VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

DŮVĚRYHODNÝ DLOUHODOBÝ ELEKTRONICKÝ ARCHIV

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

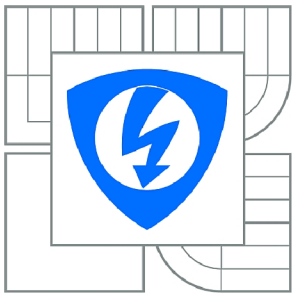
AUTOR PRÁCE
AUTHOR

ROMAN MRAVEC

BRNO 2014

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

DŮVĚRYHODNÝ DLOUHODOBÝ ELEKTRONICKÝ ARCHIV

TRUSTED LONG-TERM DIGITAL ARCHIVE

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

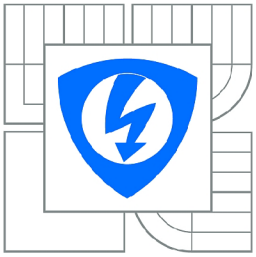
AUTOR PRÁCE — ROMAN MRAVEC

AUTHOR

VEDOUCÍ PRÁCE — Ing. VLASTIMIL ČLUPEK

SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Roman Mravec	***ID:***	146064
Ročník:	3	***Akademický rok:***	2013/2014

NÁZEV TÉMATU:

Důvěryhodný dlouhodobý elektronický archiv

POKYNY PRO VYPRACOVÁNÍ:

Formulujte požadavky kladené na důvěryhodný dlouhodobý elektronický archiv. Zaměřte se na způsoby zajištění dlouhodobé čitelnosti a důvěryhodnosti elektronických dokumentů a na autorizovaný a zabezpečený přístup k nim. Proveďte analýzu v současné době používaných řešení důvěryhodné dlouhodobé archivace. Vypracujte návrh řešení důvěryhodné dlouhodobé archivace elektronických dokumentů.

DOPORUČENÁ LITERATURA:

[1] MENEZES, Alfred J.; OORSCHOT, Paul C. van ; VANSTONE, Scott A. Handbook of Applied Cryptography. USA: CRC Press, 1996. 816 s. ISBN 0-8493-8523-7.

[2] PIPER, F.; MURPHY, S. Kryptografie. 1. vyd. v českém jazyce. Překlad Pavel Mondschein. Praha: Dokořán, 2006, 157 s. ISBN 80-736-3074-5.

[3] KUNSTOVÁ, R. Efektivní správa dokumentů: co nabízí Enterprise Content Management. 1. vyd. Praha: Grada Publishing, 2009, 204 s. ISBN 978-80-247-3257-2.

Termín zadání:	10.2.2014	***Termín odevzdání:***	4.6.2014

Vedoucí práce: Ing. Vlastimil Člupek
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

ABSTRAKT

Bakalárska práca sa zaoberá problematikou archivácie elektronických dokumentov a to najmä z dlhodobého hľadiska. Cieľom je zaistiť bezpečnosť a dôveryhodnosť elektronických dokumentov v elektronickom archíve. Zohľadňuje dlhodobú čitateľnosť, celistvosť obsahu, legálnu záväznosť a nepopierateľnosť elektronických dokumentov. Rieši problematiku ich uloženia do časovo stálych formátov. Obsahuje návrh riešenia dôveryhodného dlhodobého elektronického archívu na základe platných zákonov, noriem a osvedčených štandardov v tejto oblasti.

KĽÚČOVÉ SLOVÁ

Dôveryhodný dlhodobý elektronický archív, digitálny certifikát, elektronický podpis, funkcia hash, elektronická časová pečiatka, elektronický dokument, archivačné formáty, formát PDF, Referenčný model OAIS

ABSTRACT

The bachelor's thesis is focused on problematics of long-term trusted preservation. Security and trustworthiness of electronic documents is one of the main aim of this research. Provides means needed to keep and maintain data integrity, non-repudiation, long-term readibility and legally-binding of electronic documents. Solves time resistant formats for archive data files. Contains design of trusted long-term archive based on valid laws and standards in field of electronic preservation.

KEYWORDS

Long-term trusted preservation, digital certificate, electronic signature, Hash function, Timestamp, Electronic document, formats for long-term archiving, PDF format, OAIS reference model

MRAVEC, Roman *Důvěryhodný dlouhodobý elektronický archiv*: bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2014. 56 s. Vedúci práce bol Ing. Vlastimil Člupek

PREHLÁSENIE

Prehlasujem, že som svoju bakalársku prácu na tému „Důvěryhodný dlouhodobý elektronický archiv“ vypracoval samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/nebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o právu autorském, o právoch súvisejúcich s právom autorským a o zmeně niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhé, hlavy VI. diel 4 Trestného zákoníka č. 40/2009 Sb.

Brno ....

(podpis autora)

POĎAKOVANIE

Rád by som poďakoval za odborné vedenie, konzultácie, pomoc, trpezlivosť a podnetné návrhy vedúcemu svojej bakalárskej práce, pánovi Ing. Vlastimilovi Člupkovi.

Brno ....

(podpis autora)

OBSAH

Úvod **9**

1 Digitalizácia dokumentov **10**
1.1 Digitalizácia podnikového obsahu 10
1.2 Legislatívne aspekty 11
1.2.1 Legislatíva Českej republiky 12
1.3 Kryptografia a jej využitie 13
1.4 Digitálny certifikát 16
1.5 Funkcia hash 17

2 Elektronické dokumenty a ich zabezpečenie **18**
2.1 Elektronický podpis 19
2.1.1 Technické štandardy pre elektronické podpisy 22
2.2 Problematika zabezpečenia dokumentov 25
2.3 Elektronická časová pečiatka 26
2.4 Linkovaný hash 27

3 Archivácia elektronických dokumentov **29**
3.1 Archivačný objekt 29
3.2 Doba archivácie elektronických dokumentov 30
3.3 Dlhodobá čitateľnosť elektronických dokumentov 32
3.3.1 Migrácia elektronických dokumentov 32
3.3.2 Formát PDF 33
3.4 Referenčný model OAIS 35
3.5 Existujúce elektronické archívy 37
3.5.1 eKeeper 38

4 Návrh dôveryhodného dlhodobého elektronického archívu **40**
4.1 Architektúra elektronického archívu 41
4.1.1 Aplikačný server 42
4.1.2 Súborový server 44
4.1.3 Databázový server 44
4.2 Archivačný systém 45
4.2.1 Archivačný proces 46
4.2.2 Požiadavky na archivačný systém 48
4.3 Výhody navrhnutého riešenia 49

5 Záver **51**

Literatúra **53**

Zoznam symbolov, veličín a skratiek **56**

ZOZNAM OBRÁZKOV

1.1 Princíp šifrovania a dešifrovania správy v symetrickej kryptografii . . 14
1.2 Princíp šifrovania a dešifrovania správy v asymetrickej kryptografii . . 15
1.3 Vytvorenie odtlačku elektronického dokumentu 17
2.1 Proces vytvorenia a overenia elektronického podpisu 20
2.2 Porovnanie jednotlivých technických štandardov elektronických podpisov 23
2.3 Pracovný postup spracovania a ošetrenia PDF dokumentu elektronickým podpisom na základe PAdES štandardu 25
2.4 Proces vytvorenia časovej pečiatky 27
2.5 Pridelenie časovej pečiatky viacerým elektronickým dokumentom . . . 28
3.1 Uchovávacie atribúty v štruktúre archivačného objektu 30
3.2 Princíp modelu OAIS 35
3.3 Podrobná schéma referenčného modelu OAIS 36
4.1 Návrh dôveryhodného dlhodobého elektronického archívu 40
4.2 Činnosť aplikačného servera 43
4.3 Proces archivácie elektronického dokumentu v archivačnom systéme . 46

ÚVOD

Archivácia dokumentov predstavuje v dnešnej dobe pre každú organizáciu záťaž, na jednej strane v podobe pracného a častokrát neprehľadného ukladania v papierovej forme, a na strane druhej v správe tej elektronickej. Mnohé dôležité dokumenty ako napríklad zmluvy, doklady, faktúry, ale aj rôzny iný elektronický obsah je potrebné archivovať v horizonte desiatok rokov. Súčasný pokrok v oblasti informačných technológii a nárast používania elektronických dokumentov prináša nové možnosti v oblasti dlhodobej elektronickej archivácie. Legislatívne zmeny umožnili zefektívniť prácu s uchovávaním množstva dát, ktoré existujú v najrôznejších formách od štruktúrovaných dát uložených v relačných databázach cez digitálne a listinné dokumenty, e-maily, faxy, zvukové záznamy, obrázky, fotografie, výkresy, webové stránky až po znalostné databázy a archívy.

Úlohou tejto bakalárskej práce bude zhrnúť požiadavky a nevyhnutné štandardy pre elektronickú archiváciu dokumentov s prihliadnutím na legislatívne možnosti v Českej republike. Jednou z priorít, aj z dôvodu rozsiahlej problematiky v tejto oblasti, bude dôveryhodnosť archívu pre dlhodobé uloženie elektronických dokumentov založená na certifikačných prostriedkoch. Aby aj po dlhšom časovom období boli dokumenty čitateľné v podobe v akej boli uložené, budú zanalyzované a uvedené konkrétne technické možnosti a riešenia. Výstup práce bude vypracovaný vlastný návrh s popisom architektúry riešenia.

Pri elektronickej archivácii sa uvažuje o uložení elektronických dát, preto sa prvá kapitola venuje digitalizácii dokumentov, možnému použitiu v súkromnej a verejnej sfére a najdôležitejším princípom súvisiacich s ich zabezpečením. Druhá kapitola definuje elektronický dokument a eletronický podpis. Zároveň uvádza mechanizmy ako časová pečiatka alebo linkovaný hash, ktoré sa využívajú v elektronickej archivácii práve v súvislosti s elektronickými podpismi. V tretej kapitole sú formulované požiadavky kladené na samotnú archiváciu elektronických dokumentov, pričom bude kladený dôraz najmä na dôveryhodnosť a dlhodobú čitateľnosť. Súčasťou tejto kapitole je aj základný model, ktorý predstavuje základný pilier každého elektronického archívu a takisto analýza najvýznamnejších existujúcich riešení používaných v Českej republike ale aj vo svete. Vychádzajúc z poznatkov z predchádzajúcich kapitol a s prihliadnutím na všetky legislatívne aspekty a požiadavky spojené s elektronickou archiváciou, je v poslednej kapitole predstavený návrh dôveryhodného dlhodobého elektronického archívu . Nakoniec sú zhrnuté hlavné charakteristiky a výhody navrhnutého riešenia.

1 DIGITALIZÁCIA DOKUMENTOV

Jedným z kľúčových faktorov pre vznik elektronických archívov je rozvoj technológií v oblasti digitalizácie dokumentov. Práca s množstvom papierových dokumentov so sebou prináša viacero obtiažností. Zákon v niektorých prípadoch prikazuje ako majú organizácie zaobchádzať s evidenciou alebo manipulovať s listinnými dokumentmi. Úrady a firmy by sa mali držať pri úkonoch ako skartácia alebo archivácia určitých pravidiel, vo väčšine prípadov je to však interná záležitosť tej ktorej organizácie. Digitalizácia dát predstavuje príležitosť ako využiť informačno-komunikačné prostriedky pre ulahčenie fungovania organizácií. Napríklad v dnešnej dobe znamená elektronická archivácia dokumentov nielen pre organizácie, ale aj štátnu správu, obrovskú úsporu nákladov, času ale hlavne priestorov. Jeden megabajt diskového priestoru pojme v textovom formáte viac ako 300 strán textu[17]. Ďalšiou užitočnou vlastnosťou elektronických archívov je vyhľadávanie uložených elektronických dokumentov pomocou vyhľadávacích metadát – podľa autora, organizácie, kľúčových slov atď. Podstatné môže byť tiež, na rozdiel od papierových dokumentov, že k tým elekronickým môže naraz v reálnom čase pristupovať viacero osôb. Prácu s každým dokumentom navyše riadia presne dané súbory oprávnení, ktoré môžu určiť kto smie daný dokument upravovať, kto doňho môže iba nahliadnuť alebo kto vôbec nemá zistiť, že dokument existuje.[12] Nespornou výhodou oproti klasickým dátam uloženým na papieri je aj nepodliehanie poveternostným vplyvom a živelným pohromám. Nové služby súvisiace s digitalizáciou dát, ktoré postupne vznikli približne od začiatku nového milénia, jednoznačne nadviazali na pokrok v jednolivých moderných technológiach. Ich využívanie ešte stále nie je rozšírene vo veľkej miere, no ich potenciál ich predurčuje k ďalšiemu vývoju. Služby využívajúce digitalizované dáta majú svoje použitie aj v súkromnej aj vo verejnej sfére.

1.1 Digitalizácia podnikového obsahu

Správa podnikového obsahu ide ruka v ruke s digitalizáciou papierových dokumentov. Európska únia preto vydala *smernicu 1999/93/EC*, ktorá chce využiť elektronicky podpísané dokumenty v oblastiach ako sú štátna správa (E-government) alebo elektronické obchodovanie (E-business). V podstate sa jedná o krátkodobú archiváciu elektronických dokumentov.

Dátová správa

Dátová správa je moderný spôsob komunikácie, ktorá má za úlohu zjednodušiť obchodný styk. Jedná sa o elektronickú obdobu klasickej doporučenej zásielky. Podľa

zákona 227/2000 Sb. sa jedná o elektronické dáta, ktoré je možné prenášať prostriedkami pre elektronickú komunikáciu a uchovávať na záznamových médiach používaných pri spracovaní a prenose dát elektronickou formou.

E-government

E-government je vlastne elektronickou formou výkonu verejnej správy s využitím informačno-komunikačných technológií v procesoch verejnej správy. Pre lepšie pochopenie je možné E-government voľne preložiť ako elektronickú podateľnu, teda slúži občanom ale aj samotným orgánom pre lepšiu a efektívnejšiu spoluprácu prostredníctvom internetu.

