a logika pro přihlašování do systému
- **BP_dir** – okno a metody pro práci s úložištěm
- **WatchDir3** – metody pro hlídání operací v úložišti provedené i mimo aplikaci
- **WriteToLog** – metoda pro zapisování událostí do logovacího souboru
- **CryptoUtils** – metody pro zašifrování a dešifrování logovacího souboru
- **XlsxToCsv** – metoda pro převedení formátu z .xlsx do .csv

Při realizaci programu byla využita řada knihoven – převážně se jedná o standardní knihovny či standardní rozšíření Javy. Pro práci se soubory bylo využito knihoven `Java IO, Java NIO`. K vytváření logů byly využity knihovny pro vytvoření časového razítka a naformátování aktuálního data `Java Text, Java Util`, dále knihovny určeny pro práci se soubory `Java IO, Java NIO`.[6] Zašifrování a dešifrování souborů je řešeno pomocí knihovny `Java Security, Java Crypto`. GUI je řešeno s využitím knihoven `Java AWT, Javax Swing`. Pro převádění formátů byla využita knihovna `Apache POI`.[7]

2.2.1 GUI

Okno pro přihlášení a hlavní okno pro práci s úložištěm bylo vytvořeno pomocí knihovny `Java Swing`. Jedná se o knihovnu, která poskytuje nástroje pro tvorbu a obsluhu GUI. Přes `Window Builder` a `Swing Designer` je tak možné vytvořit `Application Window`, kde v části `Design` lze navrhnout GUI a prostřednictvím knihovny `Swing` je generován zdrojový kód v okně `Source Code`. Je tak možné prostřednictví této knihovny vytvářet okna, tlačítka, textová pole, zaškrtávací pole apod. Okno se strukturou adresářů je standardním oknem vytvořeným pomocí `Swing` – jedná se o tzv. `JFileChooser`. Při vytváření GUI byla taktéž využita knihovna `Java AWT`, ze které `Swing` vychází.[8] GUI jednotlivých oken je možné vidět na obrázcích 2.1, 2.2, 2.3.

[6] V knihovně `Java NIO` jsou také definovány standardní operace, jejichž provedení sleduje `WatchDir` – konkrétně v balíčku `java.nio.file.StandardWatchEventKinds.*`.

[7] Dokumentace všech knihoven jsou dostupné na oficiálních stránkách Oracle <`https://docs.oracle.com/javase/7/docs/api/`>. K Apache POI viz <`https://poi.apache.org/apidocs/dev/index.html`>.

[8] Mnoho komponent, které `Swing` používá jsou rozšířenou verzí komponent které zaváděla knihovna `Java AWT`.

2.2.2 Operace se soubory

Aplikace podporuje následující operace se soubory – vložení souboru do úložiště, výmaz souboru z úložiště a převedení formátu souboru. Aplikace neumožňuje přímo provádět změny obsahu souboru, ale sleduje jakékoliv změny obsahu provedené prostřednictvím jiné aplikace (tzv. z venčí). Operace se soubory jsou implementovány prostřednictvím metody `actionPerformed` definované u konkrétního tlačítka, kterým se daná operace provádí. Při provedení jakékoliv operace je aktualizován výpis souborů v úložišti, který se zobrazuje v okně pro práci se soubory. Veškeré operace jsou monitorovány metodami pro sledování ztěchto operací a vytváření logů.

Nahrání souboru a výmaz souboru

Nahrání souboru a výmaz souboru se provádí pomocí tlačítek „Nahrát do úložiště“ a „Smazat z úložiště“. Obě operace využívají knihovny `Java IO` a `Java NIO`, což jsou standardní knihovny pro práci se soubory. Zároveň jsou v aplikaci ošetřeny případné výjimky, ke kterým by mohlo při provádění těchto operací dojít - např. `IOException`. U možnosti „Smazat z úložiště“ je navíc doplněno kontextové okno pro potvrzení, že uživatel opravdu chce daný soubor smazat.