E-government využíva elektronický podpis ako náhradu ručne písaného podpisu v styku orgánov štátnej moci a samosprávy s občanmi. Takisto má využitie v zájomnej komunikácii medzi štátnou správou a samosprávou. V Českej republike je použitie elektronického podpisu v tejto oblasti definované *vyhláškou Ministerstva informatiky č. 496/2004 Sb.* Pre štátnu správu je rovnako dôležitá aj archivácia elektronických dokumentov, obzvlášť v krátkodobom až strednodobom časovom horizonte.

E-business

Azda najväčší prínos sa očakáva v súkromnej sfére, kde elektronický podpis slúži k podpore a zefektívneniu obchodu. Európska únia vydala *smernicu 2000/31/ES*, ktorej cieľom je prispieť k riadnemu fungovaniu vnútorného trhu medzi členskými krajinami. Množstvo obchodov v súčasnosti prebieha cez internet, pričom sa využívajú technológie ako elektronický prevod finančných prostriedkov, internetový marketing alebo elektronické zjednávanie obchodných zmlúv. Myšlienku „elektronického obchodovania“ podporil rozvoj v oblasti elektronických podpisov, bez ktorého sa obchodovanie na internete nemôže zaobísť.[9]

1.2 Legislatívne aspekty

Základný pilier pre vývoj technológií v oblasti elektronického podpisu, elektronickej archivácie dokumentov a s nimi súvisiacej digitalizácie papierových dokumentov bolo prijatie už spomenutej *smernice Európskej únie 1999/93/EC.* Smernicu tvoria štyri základné body[14]:

- dobrovoľný akreditačný systém – každý poskytovateľ certifikačných služieb získa po splnení legislatívnych podmienok akreditáciu,

- každý členský štát uplatňuje svoje vnútroštátne právne predpisy, prijaté na základe tejto smernice, pre poskytovateľov certifikačných služieb,
- členské štáty dbajú na plnenie právnych požiadaviek na elektronický podpis a takisto umožňujú použiť elektronický podpis pri súdnom konaní,
- členské štáty dbajú na neodopierateľnosť právnych účinkov elektronických podpisov, aj keď majú elektornickú podobu alebo sa nezakladajú na kvalifikovanom certifikáte.

Z týcho bodov je možné rozpoznať snahu Eúrópskej únie o rozšírenie používania elektronických podpisov a s nimi súvisiacích technológií vo verejnej, ale aj v komerčnej sfére a to vo všetkých jej členských štátoch. Základným krokom pre vznik nových zákonov bolo aj špecifikovanie výrazu dokument (kapitola 2), vďaka čomu je možné akceptovať aj elektronickú formu dokumentov. Pri každom elektronickom dokumente vzniká problém s uchovateľnosťou digitalizovaných dát a s pravosťou zaznamenaných dát, preto zákon rieši túto problematiku nasledovne[9]:

- typy dokumentov, ktoré sú zákonom určené sa musia archivovať v určitom časovom meradle s možnosťou elektronickej archivácie,
- pri elektronickej forme archivácie je potrebné zaručiť nemennosť dokumentu po celú dobu archivácie a zaistiť čitateľnosť obsahu.

Z pohľadu elektronickej archivácie dokumentov má zavedenie legislatívnych opatrení svoje opodstatnenie a k ich vzniku viedli hlavne dva dôvody:

- v rámci rozvoja v oblasti elektronickej archivácie sa muselo pristúpiť k ochrane používateľov a ich dát,
- Európska únia určila štandardy, legislatívne požiadavky a návrhy zákonov pre členské štáty s cieľom ochrany osobných údajov, podporiť a usmerniť elektronickú komunikáciu a uchovávanie dátových záznamov.

Prínosom prijatých právnych predpisov je hlavne legislatívna opora pre zriaďovateľov elektronických archívov, ale takisto aj pre ich užívateľov. Dokumenty uložené v elektronickom archíve by mali mať rovnaké právne účinky ako v listinnom archíve[1]. Zároveň sa určili akési hranice, ktoré by mali jednotlivé technické riešenia elektronických archívov dodržiavať a rešpektovať.

1.2.1 Legislatíva Českej republiky

Smernica Európskej únie 1999/93/EC sa stala predlohou aj pre jej členské štáty, ktoré postupne prijali svoje vlastné zákony. V Českej republike na jej základe vznikol

[1] Ak budú splnené všetky požiadavky spojené s elektronickou archiváciou. Venujú sa im nasledujúce kapitoly.

zákon č. 227/2000 Sb., ktorý bol neskôr viackrát novelizovaný. Pre elektronickú komunikáciu a elektronickú archiváciu elektronicky podpísaných dokumentov sú podstatné tieto zákony a vyhlášky Českej republiky[4][6]:

- *zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů*, v znení neskorších predpisov,
- *zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů*, v znení neskorších predpisov,
- *zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů*, v znení neskorších predpisov,
- *zákon č. 500/2004 Sb., správní řád*, v znení neskorších predpisov,
- *vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů*,
- *vyhláška č. 194/2009 Sb., o užívání a provozování informačního systému datových schránek*,
- *vyhláška č. 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka*,
- *vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby.*

Vďaka uvedeným zákonom a vyhláškam je dnes už aj v Českej republike právne záväzné používať elektronické podpisy vo vzťahu s elektronickými dokumentmi a zároveň vznikol priestor pre ich elektronickú archiváciu. Nasledujúce časti kapitoly sa venujú zabezpečeniu elektronických dát tak, aby boli splnené spomenuté právne úpravy.

1.3 Kryptografia a jej využitie

Kryptografia je vedný odbor, ktorý sa zaoberá vytváraním šifrovacích systémov a ich implementáciou. Hlavným cieľom šifrovacieho systému je utajiť správu, aby sa jej obsah stal nečitateľným pre človeka.[16] Tak ako sa pri poštovej korešpondencii používa obálka aby sa nepovolaná osoba nedostala k obsahu správy, rovnako môžeme považovať kryptografiu za pomyselnú „obálku“ v elektronickej komunikácii. Najmä v elektronickej archivácii je potrebné zaistiť bezpečnosť archivovaných dát a poskytnúť vlastníkovi archívu dôveryhodné úložisko pre svoje elektronické dokumenty.

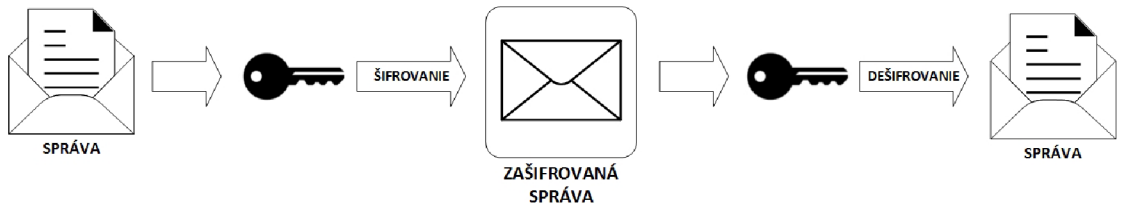
Súčasné kryptografické algoritmy, ktoré využívajú šifrovacie kľúče pre poskytnutie bezpečnosti elektronickýcm dokumentom, sa stávajú čoraz viac a viac zraniteľnými. Výpočtový výkon moderných počítačov rapídne stúpa, čo predstavuje

riziko „prelomenia“ šifrovacích algoritmov a prístup k samotným dátam. Napríklad elektronické podpisy predstavujú zašifrované dáta podpísané súkromným kľúčom s určitou bitovou dĺžkou a pri nedostatočnom zabezpečení sú potencionálne ohrozené – preto nemôžu ponúkať adekvátnu dlhodobú bezpečnosť. Hlavným problémom je však čas. Aby bola zabezpečená dostatočná úroveň bezpečnosti, šifrovacie algoritmy sú nahradené novými každých pár rokov.[21]

Modernú kryptografiu rozdeľujeme podľa šifrovacích systémov na dve skupiny – **symetrickú** a **asymetrickú**.

Symetrická kryptografia

Symetrická kryptografia využíva tzv. symetrické šifry, ktoré fungujú na princípe utajenia správy medzi komunikujúcimi stranami prostredníctvom tajného šifrovacieho kľúča. Na tomto kľúči sa musia obe strany vopred spoločne dohodnúť (obr. 1.1).



Obr. 1.1: Princíp šifrovania a dešifrovania správy v symetrickej kryptografii

Komunikácia pomocou symetrickej kryptografie prebieha na veľmi jednoduchom princípe. Jedna strana správu zašifruje pomocou dohodnotého (šifrovacieho) kľúča, a následne použije druhá strana po obdržaní správy na dešifrovanie ten istý (šifrovací) kľúč.

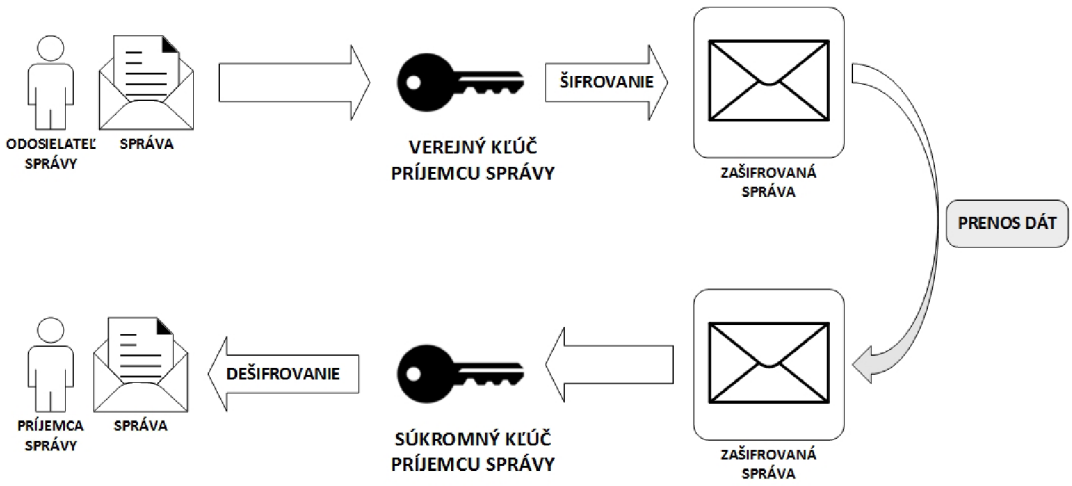
Kedže pri symetrickej kryptografii reálne hrozí, že sa k šifrovaciemu kľúču dostane tretia osoba, využívajú sa techniky ako predzdielanie šifrovacieho kľúča, jeho doručenie príjemcovi správy kuriérom alebo môže byť pre jeho bezpečné stanovanie použitý asymetrický protokol Diffie-Hellman. V elektronickej komunikácii sa využíva zväčša v kombinácii s asymetrickou kryptografiou. Pomocou asymetrickej kryptografie je dohodnutý kľúč pre symetrickú šifru, a potom je samotná komunikácia šifrovaná pomocou symetrickej kryptografie. Výhodou tohto riešenia je rýchlosť šifrovania – rýchlosť šifrovania pomocou asymetrickej kryptografie je omnoho menšia ako pomocou symetrickej (symetrická kryptografia používa kratšie kľúče).

Asymetrická kryptografia

Asymetrická kryptografia využíva tzv. asymetrické šifry, ktoré narozdiel od symetrických šifier nevyužívajú jeden šifrovací kľúč, ale vždy jeden pár šifrovacích kľúčov – jeden sa používa pre šifrovací algoritmus a druhý pre dešifrovací algoritmus. Keďže napríklad pri elektornickom podpise dochádza pri niektorých šifrách k zámene šifrovacích a dešifrovacích operácií, nehovoríme o šifrovaciom a dešifrovaciom kľúči, ale o verejnom a súkromnom kľúči.

Komunikácia pomocou asymetrickej kryptografie prebieha nasledovne (obr. 1.2):

1. príjemca správy si vygeneruje dvojicu kľúčov – verejný a súkromný kľúč,
2. príjemca správy si bezpečne uloží svoj súkromný kľúč (napr. na zabezpečený disk, do dôveryhodného úložiska kľúčov atď. . .),
3. príjemca správy odošle svoj verejný kľúč odosielateľovi (kľudne aj prostredníctvom tretej osoby),
4. odosielateľ správy zašifruje správu prijatým verejným kľúčom príjemcu správy,
5. príjemca správy dešifruje prijtú šifrovanú správu svojím súkromným kľúčom a získa pôvodnú správu.



Obr. 1.2: Princíp šifrovania a dešifrovania správy v asymetrickej kryptografii

V asymetrickej kryptografii sa najčastejšie používa šifrovací algoritmus RSA. Dĺžka šifrovacích kľúčov pre algoritmus RSA sa považuje za bezpečnú, ak obsahuje aspoň 2048 bitov. Častokrát sa však používajú kľúče s dĺžkou aj 4096 bitov a viac (v závislosti od požadovanej bezpečnosti).[9]

Výhodou šifrovania na báze asymetrických algoritmov je, že útočník síce môže zistiť verejný kľúč, ale správu nedokáže dešifrovať bez súkromného kľúča. Pre väčšiu výpočetnú náročnosť šifrovacích algoritmov založených na asymetrickej kryptografii sa kombinuje už so spomenutou symetrickou kryptografiou.

1.4 Digitálny certifikát

Digitálny certifikát je podpísaný dátový súbor obsahujúci špecifický a jedinečný identifikátor, spojený s informáciami o jeho vlastníkový, ktorý nazývame verejný kľúč. Aby bol digitálny certifikát dostatočne dôveryhodný inštrument, kedže sa využíva v kombinácii s elektronickým podpisom (venuje sa mu kapitola 2.1), je potrebné aby ho vydával nezávislý subjekt. Takýmto subjektom je poskytovateľ certifikačných služieb – **certifikačná autorita**. Vydaním certifikátu certifikačná autorita takisto potvrdzuje, že subjekt, ktorému bol certifikát vydaný naozaj vlastní súkromný a verejný kľúč – poskytuje autenticitu podpisujúcej strany. Nakoľko digitálny certifikát predstavuje dátový súbor, je potrebné určité zabezpečenie proti jeho sfalšovaniu. Preto certifikačná autorita podpisuje certifikát svojím súkromným kľúčom a pripája ho k certifikátu – to znamená, že k nemu pripája svoj vlastný certifikát. Z toho vyplýva, že certifikát certifikačnej autority musí byť pre používateľa k dispozícii a voľne dostupný. Každý certifikát je konečný, teda má určený svoj dátum expirácie. Súvisí to s obmenou kryptografických algoritmov a teda aj s generovaním nových šifrovacích kľúčov. Po vypršaní platnosti certifikátu musí byť nahradený novým. Všeobecne sa pohybuje životnosť certifikátov okolo piatich rokov.[21] Ako dôsledok je každý elektronický podpis po vypršaní považovaný za neplatný. Primárnou snahou tohto bezpečnostného opatrenia je vytvoriť legálne platný ekvivalent klasickým ručne písaným podpisom.

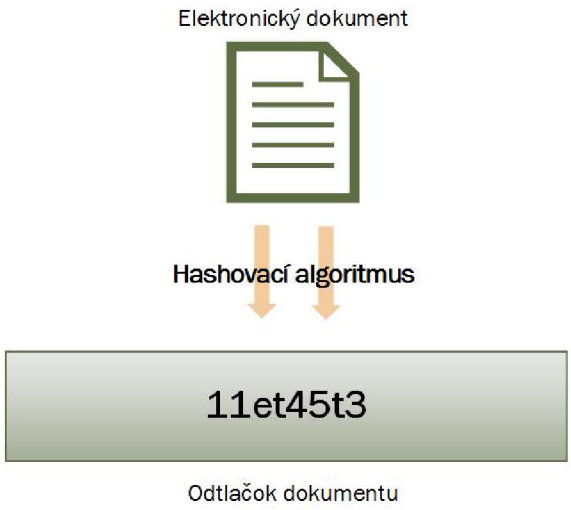
Pre digitálne certifikáty sa používa medzinárodná norma X.509, ktorá jednoznačne popisuje štruktúru certifikátu. Každý certifikát musí obsahovať nasledujúce údaje[8]:

- sériové číslo – musí byť vždy unikátne,
- dátum počiatku a konca platnosti certifikátu (doba platnosti certifikátu obvykle závisí na matematickej náročnosti určitých algoritmov verejného kľúča, ktorý je k certifikátu vydaný),
- identifikačné údaje subjektu, ktorému je certifikát vydaný,
- verejný kľúč a typ algoritmu, ktorý je pri podpisovaní používaný,
- identifikačné údaje poskytovteľa certifikačnej autority.

Kvalifikovaný certifikát je digitálny certifikát vyššieho stupňa, ktorý spĺňa náležitosti stanovené *zákonom č. 440/2004 Sb., §12* a bol vydaný poskytovateľom certifikačných služieb po overení identity žiadateľa o tento certifikát. Jeho využitie je spojené s kvalifikovaným elektronickým podpisom.

1.5 Funkcia hash

Funkcia hash je jednocestná funkcia, ktorá z ľubovoľne dlhého textu vytvorí krátky reťazec konštantnej dĺžky, tzv. **odtlačok dokumentu** (obr. 1.3). Jednocestnú funkciu predstavujú algoritmy, ktoré nie sú výpočetne náročné, ale na druhej strane je veľmi obtiažné z výsledného reťazca získať pôvodný text. Najčastejšie používaný algoritmus je v súčasnosti SHA-2, s odtlačkom dlhým 64 B. V súčasnosti už existuje najnovšia verzia šifrovacieho štandardu s označením SHA-3, ktorá pracuje na iných matematických princípoch ako SHA-2, takže v prípade prolomenia SHA-2 môže byť nahradená novším štandardom. Jedná sa o veľmi efektívny nástroj ako utajiť obsah správy. Kedže výpočetná náročnosť pri súčasnej technickej vyspelosti informačných technológii by na prelomenie odtlačku vyžadovala aj niekoľko dní, je útok na obsah dokumentu touto cestou dosť nepravdepodobný (zároveň doba odbavenia časovou autoritou je omnoho kratšia).



Obr. 1.3: Vytvorenie odtlačku elektronického dokumentu

Funkcia hash má v elektronickej komunikácii využitie ako dôkazový prostriedok integrity dokumentu v elektronickej podobe. Napríklad pri elektronickej archivácii je potrebné aby autorita časových pečiatok pridelovala dôveryhodný čas iba k odtlačku dokumentu, prípadne overila jeho platnosť. K tomu aby k elektronickému podpisu pripojila časovú pečiatku musí autorita v určitej forme prijať dokument, avšak s tou podmienkou, že sa nemôže dostať do styku s jeho obsahom . Práve k tomu slúži odtlačok dokumentu, čím je jednak zaručené súkromie obsahu dokumentu, ale aj jeho nemennosť a celistvosť.

2 ELEKTRONICKÉ DOKUMENTY A ICH ZABEZPEČENIE

Každý elektronický archív je určený pre dlhodobé uchovanie dokumentov v elektronickej podobe – tzv. **elektronických dokumentov**. Z technického hľadiska sa jedná o elektronické dáta uložené vo formáte digitálneho súboru. Jeho obsah môže tvoriť text, ale takisto aj multimédia (audio, video, animácie, grafika...) a ďalšie informačné zdroje. Takýto digitalizovaný dokument môže byť distribuovaný napríklad ako príloha e-mailu, používateľ si ju môže stiahnuť z niektorého servera, čítať alebo ďalej spravovať.

Napriek tomu, že sa bez informačných technológii dnes žiadna organizácia nezaobíde, je využívanie elektronických dokumentov stále len vo svojich začiatkoch (pre svoj virtuálny obsah prevláda najmä nedôvera v ich zabezpečenie). Postavenie elektronického dokumentu voči klasickému listinnému dokumentu v súčasnosti v Českej republike „zrovnoprávňuje“ zákon prijatý na základe smerníc Európskej únie. Podľa *zákona č. 499/2004 Sb., §2 písm. e), o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů*, sa dokumentom rozumie každá písomná, obrazová, zvuková alebo iná zaznamenaná informácia, či už v podobe analógovej alebo digitálnej, ktorá bola vytvorená pôvodcom alebo bola pôvodcovi doručená[6]. Z tohto zákona jasne badať snahu o vytvorenie právnej záväznosti elektronického dokumentu, čo jednoznačne pomôže k jeho širšiemu využívaniu aj v prípade, keď dokument obsahuje citlivejší obsah (napríklad obchodné zmluvy, patenty, osobné údaje...).

Špecifikom elektronického podpisu oproti listinnému je, že nie je nijakým spôsobom zviazaný s nosičom, na ktorom bol vytvorený a preto v jeho prípade neexistuje žiaden originál.[15] Na druhej strane však existuje možnosť vytvoriť nekonečne mnoho rovnakých kópii. Pri vytváraní elektronických dokumentov existujú dve možnosti – buď vznike priamo v elektronickej podobe (napríklad text vytvorený na počítači) alebo bude do elektronickej verzie prevedený z analógovej, teda digitalizáciou (napríklad zoskenovaním listinného dokumentu). Konverzia dokumentov môže prebiehať aj opačne – vytvorením listinnej podoby z elektronickej. Ďalším typom konverzie je aj zmena formátu elektronických dokumentov, ktorá má zásadný vplyv na ich archiváciu (archivačným formátom sa venuje kapitola 3.3.1). Veľmi dôležitým prvkom pri zmene formátu z pohľadu dôveryhodnej archivácii elektronických dokumentov je autorizovaná konverzia. Vykonávajú ju orgány verejnej moci a vďaka nej má konvertovaný dokument rovnaké právne účinky ako dokument, z ktorej vznikol.

Elektronické dokumenty sú charateristické svojimi atribútmi[15]:

- **informačná hodnota** – dokument je nositeľom informácie, ktorá má svoju

hodnotu,

- **stálosť** – dokument je stály a nemenný,
- **jazyk** – obsah dokumentu je zvyčajne vyjarený v určitom jazyku (nie je to však podmienka, obsah dokumentu môže byť vyjadrený aj v symbolike),
- **štruktúrovateľnosť** – dokument má svoju vnútornú štruktúru, s prihliadnutím na jeho účel,
- **celistvosť** – s dokumentom sa zaobchádza ako s jednoliatym celkom a môže byť rozdelený len pri určitých procesoch,
- **funkčnosť** – dôležitý atribút ovplyvňujúci množstvo vlastností dokumentu.

Z hľadiska obsahu elektronických dokumentov je potrebné zaistiť tri hlavné požiadavky – **integrita obsahu**, **dlhodobá čitateľnosť** a **nepopierateľnosť platnosti**. Ich cieľom je použiť elektronický dokument ako nespochybniteľný prostriedok (či už pri dôkladnej kontrole, audite, súdnom nariadení...) kedykoľvek v budúcnosti. Z toho vyplývajú nasledujúce požiadavky:

- elektronický dokument musí byť preukazateľný aj mimo elektronický archív,
- musí byť možné predĺžiť právnu účinnosť elektronického dokumentu a to na neobmedzenú dobu,
- dokument musí byť po dobu právnej účinnosti čitateľný.

Dokument v elektronickom formáte redukuje náklady na použitie papiera ako prostriedku pre jeho zobrazenie, ďalej náklady na umiestnenie (uskladnenie) a distribúciu. Odstraňuje limity na rozsah textu, prípadne grafickú úpravu a jednoznačne zefektivňuje a zrýchluje prácu.

Nasledujúce časti kapitoly súvisia so zabezpečením elektronických dokumentov.

2.1 Elektronický podpis

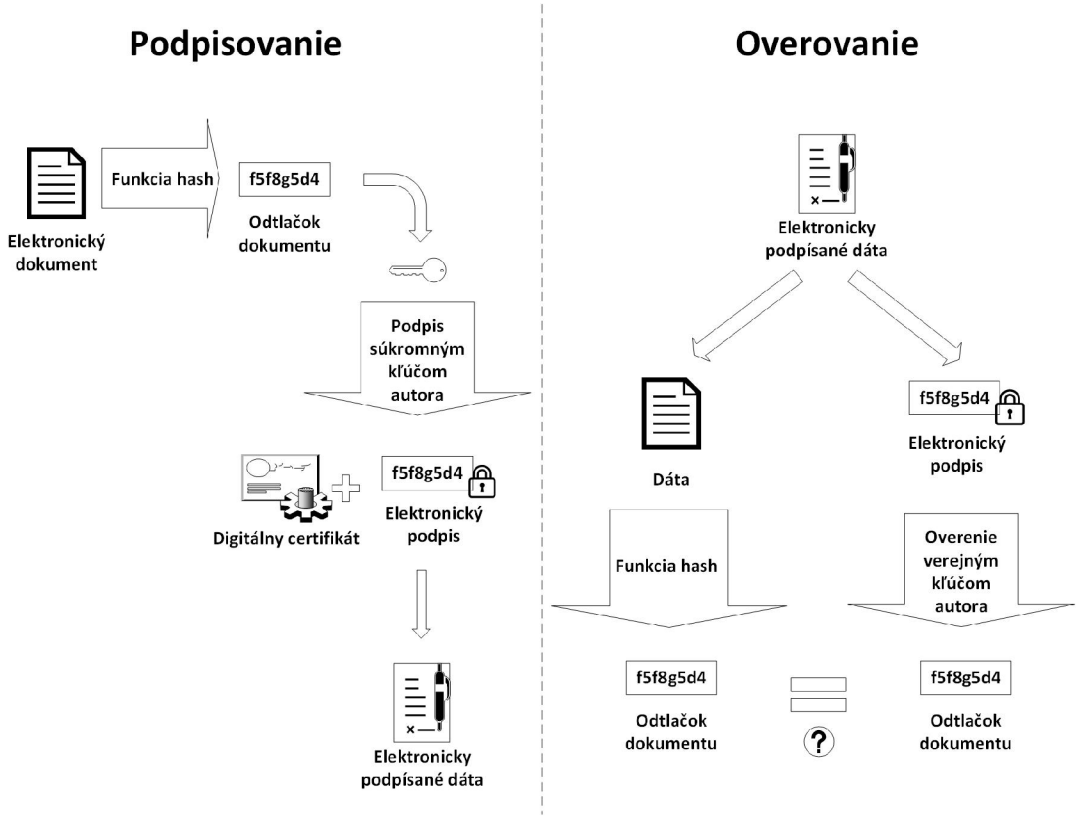
Elektronický podpis[1] predstavuje možnú súčasť elektronických dokumentov, ktorá slúži na jednoznačné overenie a preukázanie spojitosti medzi podpisujúcou osobou a daným dokumentom, presne ako pri klasickom „ručne písanom“ podpise. V podstate sa jedná o bezpapierový spôsob podpisu dokumentu použitím unikátného poverenia súvisiaceho s konkrétnou osobou, ktorá je logický spojená alebo je v určitom vzťahu s dokumentom.

Elektronický podpis je v Českej republike definovaný už spomenutým prijatým zákonom z roku 2000 – *zákon č. 227/2000 Sb.*, ako *údaje v elektronické podobě, které*

[1] Mnohokrát dochádza aj v odbornej literatúre k používaniu pojmu digitálny podpis, pričom sa nie vždy jedná o synonymá. V tejto bakalárskej práci bude použité označenie elektronický podpis v zmysle zjednotenia celej problematiky.

jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.[5] Z daného zákona vyplýva, že elektronický podpis má z legálneho hľadiska rovnakú funkciu a úlohu ako listinný podpis. Zároveň určuje, že musí byť k elektronickému dokumentu pripojený ako jeho súčasť (napr. formát PDF) alebo s ním aspoň logický spojený. Závisí to najmä od použitého technického štandardu elektronického podpisu (kapitola 2.1.1).