Převedení formátu

Jak bylo zmíněno v teoretické části práce, ne všechny formáty jsou vhodné z hlediska dlouhodobé archivace. Proto v aplikaci částečně propojujeme myšlenku spolehlivého úložiště stanovenou v § 562 odst.2 NOZ s metodou migrace navrhovanou v technickém řešení NDA. V aplikaci tak lze převést formát `.docx` na `.txt` a formát `.xlsx` na `.csv`. V rámci metody `actionPerformed` je naimplementován `switch` s případy (`cases`) pro jednotlivé formáty. V úložišti jsou ponechány obě verze dokumentu – dokument v původním formátu a tentýž dokument v novém formátu.

Pro převádění formátů je stěžejní knihovna `Apache POI`, která umožňuje práci se soubory ve formátech Microsoft Office. Kromě této knihovny jsou využívány opět standardní knihovny pro práci se soubory. Převedení formátu z `.docx` je z hlediska implementace jednodušší, neboť se využívá třída `XWPFWordExtractor`, do které je vložen původní dokument jako objekt třídy `XWPFDocument`. Text získaný `XWPFWordExtractorem` je poté vložen do textového souboru a tím je převod formátu hotov. V případě převodu formátu z `.xlsx` je však nutné procházet dokument buňku po buňce a proto se v implementaci objevuje několik vnořených cyklů. Vzhledem ke složitosti metody pro převod tohoto formátu, je tato metoda implementována v rámci samostatné třídy `XlsxToCsv`.

2.2.3 Logy

Námi vytvořená aplikace je úložištěm ve smyslu § 562 odst. 2 NOZ, proto je implementace logů stěžejní částí aplikace. Aplikace používá dvě metody pro vytváření logů – metoda `log` ve třídě `WriteToLog` a metodou `processEvents`, která je součástí třídy `WatchDir3`. Ukázka výpisu souboru `logy.txt` je zobrazen na výpise 2.1.

Logy generované třídou WriteToLog

Součástí třídy je metoda `log`, která generuje záznamy o událostech a zapisuje je do souboru `logy.txt`. Tato metoda vytváří záznamy o následujících operacích – přihlášení uživatele, neúspěšný pokus o přihlášení, ukončení aplikace, nahrání souboru do úložiště, smazání souboru z úložiště a převedení formátu souboru v úložišti. Tato metoda ovšem nerozpozná operace provedené mimo aplikaci (tj. přes průzkumníka souborů) a navíc neumí zaznamenat událost o změně obsahu souboru. Na rozdíl od metody z třídy `WatchDir3` je však konkrétnější v popisu události – například událost změny formátu metoda třídy `WatchDir3` zaznamená obecně jako úpravu souboru, zatímco metoda `log` přesněji specifikuje typ provedené operace, tedy „... uživatel převedl formát z .docx na .txt u souboru...“. Ukázka metody `log` ve třídě `WriteToLog` je na výpise 2.2. [9]

Logy generované třídou WatchDir3

Logy generované třídou `WatchDir3` jsou obecnější, ale umí detekovat jakoukoliv změnu včetně změny obsahu souboru, a to jak v úložišti, tak ve všech jeho podadresářích. Navíc detekuje změny provedené i v jiných aplikacích než je námi implementovaná aplikace pro správu elektronických dokumentů. Například vložení nového souboru do úložiště prostřednictvím průzkumníka souborů nebo změnu obsahu souboru provedenou v aplikace Microsoft Office, apod. Při implementaci třídy `WatchDir3` jsme vycházeli z návodů a příkladů publikovaných na oficiálních stránkách Oracle.[10] Tyto příklady byly modifikovány pro potřeby naší aplikace. Ukázka zdrojového kódu je na výpise 2.3. [11]

Šifrování souboru logy.txt

Logovací soubor je šifrován, aby nebylo možné měnit jeho obsah a aby tak byla zaručena věrohodnost a neporušenost záznamů v tomto souboru. K implementaci me-

[9] Některé příkazy byly pro účely přehlednějšího zobrazení ve výpise zkráceny – např. použití / namísto příkazu `File.separator`.

[10] Viz <`https://docs.oracle.com/javase/tutorial/essential/io/notification.html`>.