Elektronický podpis slúži k overeniu pôvodu dokumentu[2]. Ako už bolo spomenuté v predchádzajúcej kapitole, digitálny certifikát je založený na asymetrickej kryptografii (dáta obsiahnuté v ňom[3] sú podpísané súkromým kľúčom) a vydáva ho certifikovaná autorita. V súčasnosti sa používajú certifikáty pre elektronické podpisy založené na norme X.509.



Obr. 2.1: Proces vytvorenia a overenia elektronického podpisu

[2]Autenticita podpisujúcej strany sa zaisťuje pomocou digitálneho certifikátu, ktorý obsahuje verejný kľúč matematicky spojený so súkromným kľúčom a pomocou ktorého bol odtlačok dokumentu podpísaný.

[3]Digitálny certifikát obsahuje informácie ako identu vlastníka, použitý verejný kľúč atď.

Elektronický podpis sa vytvára pomocou nasledovného procesu zloženého z dvoch krokov (obr. 2.1):

1. vytvorí sa odtlačok z dokumentu pomocou funkcie hash,
2. výsledný odtlačok sa podpíše súkromným kľúčom podpisujúcej strany.

Opačný proces je potom verifikácia digitálneho podpisu. Ten sa skladá z týchto troch krokov:

1. príjemca správy spočíta odtlačok z prijatej správy,
2. príjemca správy overí prijatý digitálny podpis verejným kľúčom odosielateľa,
3. príjemca porovná výsledok získaný z kroku 1 s výsledkom získaným z kroku 2; ak sú výsledky zhodné tak vyplýva, že odosielateľ je vlastníkom súkromného kľúča a navyše, že správa nebola počas prenosu pozmenená.

Je dôležité, aby si vlastníci svoje súkromné kľúče strážili, pretože na ich základe sa preukazuje autenticita elektronického podpisu.[9]

Zámerom elektronického podpisu je vytvoriť „virtuálnu“ alternatívu pre pripojenie identity podpisujúcej strany k samotnému dokumentu. Vďaka prijatým zákonom v členských štátoch Európskej únie sú v súčasnosti organizácie omnoho viac flexibilnejšie a agilnejšie pri neustále sa rozvíjajúcom podnikateľskom prostredí a s pokrokom v informačno-komunikačných technológiach. Tak ako sa vo verejnej a súkromnej sfére zistili obrovské úspory elektronizáciou papierových dokumentov, elektronický podpis sa môže stať ešte oveľa atraktívnejším aj vo vzťahu so zabezpečením elektronických dokumentov. Dnes už napríklad štáty Európskej únie bežne vydávajú svojim občanom občianske preukazy s elektronickým čipom, ktorý je jednoznačne a jedinečne spojený s ich osobou, a tak je širšie využitie elektronického podpisu len otázkou času.

Existujú dva vyššie stupne zabezpečenia elektronického podpisu – **zaručený** elektronický podpis (z anglického „Advanced Electronic Signature“) a **kvalifikovaný** elektronický podpis (z anglického „Qualified Electronic Signature“). Výklad týchto termínov upravuje v Českej republike *zákon o elektronickom podpise 227/2000 Sb.*, ktorý bol neskôr viackrát novelizovaný.

Zaručený elektronický podpis

Zaručený elektronický podpis (často používaná anglická skratka AdES) je elektronický podpis, ktorý vyžaduje nasledujúce požiadavky[1]:

- je jednoznačne spojený s podpisujúcou stranou,
- je schopný identifikovať podpisujúcu stranu,
- je vytvorený spôsobom, nad ktorým podpisujúca strana dokáže udržiavať výhradnú kontrolu,

- je spojený s dátami, ku ktorým sa vzťahuje takým spôsobom, že je možné zistiť všetky ďalšie zmeny dát.

Zaručený elektronický podpis teda zaručuje celistvosť obsahu elektronického dokumentu. Taktiež je zaručená nepopierateľnosť pripojenia elektronického podpisu jeho vlastníkom (pripája svoje osobné údaje). To však neznamená, že vlastník podpisu je skutočne aj tým, za koho sa vydáva. Pri zaručenom elektronickom podpise sa nekontroluje identita vlastníka elektronického podpisu, preto hrozí riziko sfalšovania osobných údajov. Kvôli tejto hrozbe vznikol kvalifikovaný elektronický podpis.

Kvalifikovný elektronický podpis

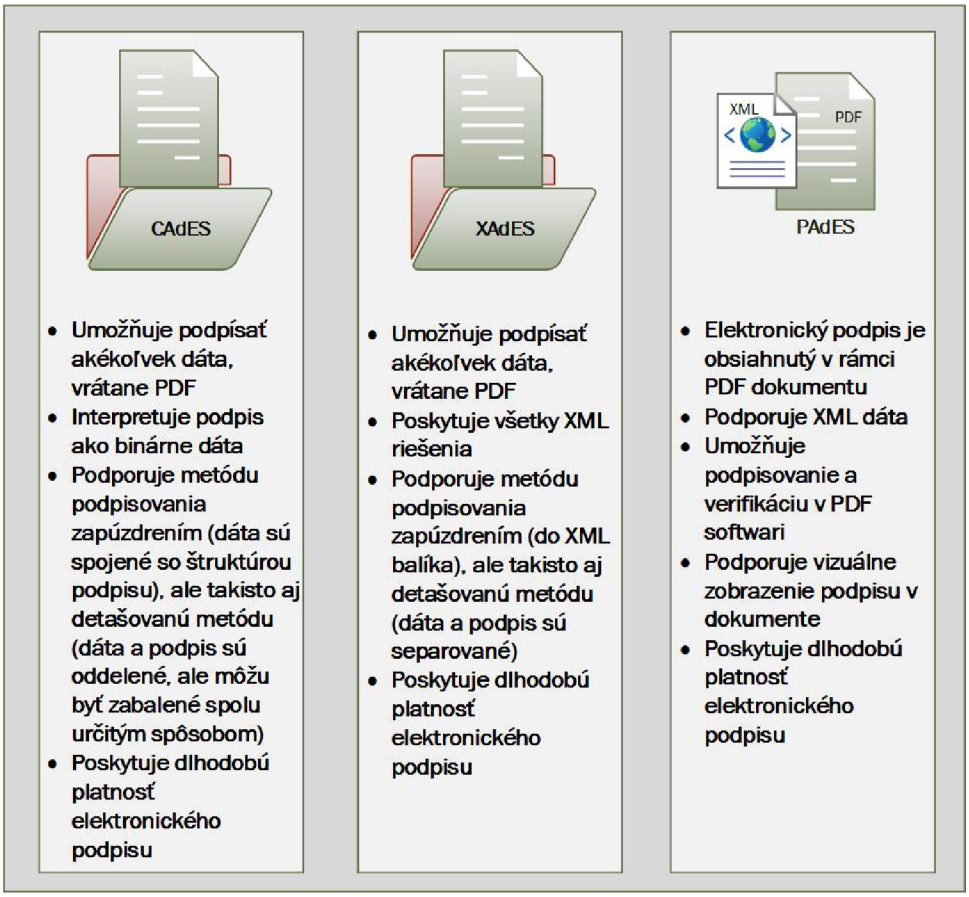
Kvalifikovaný elektronický podpis (často používaná anglická skratka QES) je zaručený elektronický podpis založený na kvalifikovanom certifikáte a vytorený prostredníctvom prostriedkov pre bezpečné vytváranie podpisov (z anglického „secure signature – creation device“). Vydáva ho certifikačná autorita, ktorá preveruje identitu vlastníka elektronického podpisu. Kvalifikovaný elektronický podpis je vydaný žiadateľovi až po preukázaní totožnosti (občianskeho preukazu) a teda tento krok nie je možné vykonať elektronicky. Takáto forma elektronického podpisu sa najviac približuje listinnému podpisu, ktorý je notársky overený.

Elektronická značka

Elektronická značka je obdobou elektronického podpisu, ktorú používajú organizácie, štátna správa a právnické osoby. Jej využitie je teda podobného charakteru ako majú klasické pečiatky, ktorými zamestnanci podpisujú a potvrdzujú dokument v rámci danej organizácie (napríklad v e-podateľni slúži ako elektronický podpis, bez toho aby bol viazaný na konkrétnu osobu, ale priamo na organizáciu). Elektronická značka je založená na kvalifikovanom systémovom certifikáte vydanom certifikačnou autoritou. Z technického hľadiska rozumieme pod elektronickou značkou údaje v elektronickej podobe, ktoré sú pripojené k štruktúre elektronického dokumentu alebo sú s ňou logicky spojené.[1] Najčastejšie má elektronická značka grafickú podobu loga danej organizácie a na prvý pohľad nemusí byť rozpoznateľné, že sa jedná v podstate o elektronický podpis. Takýto „grafický“ vzhľad podporuje dnes často používaný PDF formát.

2.1.1 Technické štandardy pre elektronické podpisy

ETSI (European Telecommunications Standards Institute) – Európsky úrad pre telekomunikačné normy, vytvoril štandardy pre elektronické podpisy, ktoré spĺňajú



Obr. 2.2: Porovnanie jednotlivých technických štandardov elektronických podpisov

požiadavky Európskej únie pre AdES a QES. Hlavným cieľom je definovať štandardy pre elektronický podpis, ktoré budú platné aj po dlhšom časovom období a vďaka ktorým bude v budúcnosti možné získať dostatočne veľa informácii a dôkazov o platnosti elektronického podpisu v konkrétnom čase v minulosti. Takéto štandardy sú založené na infraštruktúre verejného kľúča, pričom musia zabezpečiť dve základné kritéria:

- jednoznačnú spojitosť identity podpisujúcej strany s podpísaným súborom,
- nemennosť a nenahraditeľnosť podpísaného objektu bez prípadnej požiadavky na zmenu.

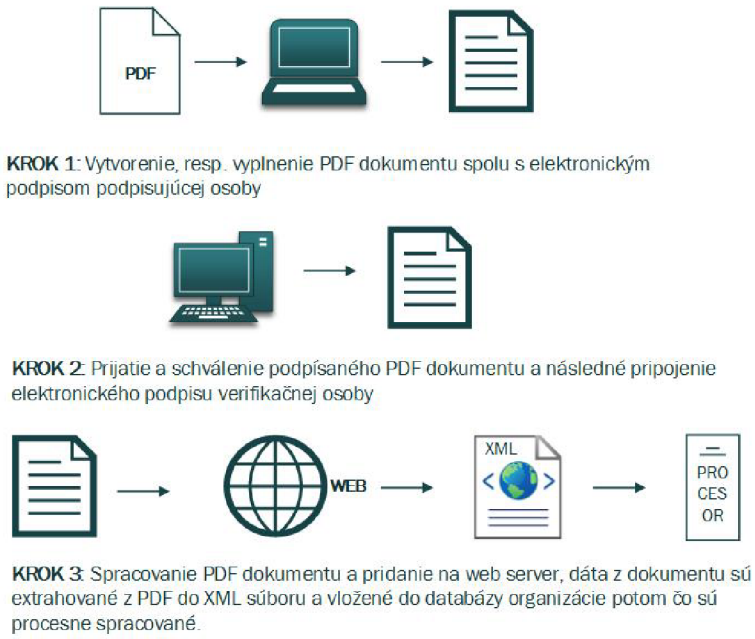
CAdES – štandard vyvinutý na základe formátu CMS (Cryptographic Message Syntax), tvorí základný stupeň pre elektronické podpisy založené na infraštruktúre verejného kľúča PKI (Public Key Infrastructure). Medzi jeho prednosti patrí predovšetkým jednoduchosť vytvárania a overovania elektronického podpisu a to v krátkodobom, strednodobom ale aj dlhodobom horizonte. Na druhej strane, keďže neexistuje vhodný referenčný model, nastáva problém s kontrolou správnej implementácie

a verifikácie algoritmu vytvárania a overovania elektornických podpisov podľa návrhu ETSI.
XAdES – štandard založený na XML štruktúre, avšak môže byť použitý pre všetky typy dát. Rovnako ako CAdES, aj XAdES poskytuje základnú autentifikáciu a tiež ochranu celistvosti dát. Výhoda tohto štandrdu spočíva v tom, že elektronický podpis využívajúci XML formát môže zostať v platnosti počas dlhého časového obdobia.
PAdES – predstavuje štandard vytvorený špeciálne pre formát PDF (Portable Document Format). Definuje požiadavky, ktoré musí softvér pre prehliadnie alebo editáciu PDF súborov spĺňať. Kedže tento štandard je súčasťou elektronického dokumentu, podporuje a definuje ako môže byť elektronický podpis zobrazený priamo na príslušnej strane dokumentu. Súčasťou tohto štandardu je aj spôsob integrácie vypĺňaných súčasti PDF formátu.

Najväčším rozdielom medzi CAdES a XAdES, ktoré fungujú na veľmi podobnom princípe a medzi PAdES je v tom, že PAdES definuje ako by software, ktorý spracováva elektronický podpis v PDF dokumente mal pracovať. Na druhej strane CAdES a XAdES iba definujú technológiu, ktorá musí byť použitá pri vývoji aplikácie, ktorá bude schopná pracovať s elektronickými podpismi. Pri týchto dvoch štandardoch existujú iba dve možnosti ako uchovať elektronický podpis spolu s podpisovanými dátami. Jednou je vytvoriť miesto v rámci dátovej štruktúry dokumentu a byť jeho priamou súčasťou. Druhou je vytvorenie určitého „baliaceho“ formátu a vložiť do neho elektronický podpis spolu s dátami, pričom tie sú od seba oddelené. Pri použití CAdES a XAdES môžu byť dáta rôzneho druhu a formátu, vrátane PDF formátu, a proces podpisovania a verifikácie môže byť vykonaný nezávisle od softwaru, ktorý spracováva dáta. Obr. 2.2 prehľadne zobrazuje hlavné vlastnosti a charakteristiky CAdES, XAdES a PAdES.

Kľúčovým faktorom, ktorý rozhodne o primárnom využívaní jedného zo štandardov, bude vhodnosť použitia pre aplikácie, ktoré pracujú s „ľudsky čitateľnými dokumentmi“. Z tohto pohľadu sa javí PAdES ako najperspektívnejší štandard najmä vo vzťahu k elektronickej archivácii elektronických dokumentov.

Obr. 2.3 zobrazuje ako môže štandard PAdES pracovať v súvislosti s PDF dokumentom v typickom pracovnom postupe, od vyplnenia dokumentu až po jeho procesné spracovanie organizáciou. Najprv je dokument elektronicky podpísaný jeho autorom, pričom tento podpis je priamo dátovou súčasťou PDF dokumentu, a následne je odoslaný overovateľovi dokumentu. Ten po verifikácii pripojí svoj elektronický podpis a odošle dokument do informačného systému organizácie, kde môže byť dokument extrahovaný z PDF do XML súboru a vložený do elektronického archívu. [1]



Obr. 2.3: Pracovný postup spracovania a ošetrenia PDF dokumentu elektronickým podpisom na základe PAdES štandardu

2.2 Problematika zabezpečenia dokumentov

Už spomenuté legislatívne obmedzenia (v predchádzajúcej kapitole 1.2) limitujú plné využitie elektronických dokumentov. Ak sú však dáta správne spracované a zabezpečené môžu predstavovať modernú protiváhu k tradičným papierovým dokumentom. Samozrejme elektronické dáta sú svojou formou náchylné z hľadiska bezpečnosti, preto je pri ich použití potrebné vyriešiť minimálne tri problémy súvisiace s ich platnosťou a právnou záväznosťou:

1. Dokumenty v elektronickej forme, ktorých integrita nie je dostatočne zaistená, sa môžu stať cieľom manipulácie. Preto musia byť prostriedky demonštrujúce jednoznačnú integritu a platnosť elektronických dokumentov vždy prítomné a prístupné. Obzvlášť ak sa jedná o dokumenty s veľmi privátnym obsahom (napríklad zmluvy).
2. Často musí byť právoplatne preukázaná existencia špecifických dokumentov (ako napríklad faktúr) v konkrétnom časovom okamžiku. Z tohto dôvodu musia elektronické dokumenty obsahovať určitú časovú zložku, ktorú nebude možné žiadnym spôsobom pozmeniť.
3. Platnosť elektronicky podpísaných dokumentov musí byť chránená celý archivačný cyklus. To znamená predlžovať limitovanú platnosť digitálnych certifikátov a na nich založených elektronických podpisov.

Elektronický podpis v podstate neobsahuje vo svojej štruktúre informáciu o dôveryhodnosti elektronického dokumentu, ktorý podpisuje. Preto je elektronicky podpísaný dokument legálne záväzný len počas platnosti digitálneho certifikátu. Najväčším problémom v praxi je predlžovanie platnosti digitálnych certifikátov, ktorými sú elektronické dokumenty podpísané. Dve všeobecne známe a používané riešenia sú[21]:

1. **Opätovné podpísanie elektronickým podpisom** pred expiráciou digitálneho certifikátu. Táto možnosť vyzerá na prvý pohľad realizovateľne, ale je prakticky nemožné ju využiť napríklad pri multilaterálnych zmluvách, kde je viacero elektronických podpisov a prístup k nim je problematický,
2. **Doplnenie elektronického podpisu časovou pečiatkou** (časovým pečiatkam sa venuje nasledujúca kapitola 2.3).

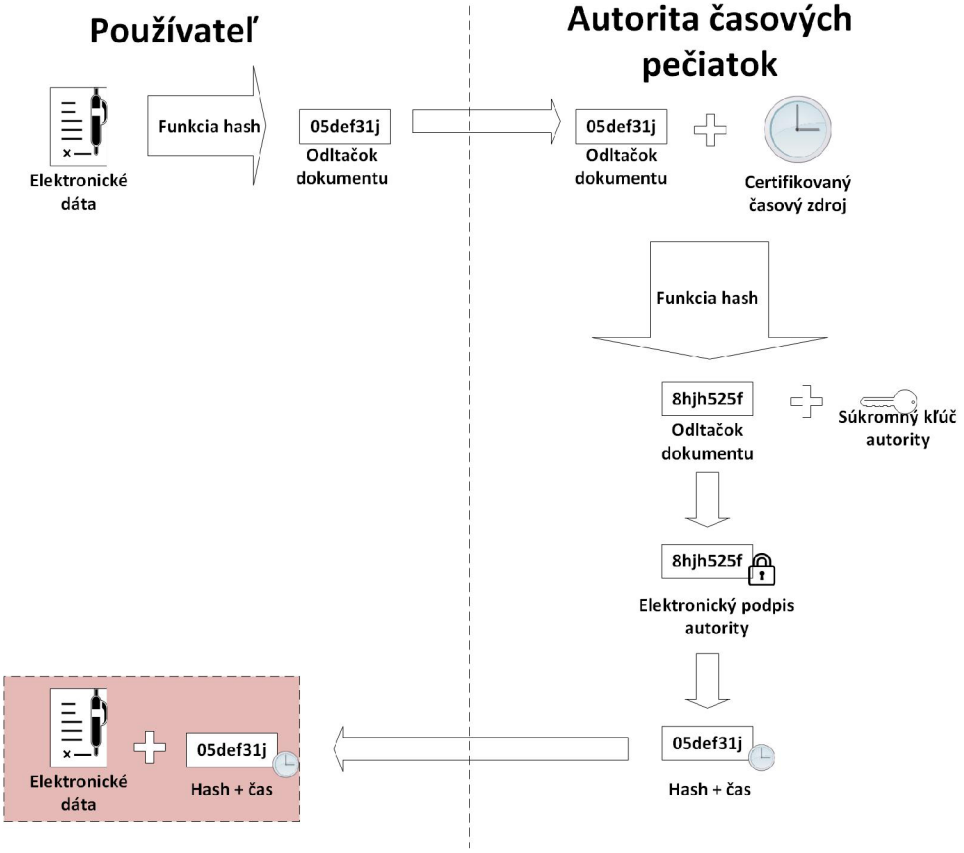
2.3 Elektronická časová pečiatka

Elektronická časová pečiatka (z anglického „timestamp“) je v podstate doplnok elektronického podpisu. Je výhodné, aby každý podpísaný elektronický dokument obsahoval dátum svojho vzniku (resp. dĺžku svojej platnosti), pretože tak odpadá potreba opätovne podpisovať dokument po uplynutí platnosti digitálneho certifikátu. Navyše ak dokument neobsahuje údaj o dátume a čase vzniku, nie je možné overiť, či bol dokument podpísaný práve v čase platnosti certifikátu. Zároveň poskytuje aj dôkaz o existencii elektronického dokumentu v konkrétnom čase, čím zabezpečuje jeho nepopierateľnosť.

Časovú pečiatku vydáva **autorita časových pečiatok** TSA (obr. 2.4). Tu je možné získať na základe požiadavky, do ktorej je potrebné uviesť vstupné dáta – odtlačok dokumentu, respektíve hash (ako bolo uvedené v kapitole 1.5, prakticky nie je možné odvodiť z neho obsah dokumentu). Autorita časových pečiatok následne pripojí k odtlačku potrebné atribúty, ako aktuálny dátum a čas (pričom využíva akreditovaný časový zdroj), sériové číslo pečiatky a nakoniec celé dáta podpíše pomocou svojho súkromného kľúča, čím prakticky ručí za správnosť podpísaných dát. Takýto celok je potom odoslaný späť žiadateľovi. Proces pridelovania časovej pečiatky je veľmi podobný samotnému procesu vytvárania elektronického podpisu (rozdiel je v pridaní časového údaju).

Treba si však uvedomiť, že časová pečiatka má takisto limitovanú platnosť (keďže je podpísaná elektronickým podpisom TSA autority). Z toho dôvodu musí byť periodicky obnovovaná v rámci predpísanej archivačnej periódy vo vzťahu k legálne záväzným elektronickým dokumentom, aby došlo k predĺženiu jej platnosti.

Elektronický podpis spolu s časovou pečiatkou uvádza do súvislosti nie len do-

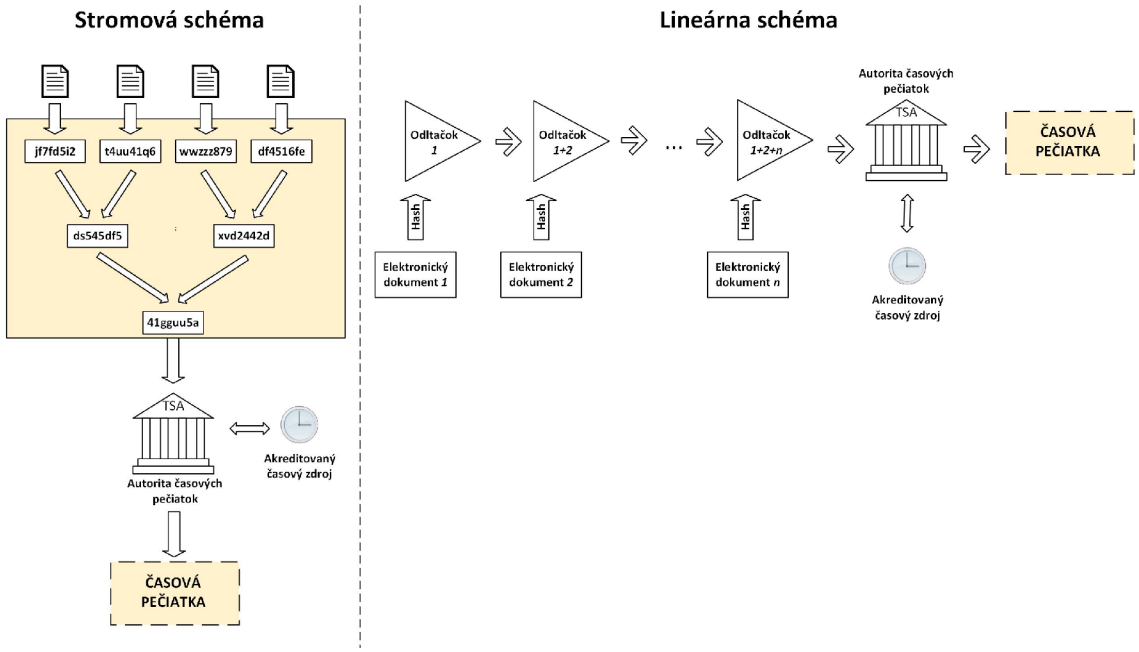


Obr. 2.4: Proces vytvorenia časovej pečiatky

kument a osobu, ktorá ho podpísala, ale aj časový okamžik, pred ktorým dokument zaručene existoval. Dôležité na tomto procese je, že príslušná autorita pri vytváraní časového razítka nie je žiadnym spôsobom závislá na obsahu dokumentu a nemá možnosť doňho nahliadnuť, kedže vychádza len z odtlačku dokumentu.[20]

2.4 Linkovaný hash

Ako už bolo spomenuté, použitím časovej pečiatky je v podstate možné donekonečna predlžovať platnosť elektronického podpisu. Ak však vstupuje napríklad do elektronického archívu naraz väčšie množstvo elektronických dokumentov, je časovo zdĺhavejšie postupne obstarať všetky elektronické podpisy časovými pečiatkami. Z toho dôvodu sa využíva technika nazývaná **linkovaný (previazaný) hash**. Je založená na rovnakom princípe ako klasická funkcia hash, teda na vytvorení odtlačku z elektronického dokumentu. Rozdiel je v tom, že pri viacerých dokumentoch sa využívajú mechanizmy ako **stromová schéma** a **lineárna schéma** (obr. 2.5).



Obr. 2.5: Pridelenie časovej pečiatky viacerým elektronickým dokumentom

Linkovaný hash sa využíva pre získanie časovej pečiatky. Z každého elektronického dokumentu sa pomocou funkcie hash vytvorí odtlačok dokumentu. Následne sa z každého páru odtlačkov vytvorí ďalší (spoločný) odtlačok, až kým nevznikne jeden **koreňový odtlačok**. Ten je odoslaný autorite časových pečiatok, ktorá pridelí skupine elektronických podpisov časovú pečiatku.

Postup vytvorenia linkovaného hashu sa dá vyjadriť aj matematicky – využívajúc súvislosť časovej postupnosti, s ktorou sú elektronické dokumenty vkladané do elektronického archívu. Predstavme si, že dokument ED_n bol do archívu vložený medzi dobou vloženia predchádzajúceho dokumentu ED_{n-1} a nasledujúceho ED_{n+1}. Ak počítame s tým, že sa do archívu denne vkladá 100 dokumentov, tak stačí pripojiť časovú pečiatku na každý stý elektronický dokument. Následne je ľahké získať časovú postupnosť dokumentov „ukotvením“ k predchádzajúcemu a nasledujúcemu dokumentu pomocou linkovaného hashu. Ten sa získa tak, že k hash ED_n sa pridá zľava hash ED_{n-1} a sprava hash ED_{n+1}, a na výsledný reťazec sa aplikuje hashovacia funkcia. Novovzniknutý linkový hash sa podpíše súkromným kľúčom a zapíše sa do ED_n. Tento proces sa v súvislosti s elektronickou archiváciou aplikuje na každý elektronický dokument, ktorý vstupuje do archívu.[11]

Podmienkou je spoločné uloženie elektronických dokumentov v jednom úložisku. Nevýhodou je, že pri skončení platnosti časovej pečiatky je potrebné všetky elektronické podpisy znovu opatriť pečiatkami.