[11] Vzhledem k rozsahu třídy `WatchDir3` byl pro ukázku vybrán for cyklus, ve kterém byl naimplementován switch se zápisy do logovacího souboru pro konkrétní události.

tod pro šifrování a dešifrování jsme využili standardních knihoven `Java Security`, `Java Crypto`. Metody pro šifrování a dešifrování jsou implementovány v rámci třídy `CryptoUtils` a volány ze třídy `WriteToLog`. K šifrování souboru byla zvolena standardizovaná symetrická šifra AES. Zašifrovaný soubor má příponu `.crp`. Pro demonstrativní účely byl však v adresáři s logovacími soubory ponechán i nešifrovaný soubor `logy.txt`. Ukázka zdrojového kódu je na výpise 2.4.

Výpis 2.3: For cyklus v metodě processEvents třídy WatchDir3

```
1  for (WatchEvent<?> event : key.pollEvents()) {
2          WatchEvent.Kind kind = event.kind();
3          if (kind == OVERFLOW) {
4            System.err.println("OVERFLOW␣!");
5            continue;
6          }
7          WatchEvent<Path> ev = cast(event);
8          Path name = ev.context();
9          Path child = dir.resolve(name);
10
11         switch (event.kind().name()) {
12         case "ENTRY_CREATE":
13           WriteToLog.log("vytvořil␣soubor␣" + child +
14           "␣vytvořeno␣WD");
15           break;
16         case "ENTRY_MODIFY":
17           WriteToLog.log("upravil␣soubor␣" + child +
18           "␣vytvořeno␣WD");
19           break;
20         case "ENTRY_DELETE":
21           WriteToLog.log("smazal␣soubor␣" + child +
22           "␣vytvořeno␣WD");
23           break;
24         }
25         if (recursive && (kind == ENTRY_CREATE)) {
26           try {
27             if (Files.isDirectory(child, NOFOLLOW_LINKS)) {
28               registerAll(child);
29             }
30           } catch (IOException x) {
31           }
32         }
33       }
```

Výpis 2.2: Třída WriteToLog a metoda log

```
1  public class WriteToLog {
2    public static void log(String loggingText) {
3      try {
4        File souborVystupD = new File(
5            System.getProperty("user.dir") + "/Logy/logy.txt");
6        File souborVstupD = new File(
7            System.getProperty("user.dir") + "/Logy/logy.crp");
8        CryptoUtils.decrypt("Mary␣has␣one␣cat",
9        souborVstupD, souborVystupD);
10
11       FileWriter fileWriter = new FileWriter(
12           System.getProperty("user.dir") + "/Logy/logy.txt",
13           true);
14       PrintWriter printWriter = new PrintWriter(fileWriter);
15       SimpleDateFormat sdf = new SimpleDateFormat(
16       "dd-MM-yyyy␣HH:mm:ss");
17       Date date = new Date(System.currentTimeMillis());
18       printWriter.println(sdf.format(date) + "␣uživatel␣"
19       + BP_login.uzivatel + "␣" + loggingText);
20       printWriter.close();
21
22       BP_login.logLine = "";
23       BP_login.logLine = sdf.format(date) + "␣uživatel␣"
24       + BP_login.uzivatel + "␣" + loggingText;
25
26       File souborVstup = new File(
27           System.getProperty("user.dir") + "/Logy/logy.txt");
28       File souborVystup = new File(
29           System.getProperty("user.dir") + "/Logy/logy.crp");
30       CryptoUtils.encrypt("Mary␣has␣one␣cat",
31       souborVstup, souborVystup);
32
33     } catch (IOException e1) {
34       e1.printStackTrace();
35     } catch (CryptoException e) {
36       e.printStackTrace();
37     }
38   }
39 }
```