3 ARCHIVÁCIA ELEKTRONICKÝCH DOKUMENTOV

Ako je uvedené v úvode, pre čoraz častejšie využívanie elektronickej komunikácie vzrastá požiadavka na uchovanie vzniknutých elektronických dokumentov. Tie sú centralizované v **elektronickom archíve**, ktorý predstavuje úložisko a systém pre správu takýchto dokumentov. V súčasnosti média po hardwarovej a softwarovej stránke rýchlo starnú, takže je potrebné zabezpečiť, aby archivované dáta boli uložené vo formátoch a na médiach, pri ktorých nebude problém s čitateľnosťou a manipuláciou aj v budúcnosti. Pri zostarnutí pôvodných technológii je potrebné dáta preniesť na nové média či konvertovať do aktuálnych formátov. Elektronická archivácia je však obmedzená legislatívou konkrétnych krajín a preto musí spĺňať určité právne podmienky, ktoré treba splniť a dodržať. Tie sú v Českej republike definované a upravené v *zákone č. 499/2004 Sb., o archivnictví a spisové službě*, ktorý bol neskôr viackrát novelizovaný. Tento zákon zavádza pravidlá pre elektronickú archiváciu, ďalej sa venuje vedeniu a nakladaniu so spismi (v papierovej podobe) a taktiež digitalizácii a elektronickému ukladaniu dát.

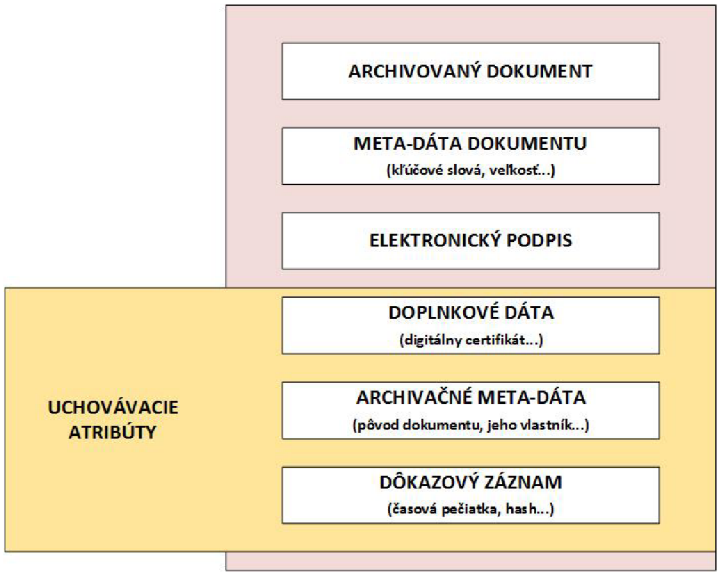
Z hľadiska funkcionality by mal byť každý elektronický archív vybavený[14]:

- bohatou štruktúrou metadát, podľa ktorých by bolo možné dokumenty v archíve vyhľadávať,
- zabezpečeným prístupom k elektronickým dokumentom prostredníctvom prístupového systému alebo internetového prehliadača,
- určenie doby archivácie a nastavenie skartačného procesu,
- konverzia dokumentov do štandardných formátov, ktoré budú zárukou čitateľnosti a zobraziteľnosti dokumentov aj v budúcnosti,
- export dát na archívne neprepisovateľné média.

3.1 Archivačný objekt

Každý elektronický dokument, respektíve dáta v elektronickej podobe, sa po uložení do elektronického archívu stávajú súčasťou **archivačného objektu**. Jeho úlohou je v podstate zjednotiť všetky dáta súvisiace s konkrétnym archivaným dokumentom a zachovať ho tak v originálnej podobe. Takýmto spôsobom je potom jednoduchšie generovať dôkazové informácie potrebné pre dlhodobú a najmä dôveryhodnú elektronickú archiváciu. V štruktúre archivačného objektu, ktorá je prehľadne zobrazená na obr. 3.1, majú na starosti túto úlohu **uchovávacie atribúty**. Funkciou týchto atribútov je poskytnúť dôveryhodnú informáciu o existencii archivovaných dát, ich integrite, autenticite a platnosti (napríklad pri elektronickom podpise).[3]

Počas archivačného procesu môžu byť doplnené určité dodatkové informácie o dokumente – meta-dáta (napríklad kľúčové slová, počet strán...), pomocou ktorých bude potom dokument v archíve v budúcnosti jednoduchšie vyhľadať. Nevyhnutnou entitou každého archivačného objektu je elektronický podpis. Informácie o jeho digitálnych certifikátoch sú obsiahnuté v doplnkových dátach, pretože sú súčasťou uchovávacích atribútov. V niektorých konkrétnych prípadoch môžu byť vyžadované špecifické informácie o archivovanom dokumente, ako napríklad na základe legislatívnej požiadavky údaje o vlastníkovi, pôvode dokumentu alebo archivačnom čase. Veľmi podstatnou entitou z hľadiska dôveryhodnosti elektronického archívu je dôkazový záznam, ktorý je generovaný archivačným systémom alebo je vyhľadávaný v štruktúre dokumentu (napríklad časová pečiatka alebo hash).



Obr. 3.1: Uchovávacie atribúty v štruktúre archivačného objektu

Archivačné objekty sú v archíve udržiavané počas celého archivačného cyklu archivačným systémom. Archivačný systém musí archivačný objekt po jeho vytvorení kontinuálne udržiavať z dôvodu zabezpečenia dlhodobej integrity dokumentu a jeho časovej existencie. Takýmto udržiavaním sa rozumie nahradenie starých dôkazových záznamov novými, a to počas celej archivačnej doby.

3.2 Doba archivácie elektronických dokumentov

Pri archivácii je takisto dôležité, o akú dobu uchovania z hľadiska času sa jedná. V praxi si každá orgnizácia, častokrát vychádzajúc z legislatívnych podmienok, určuje dĺžku archivácie dokumentov. Pri elektronickej archivácii je však dôležité udržia-

vať všetky potrebné ukazovatele pravosti dokumentov (napr. obnovovať elektronické podpisy alebo časové pečiatky).Vychádzajúc z tejto podmienky sa rozlišuje:

- Krátkodobá archivácia
- Strednodobá archivácia
- Dlhodobá a trvalá archivácia

Krátkodobá archivácia

Pre archiváciu elektronických dokumentov v krátkodobom horizonte je podstatou zabezpečiť indície o ich existencii v konkrétnom čase. Za najvhodnejší mechanizmus sa v krátkodobej archivácii považuje elektronická časová pečiatka dokumentu. Tú treba k dokumentu pripojiť ihneď po vzniku elektronického podpisu alebo až pri vstupe do archívu. Takéto ošetrenie dokumentov by malo byť z hľadiska efektivity a časovj náročnosti zautomatizované archivačným systémom.

Strednodobá archivácia

Pri strednodobej archivácii sa predpokladá, že dokument bude uložený v elektronickom archíve roky. Problém predstavuje platnosť certifikátov, ktoré sú potrebné pre overenie elektronických podpisov a časových pečiatok. Informačný systém by mal byť preto vybavený funkciou automatického obnovenia elektronických podpisov, t.j. mal by podporovať dlhodobé elektronické podpisy (obsahujú digitálne certifikáty s dlhodobejšou platnosťou) a linkovaný hash. Medzi typické strednodobé archívy patria DMS a ECM systémy, ktoré spravujú dokumenty (napr. systém prístupových dát, prehľadávanie obsahu dokumentov a pod.). K týmto systémom sa ešte zvyčajne implementujú kryptografické knižnice zabezpečujúce správu elektronických podpisov.[9]

Dlhodobá a trvalá archivácia

Dlhodobou archiváciou sa myslí uloženie aj po dobu desiatok rokov a dokonca ani nemusí nikdy nastať skartačný proces (v tom prípade sa jedná o trvalú archiváciu). V takomto časovom horizonte nastáva pri archivácii problém s dátovými formátmi a takisto sa vynára otázka sily a právnej váhy samotného elektronického podpisu. Z toho dôvodu predtavuje najväčší problém zaručenie dôveryhodnosti samotných archivovaných elektronických dokumentov. Dokumenty by nemali byť preto zverené bežným informačným systémom, ale špecializovaným systémom pre dlhodobú archiváciu elektronických dokumentov. Tieto systémy sa nazývajú dôveryhodné archivačné autority (TAA) a predstavujú obdobu klasických verejných archívov.[9]

3.3 Dlhodobá čitateľnosť elektronických dokumentov

Archivácia elektronických dokumentov, a to hlavne z hľadiska dlhodobej archivácie, predpokladá ich dlhodobú čitateľnosť. V súčasnom tempe technologického vývoja môže nastať zostarnutie hardwarovej platformy, operačného systému, aplikací, zmeny kódovania a hlavne súborových formátov, a tým hrozí strata čitateľnosti archivovaného elektronického dokumentu.[11] Z toho dôvodu bolo potrebné vytvoriť mechanizmy, ktoré dokážu zaručiť, že obsah elektronických dokumentov bude prístupný v čitateľnej forme. Prax ukázala, že čitateľnost elektronických dokumentov je možné obnovovať v podstate len dvomi spôsomi – **migráciou** a **emuláciou**. Zároveň je možné každú z nich **virtualizovať**.

3.3.1 Migrácia elektronických dokumentov

Migrácia je najvhodnejší spôsob ako už vopred zväčšiť pravdepodobnosť, že obsah archivovaného elektronického dokumentu bude čitateľný aj o niekoľko rokov. Migrácia je prevod elektronických dokumentov do nových formátov, prípadne hardwarových konfigurácii alebo softwarových aplikácii. Migráciu dokumentov je vhodné, z hľadiska dlhodobej čitateľnosti, vykonať už pri ukladaní do elektronického archívu a to do časovo stálych formátov. Medzi tie môžeme považovať dlhodobo používané formáty, odporúčané normou ISO a stanovené *Vyhláškou č. 191/2009 §20 Sb., o podrobnostech výkonu spisové služby* z dňa 23. júna 2009[4]:

- **statické textové a statické textovo-obrazové dokumenty** – formát PDF/A (norma ISO 19005),
- **statické obrazové dokumenty** – formáty PNG (norma ISO/IEC 15948), TIFF (revízia 6, nekomprimovný), JPEG (norma ISO/IEC 10918),
- **dynamické dátové dokumenty** – formáty MPEG-2 (norma ISO/IEC 13818), MPEG-1 (norma ISO/IEC 11172), GIF,
- **zvukové dokumenty** – formáty MP2 (MPEG-1 Audio Layer 2), MP3 (MPEG-1 Audio Layer 3), WAV (PCM modulácia),
- **metadáta dokumentov** – formát XML (podľa schémy prílohy národného štandardu pre elektronické systémy spisovej služby).

Použitie konkrétných dátových formátov počítačových súborov je upresnené aj v niektorých ďalších právnych predpisoch Českej republiky, ktoré sú vhodné aj pre dôveryhodnú dlhodobú elektronickú archiváciu. Jedná sa o vyhlášky[15]:

- *vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby,*
- *vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů,*

- *vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, ve znění vyhlášky č. 422/2010 Sb.*

Migrácia elektronických dokumentov má však niekoľko úskalí a to v možnej deformácií obsahu dokumentu pri zmene formátu. Preto sa v súčasnosti (ak nie je potreba uložiť multimédialný obsah) preferuje hlavne PDF formát (viac sa mu venuje kapitola 3.3.2). Najväčšou hrozbou je znehodnotenie elektronického podpisu dokumentu a teda zachovanie autentickosti.

Emulácia

Emulácia je simulácia pôvodného hardwarového prostredia (architektúry, operačného systému) na aktuálnej platforme. Vďaka emulácii je možné zobraziť elektronický dokument v originálnom softwari a je to jeden z možných spôsobov ako ho zobraziť v pôvodnej podobe. Pri emulácii je potrebné uchovávať aj inštalačné súbory pôvodnej platformy. Výhodou emulácie je možnosť uchovávať aj vektorovú grafiku a multimediálne elektronické dokumenty. Rizikom je strata schopnosti emulovať niektorú vlastnosť pôvodnej platformy.[11]

Virtualizácia

Princípom virtualizácie elektronických dokumentov je ich uchovanie v pôvodnom formáte spolu s programom, ktorý umožní jeho interpretáciu v strojovom jazyku „univerzálneho virtuálneho počítača“. Tento jazyk si vyžaduje jednoduchosť, otvorenosť a všeobecnosť. Pri prechode na novú plaformu potom už len postačí, aby obsahovala interpret tohto jazyka.[11]

3.3.2 Formát PDF

Pri elektronických dokumentoch je podstatná otázka, v akom formáte budú uložené, a to najmä z hľadiska dlhodobej čitateľnosti. V súčasnosti sa vo veľkej miere používa rokmi overený a celosvetovo uznávný formát **PDF** vytvorený americkou spoločnosťou Adobe Systems. Jedná sa o otvorený formát spĺňajúci normu *ISO:32000*[1], ktorý je možné prehliadať a tlačiť na rôznych technologických platformách(MS Windows, Unix, Android...).

PDF formát sa stal populárny a teší sa veľkej obľube nie len medzi bežnými užívateľmi, ale aj samotnými organizáciami. Popularite vďačí hlavne vďaka svojim vlastnostiam. PDF umožňuje jednoduchý prevod elektronických dát do papierovej podoby, pričom po vytlačení vyzerajú úplne rovnako ako pri zobrazení v PDF formáte – zachováva integritu dokumentu. Zároveň dovoľuje uložiť „bohatší“ digitálny

[1]ISO – Medzinárodná organizácia pre normalizáciu tento formát zároveň spravuje.

obsah a prezentovať ho užívateľovi. Využívanie tohto formátu je výhodné aj preto, že dokáže reprezentovať takmer každú formu papierového dokumentu a podporuje elektronický podpis založený na štandarde PAdES. Oproti iným formátom má výhodu v tom, že ponúka klikacie odkazy na URL odkazy a umožňuje vysokú kompresiu obsiahnutých dát (jeho výsledná veľkosť je potom omnoho menšia).

Pre elektronickú archiváciu je tento formát výhodný aj z pohľadu zabezpečenia elektronického dokumentu. Obsahuje funkciu ochrany pomocou hesla, vďaka ktorej dokáže zabrániť prístupu k obsahu dokumentu a ďalšej manipulácii s ním. Navyše každý elektronický dokument je možné podpísať elektronicky a to aj pomocou bezplatného softwaru (Adobre Reader). Podpora elektronického podpisuje je založená na certifikáte overovanom certifikačnou autoritou, čo je pre dôveryhodnosť elektronického archívu jedna z kľúčových podmienok.

Formát PDF/A

Pre archiváciu elektronických dokumentov však existuje špeciálna modifikácia s názvom **PDF/A**. Tá bola normou *ISO 19005-1:2005* uznaná ako celosvetový štandard pre dlhodobú archiváciu. PDF/A je obmedzená verzia PDF formátu s predurčením slúžiť pre dlhodobú archiváciu elektronických dokumentov. Medzi najdôležitejšie obmedzenia tohto formátu, vzhľadom k dlhodobému zachovaniu zobraziteľnosti a využiteľnosti obsahu dokumentu nezávislé na použitých prostriedkoch, patrí napríklad[13]:

- audio a video obsah je zakázaný,
- PDF/A musí obsahovať všetky písma použité v jeho texte,
- určité meta-dáta musia byť vytvorené (meta-dáta sú nevyhnutné pre elektronickú archiváciu),
- využitie len takých farieb, ktoré sú nezávislé na použitom zariadení,
- je zakázané šifrovanie a JavaScript.

Jasným zámerom tejto modifikácie, aj na základe uvedených obmedzení, je bezproblémové zobrazenie dokumentu na akejkoľvek platforme a jednoduchšie zatriedenie v archíve. Zároveň eliminuje problémy so šifrovaním, multimediálnym obsahom a s nimi súvisiacimi nastaveniami.

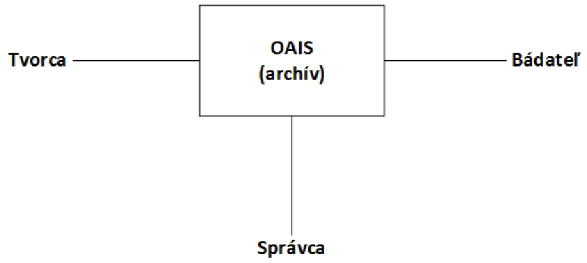
Z hore uvedených obmedzení vyplýva, že hlavným cieľom pri vývoji[2] tohto štandardu bola dlhodobá čitateľnosť obsahu dokumentu aj v budúcnosti. Archivácia elektronických dokumentov uložených v tomto formáte predstavuje zjavnú výhodu a pri súčasnej obľube využívania PDF formátu je možné predpokladať, že zámer vytvoriť časovo stály formát mohol byť úspešný.

[2]Pri vývoji PDF/A štandardu sa zúčastnili predstavitelia vlád, priemyslu a odborníci z Adobe Systems, Xerox, Honeywell či Library of Congress.

Formát PDF/A je vhodný najmä pre dlhodobú a dôveryhodnú elektronickú archiváciu, kde je prioritou archivovať elektronicky podpísané dokumenty. Výber podporovaných formátov konkrétnym elektronickým archívom by mal byť vždy podriadený svojmu účelu a nárokom jeho vlastníka (z pohľadu typu obsahu elektronických dát, požadovanej bezpečnosti, dlhodobej čitateľnosti. . .).

3.4 Referenčný model OAIS

Archivácia elektronických dokumentov je zložitá koncepčná a technologická výzva. Už od počiatku sa preto pri vývoji archívov sústredilo na definíciu stabilného prostredia pre uloženie, prístup a interpretáciu elektronických dokumentov.[2] Snaha o naozaj dlhodobý až trvalý dôveryhodný archív nakoniec vyústila vytvorením referenčného modelu **OAIS**, ktorý sa stal základom štandardu ISO 14721:2003 pre dlhodobé úložisko elektronického archívu. Princíp tohto modelu vystihuje obr. 3.2. Tvorca archiválií predáva dáta k archivácii do archívu. Archív je spravovaný správcom. Archiválie (dokumenty) sú potom sprístupňované bádateľom.



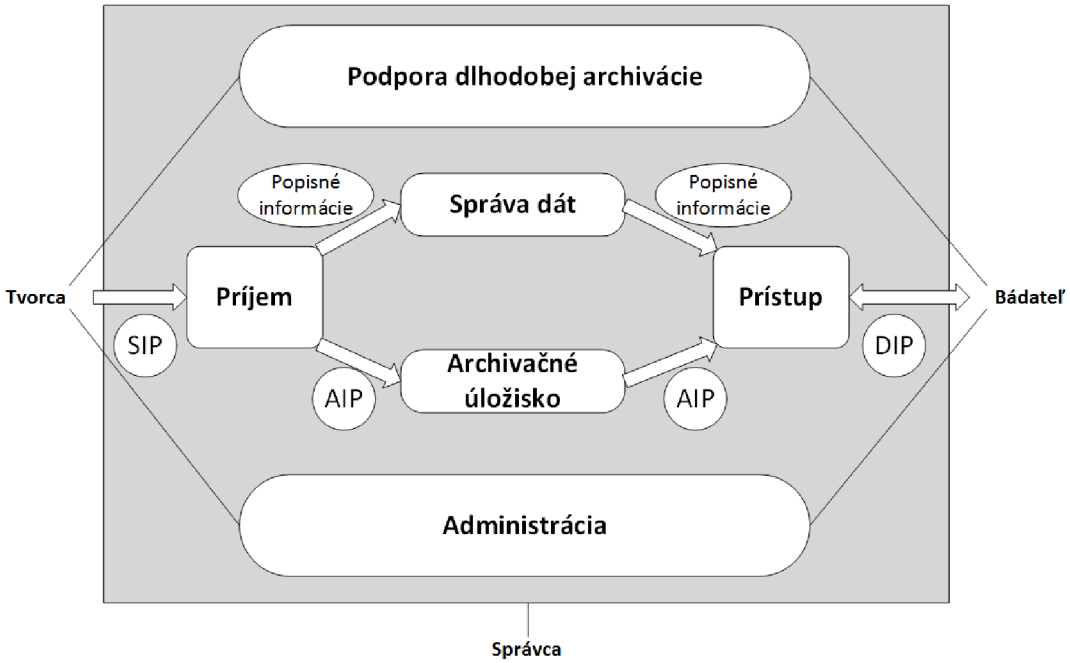
Obr. 3.2: Princíp modelu OAIS

Základnou archivačnou jednotkou je balík informácií (z anglického „information package“). Ten tvorca zasiela do archívu, správca ju archivuje a následne ju bádateľ vyzdvihne. Existujú tri typy balíkov informácií:

- balík informácií zaslaný tvorcom do archívu (SIP),
- balík informácií udržiavný v archíve (AIP),
- balík informácií vydaný bádateľovi –prezentačný balík (DIP).

OAIS je formálny model (obr. 3.3) identifikujúci a popisujúci základný mechanizmus, ktorým sa realizuje dlhodobá archivácia dokumentov a prípadne ich sprístupnenie. Model obsahuje šesť komponentov, ktorých úlohou je zabezpečiť uloženie archivovaných dokumentov a ich sprístupnenie. Tvorca archiválií predá dopredu dohodnutým spôsobom SIP archívu. Prvý komponent na strane archívu, „Príjem“, preberá SIP. Tento komponent je zodpovedný za príjem dát od tvorcu a ich prípravu

pre uloženie do archívu – verifikuje SIP a generuje AIP a príslušné metadáta k AIP. Z „Príjmu“ putuje AIP do „Archívneho úložiska“, ktoré zaistí jeho trvalé uloženie. Tento komponent sa stará o údržbu AIP, ktorá zahŕňa obnovovanie archivačných médií a takisto poskytuje AIP komponentu „Prístup“. Tento komponent slúži bádateľom pre žiadosť a následný prístup k elektronickým dokumentom prostredníctvom DIP. Zatiaľ čo AIP smeruje z „Príjmu“ do „Archívneho úložiska“, metadáta putujú do komponentu „Správa dát“. Tu sa spravujú metadáta týkajúce sa AIP spolu so systémovými informáciami, ktoré sa využívajú pre podporu operácií s archívom. Špeciálne postavenie má komponent „Administrácia“ zodpovedajúci za chod celého archívu, sledujúci komunikáciu medzi jednotlivými komponentami archívu a spravujúci konfiguráciu hardwéru a softwéru.



Obr. 3.3: Podrobná schéma referenčného modelu OAIS

Taktiež zaujímavý je komponent „Podpora dlhodobej archivácie“, ktorý sleduje AIP z dlhodobého pohľadu – zabezpečuje čitateľnosť v priebehu času. Tento komponent sa teda zaoberá procesmi ako sú migrácia, emulácia a sledovanie najnovších technológií. Najpodstatnejšia je však úloha ošetrovania elektronických podpisov a časových pečiatok.

Model OAIS je považovaný za štandard pre uchovanie elektronických dát a teda aj pre vývoj aplikácií pre dôveryhodné dlhodobé elektronické archívy. Zároveň poskytuje základný koncept dlhodobého DEA, definuje jeho hlavné funkcie a zjednocuje terminológiu v tejto oblasti. [9] [14]

3.5 Existujúce elektronické archívy

Aj keď ešte nie je elektronická archivácia využívaná naplno, na trhu existuje niekoľko riešení ponúkajúcich dôveryhodnú a dlhodobú archiváciu elektronických dokumentov. Poskytovatelia takýchto archivačných služieb musia spĺňať legislatívne kritéria danej krajiny a medzinárodné štandardy zavedené v tejto oblasti. Vo väčšine prípadov sú poskytované komplexné riešenia od vytvorenia elektronického podpisu až po samotné fyzické uloženie elektronických dát. V Českej republike pôsobí viacero spoločností ponúkajúcich elektronickú archiváciu[3]:

- Dlouhodobý archiv – **Software602, a.s.**,
- Důvěryhodný elektronický archiv – **Sefira, s.r.o.**,
- Orion EDI – **CCV, s.r.o.**,
- Elektronický archiv dokumentů – **Syconix, a.s.**,
- Zabezpečený elektronický archiv (ZEA) – **Styrax, a.s.**,
- QSign Archive – **Ardaco, a.s.**,
- Dlouhodobá archivace – **T-Systems Czech republic, a.s.**

Momentálnym lídrom na trhu je spoločnosť Software602, a.s. Ponúka viacero služieb spojených s elektronickou archiváciou. V rámci elektronickej archivácie sa jedná o ucelené riešenie podporujúce elektronické podpisy založené na technických štandardoch CAdES a PAdES, pričom dokumenty konvertuje do formátu PDF/A. Kontroluje neporušiteľnosť obsahu dokumentu na základe digitálneho certifikátu, časovej pečiatky a súborových meta-dát. Rešpektuje normy ETSI a v rámci nich pravidelne obnovuje pečiatky, ktorým už skončila platnosť. Archivované dáta sú prístupné bez obmedzenia typu zariadenia alebo operačného systému (podporuje dokonca prístup cez mobilné zariadenia bežiace na operačnom systéme Android).[19] Ostatní dodávatelia sa takisto na svojich stránkach zaväzujú k rešpektovaniu legálnych požiadaviek po celú dobu archivácie, avšak na normy ETSI sa neodvolávajú.

Z celosvetového hľadiska existuje množstvo elektronických archívov, medzi najvýznamnejšie patria:

- E-keeper – **Setcce**,
- USC Digital Repository – **University of Southern California**,
- Trusted Digital Repository – **Ontario Council of University Libraries**,
- The Florida Digital Archive – **Florida Center for Library Automation**,
- O2 Smart Trusted Archive – **Telefónica O2**.

USC Digital Repository, Trusted Digital Repository, The Florida Digital Archive sú americké univerzitné elektronické archívy sprístupnené pre širšiu verejnosť. Z technického hľadiska je zaujímavý hlavne The Florida Digital Archive, ktorý vznikol

[3]Boli vybraté najpoužívanejšie riešenia v Českej republike. Zdrojom informácií sú webstránky daných spoločností.

centralizáciou viacerých knižníc a je založený na tzv. tmavom archíve (z anglického dark archive), čo znamená že plní funkciu repozitára – nie je prístupny verejnosti a podobá sa teda svojou funkciou na súkromný archív. O2 Smart Trusted Archive je komerčne využívané riešenie poskytované stabilnou medzinárodnou spoločnosťou.

Existujú už aj softwarové riešenia elektronických archívov s otvoreným prístupom (z anglického open-source) k obsahu zdrojového kódu. Každý používateľ si môže takto modifikovať archivačný systém podľa svojich predstáv a implementovať ho vo svojom elektronickom archíve. Medzi najpoužívanejšie patria:

- **OpenArchive**,
- **Archivematica**,
- **Kramerius**.

Všetky tieto riešenia sú prístupne na ich internetových stránkach pre stiahnutie a inštaláciu. Sú dizajnované pre operačné systémy Ubuntu a Linux. Kramerius je vytvorený v Českej republike[4], kde je aj najviac využívaný.

3.5.1 eKeeper

Jedným z priekopníkov v oblasti dôveryhodnej dlhodobej elektronickej archivácie v Európe ale aj na svete je slovinská firma SETCCE, ktorá vytvorila elektronický archív s názvom eKeeper. Predstavuje riešenie pre archiváciu elektronicky podpísaných, ale aj nepodpísaných elektronických dokumentov v dlhodobom časovom horizonte. eKeeper zabezpečuje a udržuje autenicitu archivovaného obsahu a dodržuje striktné požiadavky a štandardy v tejto technologickej oblasti. [10]

Elektronický archív eKeeper je založený na technológii verejného kľúča PKI, referenčnom modeli OAIS a báze klient – server. To znamená, že je prispôsobený komunikácii s klientom a umožňuje koncovému užívateľovi plné využitie služieb ako vytváranie meta-dát a ich odosielanie na server, tvorbu vlastných archivačných funkcií, editáciu a odstraňovanie elektronických dokumentov. Výhodou tohto archívu je jeho autonómna verifikácia pravosti elektronického podpisu v prípade elektronicky podpísaných dokumentov. Zároveň je navrhnutý tak, aby dokázal vytvoriť uchovávacie atribúty demonštrujúce celistvosť každého archivovaného elektronického dokumentu a udržiaval jeho legálnu platnosť.