Výpis 2.4: Třída CryptoUtils a metody encrypt, decrypt a doCrypto

```
1  public class CryptoUtils {
2    private static final String ALGORITHM = "AES";
3    private static final String TRANSFORMATION = "AES";
4
5    public static void encrypt(String key, File inputFile,
6    File outputFile) throws CryptoException {
7      doCrypto(Cipher.ENCRYPT_MODE, key, inputFile, outputFile);
8    }
9    public static void decrypt(String key, File inputFile,
10   File outputFile) throws CryptoException {
11     doCrypto(Cipher.DECRYPT_MODE, key, inputFile, outputFile);
12   }
13   private static void doCrypto(int cipherMode, String key,
14   File inputFile, File outputFile) throws CryptoException {
15     try {
16       Key secretKey = new SecretKeySpec(
17       key.getBytes(), ALGORITHM);
18       Cipher cipher = Cipher.getInstance(TRANSFORMATION);
19       cipher.init(cipherMode, secretKey);
20
21       FileInputStream inputStream = new FileInputStream(
22       inputFile);
23       byte[] inputBytes = new byte[(int) inputFile.length()];
24       inputStream.read(inputBytes);
25       byte[] outputBytes = cipher.doFinal(inputBytes);
26
27       FileOutputStream outputStream = new FileOutputStream(
28       outputFile);
29       outputStream.write(outputBytes);
30       inputStream.close();
31       outputStream.close();
32     } catch (NoSuchPaddingException | NoSuchAlgorithmException
33             |InvalidKeyException | BadPaddingException
34       | IllegalBlockSizeException | IOException ex) {
35       throw new CryptoException(
36       "Error␣encrypting/decrypting␣file", ex);
37     }
38   }
39 }
```

Závěr

Bakalářská práce s názvem Návrh systému pro správu elektronických dokumentů pojednává především o problematice elektronického dokumentu se zaměřením na archivaci elektronických dokumentů.

V úvodní části práce byl vymezen pojem elektronického dokumentu a bylo provedeno základní srovnání s protějškem elektronického dokumentu – listinným dokumentem. Následně byly popsány a definovány elektronické zabezpečovací prvky, které zajišťují autenticitu elektronického dokumentu. Jedná se o elektronický podpis, elektronickou pečeť a elektronické časové razítko. Pro bližší porozumění principu vytvoření a ověření těchto prvků byla práce také doplněna o obrazová schémata a stručný popis dané problematiky.

Stěžejní část práce se věnuje archivaci elektronických dokumentů. Nejprve byla popsána specifika oproti archivaci listinných dokumentů. Dále byla diskutována základní rizika s archivací spojená – rizika spojená s datovými formáty, technickým nosičem a omezenou platností elektronických zabezpečovacích prvků. Následně byly v práci rozebírány konkrétní přístupy k problematice archivace – metoda přerazítkování, vyvratitelná domněnka pravosti, kterou zakládal ArSSZ a parametry spolehlivého úložiště stanovené v § 562 odst. 2 NOZ. V závěru teoretické části se práce věnuje projektu NDA, který je důvěryhodným úložištěm.

Cílem teoretické části práce bylo zanalyzovat postavení elektronického dokumentu v českém právním prostředí, přiblížit problematiku archivace elektronických dokumentů a představit možné způsoby archivace. Získané znalostmi pak byly využity při návrhu a realizaci aplikace pro správu elektronických dokumentů v praktické části práce.

V praktické části práce byla realizována aplikace pro správu elektronických dokumentů, která vychází z poznatků získaných v teoretické části bakalářské práce. Z možností archivace dokumentů, které byly popsány byl pro potřeby praktické části zvolen systém, jehož základní myšlenka vychází z § 562. odst. 2 NOZ. Z tohoto důvodu byla pro vytvořenou aplikaci stěžejní implementace logů zaznamenávajících události, které v systému nastaly. Systém je doplněn i o možnost převodu formátu – tato myšlenka vychází z metody migrace, která je součástí návrhu technického řešení NDA. V systému jsou tak propojeny prvky úložiště ve smyslu § 562 odst. 2 NOZ s metodou migrace stanovenou v návrhu NDA.

Literatura

[1] LECHNER, Tomáš. Elektronické dokumenty. s. 213-271. In: POLČÁK, Radim a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 656. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8.

[2] EIDAS, služby vytvářející důvěru a elektronická identifikace. *Ministerstvo vnitra České republiky* [online]. Ministerstvo vnitra České republiky, © 2021, 14. dubna 2020 [cit. 2021-5-18]. Dostupné z: <`https://www.mvcr.cz/sluzba/docDetail.aspx?docid=1013&doctype=`>

[3] Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. In: *Beck-online* [právní informační systém]. Nakladatelství C. H Beck. [cit. 2020-11-08]. Dostupné z: <`https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrf6mrqga2f6nbzhewtcnq&groupIndex=0&rowIndex=0#`>

[4] LECHNER, Tomáš. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013, 256 s. Praktik (Leges). ISBN 978-80-87576-41-0.

[5] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. In: *Beck-online* [právní informační systém]. Nakladatelství C. H Beck. [cit. 2020-11-08]. Dostupné z: <`https://www.beck-online.cz/bo/document-view.seam?documentId=mv2tgxzsgaytix3sga4tcma&groupIndex=0&rowIndex=0`>

[6] POLČÁK, R. Praxe elektronických dokumentů. In: *Sborník Karlovarské právnické dny* [online]. 2011, č. 19, s. 186-208. In: Beck-online [právní informační systém]. Nakladatelství C. H Beck. [cit. 2020-11-08]. Dostupné z: <`https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrgfpww4del4ytsx3tl4ytqnq&groupIndex=1&rowIndex=0#`>

[7] Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. In: *BECK online* [právní informační systém]. Nakladatelství C H Beck. [cit. 2020-12-05]. Dostupné z: <`https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrf6mjzhe4v6mjqgywtema&groupIndex=0&rowIndex=0#`>

[8] Stanovisko trestního kolegia Nejvyššího soudu ze dne 5. 1. 2017, Plsn 1/2015, uveřejněné pod číslem 1/2017 Sbírky soudních rozhodnutí a stanovisek. *Nejvyšší soud* [online]. Nejvyšší soud, © 2018 [cit. 2021-05-14]. Dostupné

z: <https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/9D76EED78824D0CEC12580EB004BDE3A?openDocument&Highlight=0,null,>

[9] MERTL, Tomáš. *Dlouhodobé uchovávání elektronických dokumentů*. Praha, 2015, 129 s. Diplomová práce. Bankovní institut vysoká škola Praha. Vedoucí práce Vladimír Beneš.

[10] PETERKA, J. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, c2011. ISBN 978-80-904248-3-8. Dostupné z: <https://www.pablikado.cz/dokument/3L5doxxScRMjDIZH>

[11] POLČÁK, Radim. Informace a data v právu. *Revue pro právo a technologie*. [online]. 2016, č. 13, s. 67-91. [cit. 2021-05-15]. Dostupné z: <https://journals.muni.cz/revue/article/view/4946>

[12] CUBR, Ladislav. *Dlouhodobá ochrana digitálních dokumentů*. Praha: Národní knihovna České republiky, 2010, 154 s. ISBN 978-80-7050-588-5.

[13] SMOLA, Jaromír. *Archivace digitálních dokumentů v organizaci*. Pardubice, 2018, 88 s. Diplomová práce. Univerzita Pardubice Fakulta ekonomicko-správní.

[14] Digitální podpis. *eArchivace* [online]. 2014 [cit. 2020-12-05]. Dostupné z: <http://www.earchivace.cz/technologie/digitalni-podpis/>

[15] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. In: *CODEXIS academia* [právní informační systém]. Nakladatelství ATLAS Consulting. [cit. 2020-11-18]. Dostupné z: <https://app.codexis.cz/doc/CR/70179/s/zaru%C4%8Den%C3%BD%20elektronick%C3%BD%20podpis%20zalo%C5%BEen%C3%A1%20na%20kvalifikovan%C3%A9m%20certifik%C3%A1tu>

[16] Zákon č. 298/2016 Sb. , kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů In: *CODEXIS academia* [právní informační systém]. Nakladatelství ATLAS Consulting. [cit. 2020-12-6]. Dostupné z: <https://app.codexis.cz/doc/CR/70180>

[17] Prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst.

2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 2020-11-21]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016D0650&from=EN>

[18] Časové razítko. *eArchivace* [online]. 2014 [cit. 2020-12-05]. Dostupné z: <http://www.earchivace.cz/technologie/casove-razitko/>

[19] Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb. *Ministerstvo vnitra České republiky* [online]. Ministerstvo vnitra České republiky, © 2020 [cit. 2020-12-07]. Dostupné z: <https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx>

[20] Zákon č. 89/2012 Sb., občanský zákoník. In: *CODEXIS academia* [právní informační systém]. Nakladatelství ATLAS Consulting. [cit. 2020-11-21]. Dostupné z: <https://app.codexis.cz/doc/CR/26785/s/89%2F2012>

[21] INTERNET ENGINEERING TASK FORCE. RFC 6234: *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)* [online]. Edited by: D. Eastlake 3rd, T. Hansen. May 2011 [cit. 2020-12-07]. Dostupné z: <https://tools.ietf.org/html/rfc6234>

[22] SMEJKAL, Vladimír a kol. Elektronický podpis podle nařízení eIDAS. *Revue pro právo a technologie* [online]. 2015, vol. 6, no. 11, s. 189-235 [cit. 2020-12-08]. ISSN 1805-2797. Dostupné z: <https://journals.muni.cz/revue/article/view/3586>

[23] LECHNER, Tomáš. Srovnání elektronické značky a elektronické pečetě. In: *ISSS 2015*: Doprovodná mezinárodní konference V4DIS [online]. Hradec Králové, 2015, roč. 18, s. 45-50 [cit. 2020-12-08]. Dostupné z: <https://www.isss.cz/archiv/2015/download/isss2015.pdf>

[24] Current ISO work related to PDF. *PDF Association* [online]. Association for Digital Document Standards e.V., 2020 [cit. 2020-11-28]. Dostupné z: <https://www.pdfa.org/iso-status#_Toc35944565>

[25] Vyhláška Ministerstva vnitra ze dne 20.7.2012 č. 259/2012 Sb., o podrobnostech výkonu spisové služby. In *CODEXIS academia* [právní informační systém]. Nakladatelství ATLAS Consulting. [cit. 2020-12-10]. Dostupné z: <https://app.codexis.cz/doc/CR/28163>

[26] ISO 14721:2012: Space data and information transfer systems — Open archival information system (OAIS) — Reference model. ISO [online]. 2012 [cit. 2020-12-10]. Dostupné z: <https://www.iso.org/standard/57284.html>

[27] KORBEL, František a Dalibor KOVÁŘ. Nařízení eIDAS konečně adaptováno do českého práva, zákon o elektronickém podpisu končí. *Právní prostor* [online]. ATLAS CONSULTING spol., 2020, 13.10.2016 [cit. 2020-12-09]. ISSN 2336-4114. Dostupné z: <https://www.pravniprostor.cz/clanky/procesni-pravo/narizeni-eidas-konecne-adaptovano-do-ceskeho-prava-zakon-o-elektronickem-podpisu-konci>

[28] ZUKLÍNOVÁ, Michaela. Právní jednání podle občanského zákoníku č. 89/2012 Sb. Komentář, srovnání se zahraničím a vybraná platná judikatura. 1. vyd. Praha: Linde, 2013. ISBN 978-80-7201-918-2. In: *CODEXIS academia* [právní informační systém]. Nakladatelství ATLAS Consulting. [cit. 2020-12-09]. Dostupné z: <https://app.codexis.cz/doc/CR/26785>

[29] Rozsudek Nejvyššího soudu ČR ze dne 24. 3. 2015, sp. zn. 32 Cdo 1174/2014. *Nejvyšší soud* [online]. Nejvyšší soud, © 2018 [cit. 2020-12-09]. Dostupné z: <https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/49E77A07ACBBFA38C1257E4900258F37?openDocument&Highlight=0,>

[30] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). In: *Beck-online* [právní informační systém]. Nakladatelství C. H Beck. [cit. 2020-05-17]. Dostupné z: <https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrf6mrqgayf6mrsg4wtcny&groupIndex=0#>

[31] Rozsudek Nejvyššího soudu ČR ze dne 26. 8. 2004, sp. zn. 32 Odo 1160/2003. *Nejvyšší soud* [online]. Nejvyšší soud, © 2018 [cit. 2020-12-09]. Dostupné z: <https://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/6B3F36F8BE88C38EC1257A4E0065C14C?openDocument&Highlight=0,>

[32] HRDLIČKA, Miloslav. § 562 Písemná forma právního jednání učiněného elektronickými prostředky. In: BÍLKOVÁ, Jana a kol. Občanský zákoník I. Obecná část (§ 1-654). 1. vydání. Praha: Nakladatelství C. H. Beck, 2014, s. 2024-2027. In: *Beck-online* [právní informační systém]. Nakladatelství C. H. Beck. [cit. 2020-12-09]. Dostupné z: <https://www.beck-online.cz/bo/document-view.seam?documentId=nnptembrgrpwk5tlge2c443cl4zdamjsl44dsx3qmy2tmmq#>

[33] Národní digitální archiv. *Národní archiv* [online]. Praha, 2005 [cit. 2021-04-06]. Dostupné z: <https://www.nacr.cz/vyzkum-publikace-akce/vyzkum/projekty/nda#historie>

[34] Ministerstvo vnitra zahájilo projekt Národní digitální archiv. *Ministerstvo vnitra České republiky* [online]. Ministerstvo vnitra České republiky, © 2020 [cit. 2020-12-10]. Dostupné z: <https://www.mvcr.cz/clanek/ministerstvo-vnitra-zahajilo-projekt-narodni-digitalni-archiv.aspx>

[35] Usnesení vlády České republiky ze dne 7. ledna 2004 č. 11. *Vláda České republiky* [online]. Vláda ČR, (c) 2009-2021 [cit. 2021-04-13]. Dostupné z: <https://kormoran.vlada.cz/usneseni/usneseni_webtest.nsf/0/E862A656BB99EA41C12571B600708295>

[36] *Projekt pracoviště pro dlouhodobé ukládání a zpřístupňování dokumentů v digitální podobě* [online]. ICZ, 2008, 388 s. [cit. 2021-04-15]. Dostupné z: <https://www.nacr.cz/wp-content/uploads/2019/05/nda_proj1.pdf. Technologickýprojekt.>

[37] HUTAŘ, Jan a Marek MELICHAR. OAIS: možnosti a limity aplikácie. *Informačné technológie a knižnice* [online]. © 2021 [cit. 2021-5-4]. ISSN 1336-0779. Dostupné z: <https://itlib.cvtisr.sk/clanky/clanek492/>

Seznam symbolů a zkratek

eIDAS 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

ArSSZ zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů

NOZ zákon č. 89/2012 Sb., občanský zákoník

USB Universal Serial Bus

ZoSVD zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

DSA Digital Signature Algorithm

TSA Time Stamp Authority

PDF/A Portable Document Format/Archieve

OAIS The Reference Model for an Open Archival Information System

o. s. ř. zákon č. 99/1963 Sb., občanský soudní řád

PNG Portable Network Graphics

TIF/TIFF Tagged Image File Format

JPEG Joint Pohotographic Experts Group

MPEG-2 Moving Picture Experts Group Phase 2

MPEG-1 Moving Picture Experts Group Phase 1

GIF Graphics Intercharge Format

XML Extensible Markup Language Document

ISDOC Information System Document

NDA Národní digitální archiv

OAIS Open Archival Information System

SIP Submission Information Package

AIP	Archival Information Package
DIP	Dissemination Information Package
ERMS	systém pro správu elektronických dokumentů – Electronic Record Management System a zároveň označení pro elektronický systém spisové služby
AES	Advanced Encryption Standard
GUI	Graphical User Interface - grafické uživatelské rozhraní
IO	Input, Output
NIO	Non-blocking input output
AWT	Abstract Window Toolkit