[4]Na jeho vývoji sa podieľú odborníci z Knihovny AV ČR, Národní knihovny ČR, Moravské zemské knihovny v Brně, Národní technické knihovny a Národní lékařské knihovny.

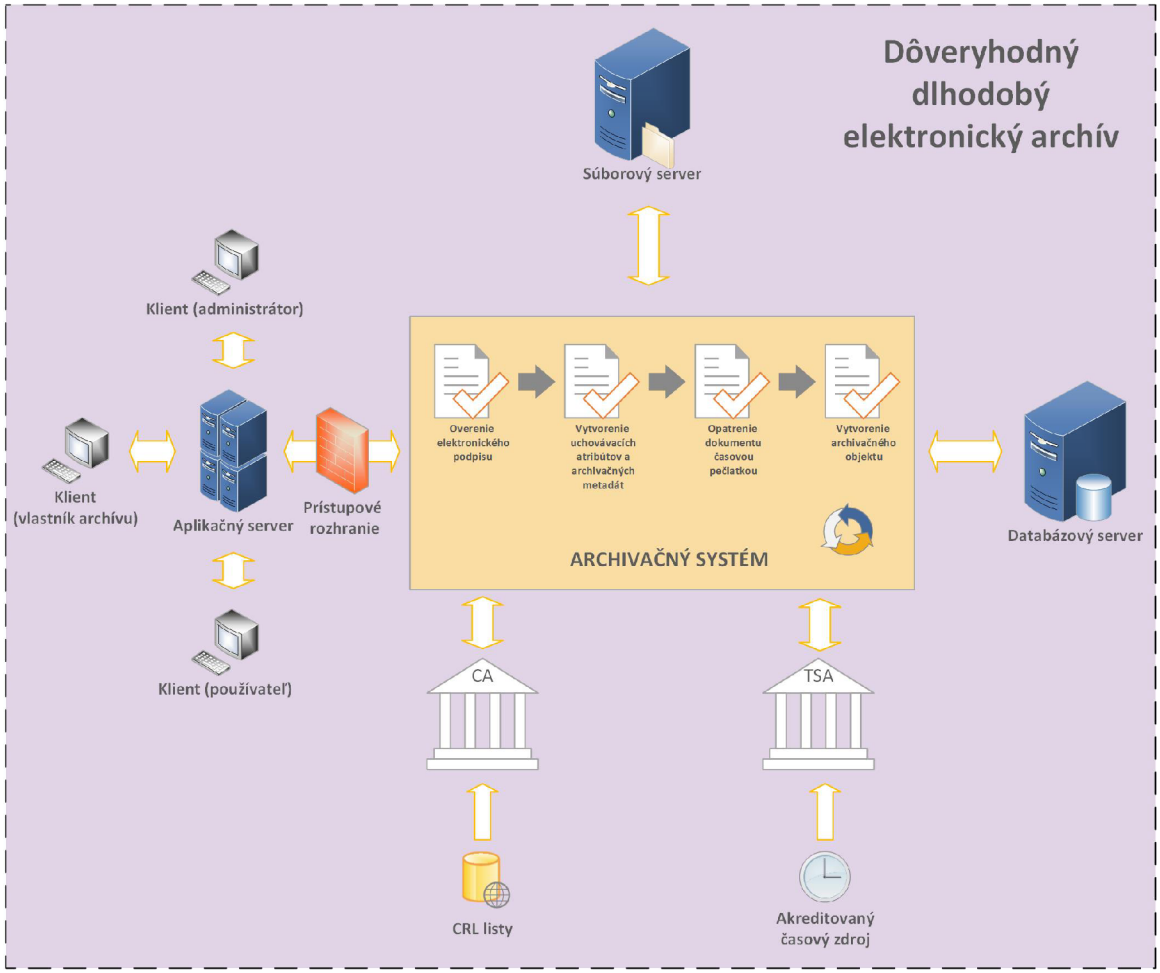
Medzi hlavné výhody eKeepru patrí[18]:

- schopnosť archivovať akýkoľvek druh elektronického dokumentu bez ohľadu na to, či je elektronický podpísaný alebo nie,
- dodržiavanie technických štandardov a legálnych požiadaviek,
- výkon, stabilita, spoľahlivosť a bezpečnosť,
- nezaťažuje klienta zbytočnými procesmi,
- dokáže prideliť jednu časovú pečiatku viacerým prijatým elektronickým dokumentom naraz,
- SOA architektúra.

Archivačné procesy riadi eKeeper prostredníctvom protokolu LTAP. Tento transportný protokol zabezpečuje odosielanie všetkých žiadostí a odpovedí súvisiacích s vytváraním uchovávacích atribútov. Výhodou tohto elektronického archívu je nezávislosť na hardwarovej a softwarovej platforme. Je určený hlavne pre rozsiahlejšie archívy – využíva linkovaný hash k opatreniu viacerých elektronických dokumentov časovými pečiatkami.

4 NÁVRH DÔVERYHODNÉHO DLHODOBÉHO ELEKTRONICKÉHO ARCHÍVU

Na základe využitých poznatkov z predchádzajúcich kapitol zobrazuje obr. 4.1 vypracovaný návrh dôveryhodného dlhodobého elektronického archívu. Navrhnutý elektronický archív je prispôsobený jednoduchému prístupu zo strany klienta a svojmu hlavnému účelu – dôveryhodnosti v dlhodobom časovom horizonte. „Srdcom“ navrhnutého dôveryhodného dlhodobého elektronického archívu je archivačný systém (obr. 4.3). Archivačný systém vykonáva procesy, vďaka ktorým je možné archivované elektronické dokumenty považovať za legálne platné a nespochybniteľné. Jeho hlavnou črtou je zabezpečenie integrity obsahu archivovaných dokumentov počas archivačnej doby pomocou dôkazových záznamov.



Obr. 4.1: Návrh dôveryhodného dlhodobého elektronického archívu

Elektronický archív je navrhnutý tak, že je možné archivovať elektronické dokumenty bez ohľadu na to, či sú elektronicky podpísané alebo nie. Vzhľadom k tomu, že elektronický podpísané dáta majú obmedzenú platnosť digitálneho certifikátu, je potrebné aby bol elektronický archív schopný overiť či je alebo nie je po dátume expirácie. K tomu využíva certifikáčnú autoritu. Po overení elektronického podpisu je k nemu nutné „pribaliť“ aj časovú pečiatku, ktorá jednoznačne potvrdzuje celistvosť obsahu dokumenov počas celého archivačného cyklu. Elektronický archív požiada autoritu archivačných pečiatok o vydanie časovej pečiatky. Po jej obdržaní ju zakomponuje pod hlavičkou dôkazových záznamov do štruktúry archivačného objektu ako súčasť uchovávacích atribútov.

Návrh rešpektuje legálne aspekty elektronickej archivácie a medzinárodné normy ETSI. Jeho prioritou je zabezpečiť:

1. **integritu obsahu** elektronických dokumentov,
2. **dlhodobú čitateľnosť** elektronických dokumentov,
3. **nepopierateľnosť a legálnu záväznosť** elektronických dokumentov.

4.1 Architektúra elektronického archívu

Architektúra navrhnutého riešenia je založená v duchu softwarovej architektúry pre poskytovanie služieb a funkcionality celému archívu – SOA (Service-oriented Architecture). Elektronický archív obsahuje podľa návrhu štyri hlavné komponenty:

1. **archivačný systém**,
2. **aplikačný server**,
3. **databázový server**,
4. **súborový server**.

Všetky servery komunikujú priamo s archivačným systémom, s ktorým su logicky spojené. Databázový a súborový server je zároveň fyzicky spojený s aplikačným serverom. Archivačný systém je implemetovaný ako aplikácia a jeho funkcionalitu zabezpečuje aplikačný server. Prístup do archívu povoľuje prístupové rozhranie na základe pridelených prístupových práv, tak aby bola zaručená nepopierateľnosť odosielateľa a prijímateľa.

Archivačný systém využíva k archivačnému procesu dôveryhodné autority – **certifikačnú autoritu** a **autoritu časových pečiatok**. Archivačný systém odošle požiadavku spolu s odtlačkom dokumentu na overienie elektronického podpisu v prípade certifikačnej autority a žiadosť o pridelenie časovej pečiatky k elektronickému podpisu v prípade autority časovej pečiatky. Autority sú nezávislé na elektronickom archíve a nikdy sa nedostanú do kontaktu s obsahom archivovaných elektronických dokumentov.

Klienti majú prístup k elektronickému archívu prostredníctvom prístupového rozhrania aplikačného servera. Jednotlivé práva prístupu sú rozdelené na tri skupiny podľa vzťahu klienta k archívu:

1. **vlastník archívu**,
2. **administrátor archívu**,
3. **používateľ archívu**.

Vlastník archívu (v modeli OAIS označený ako tvorca) by mal mať plné práva vo vzťahu ku správe archivovaných dát a manipulácii s archívom. Zároveň určuje, aké práva pridelí ďalším klientom. Z hľadiska bezpečnosti a zaistenia dôveryhodnosti elektronickému archívu je vhodné prideliť administrátorovi (v modeli OAIS označený ako správca) práva pre správu archivovaných dát, avšak bez prístupu k obsahu samotných dokumentov. To znamená, že by nemal prístup iba k súborovému serveru. V rámci správy archívu by teda pracoval iba s odtlačkami dokumentov – konkrétne s meta-dátami, elektronickými podpismi a časovými pečiatkami. Používateľ[1] (v modeli OAIS označený ako bádateľ) využíva elektronický archív pre získanie údajov z obsahu archivovaných dokumentov. Mal by mať preto prístup k súborovému serveru a databázovému serveru (aby mohol vyhľadávať dokumenty podľa kľúčových slov uvedených v meta-dátach). Používateľ však musí mať obmedzené právo zápisu a správy archivovaných dát – má len právo prístupu.

4.1.1 Aplikačný server

Aplikačný server predstavuje veľmi dôležitú súčasť navrhnutého dôveryhodného dlhodobého elektronického archívu. Predstavuje komponent, ktorý spravuje a riadi procesy a beh aplikácií v rámci elektronického archívu.

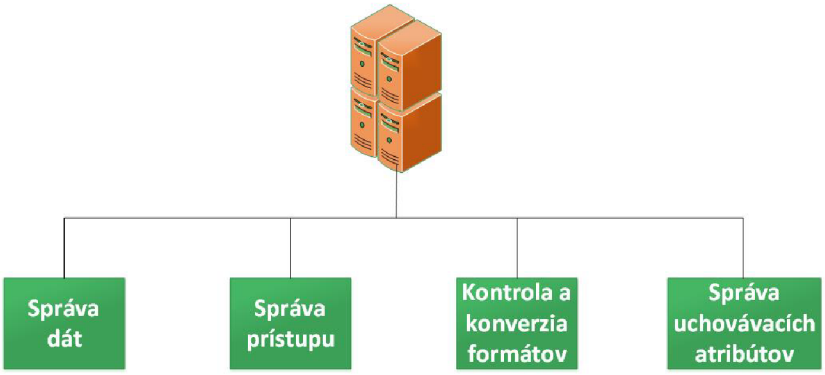
Úloha aplikačného servera je založená zo štyroch jeho hlavných činností (obr. 4.2):

1. správa dát,
2. správa prístupu,
3. kontrola a konverzia formátov,
4. správa uchovávacích atribútov.

Aplikačný server sprostredkováva spojenie a komunikáciu medzi klientom a elektronickým archívom. Dáta sú klientovi sprostredkované prostredníctvom aplikácie bežiacej priamo na aplikačnom serveri, alebo sa na server pripája cez webové rozhranie. Klient sa do elektronického archívu prihlasuje a autentizuje prostredníctvom zabezpečeného prístupu[2]. Kontrolu vstupu užívateľov do elektronického archívu má

[1] Používateľom môže byť napríklad zamestnanec, klient a podobne.

[2] Overenie identity žiadateľa o vstup do elektronického archívu sa môže vykonávať rôznymi spôsobmi, buď na základe určitej vedomosti (napr. heslo), prostriedkom (napr. autentizačná karta),biometrickým údajom...



Obr. 4.2: Činnosť aplikačného servera

na starosti vstupné rozhranie. Povolenie pridávania elektronických dokumentov do archívu (balík SIP v modeli OAIS) má iba vlastník archívu. Po prijatí aplikačným serverom je elektronický dokument (balík AIP v modeli OAIS) odoslaný na spracovanie do archivačného systému. Pomocou aplikačného servra môžu používatelia elektronického archívu vyhľadávať a pristupovať k jednotlivým dokumentom (balík DIP v modeli OAIS).

Aplikačný server má na starosti tiež definovať transakčnú logiku, čo znamená určiť v akej forme budú dáta v archíve sprostredkované. Výhodné je použiť šifrovaný prenos dát založený na asymetrickej kryptografii. Potvrdí sa tým nepopierateľnosť prijímateľa a odosielateľa. Ak príjemca pošle podpísané potvrdenie o prijatí dát, je zaistená nepopierateľnosť zodpovednosti i zo strany odosielateľa. Dáta sú v elektronickom archíve riadené a spravované aplikáciou bežiacou na aplikačnom serveri.

Elektronický archív je vzhľadom k požiadavke dôveryhodnosti primárne určený k uloženiu elektronických dokumentov s dôveryným a citlivým obsahom. Aby bola zaručená dôveryhodnosť a hlavne čitateľnosť v budúcnosti, musia byť elektronické dokumenty uložené v časovo stálych formátoch (kapitola 3.3.1). Elektronické dokumenty však môžu byť do archívu vkladané aj v iných formátoch, preto je úlohou aplikačného servera konvertovať dokumenty do podporovaných formátov. Ak sa nejedná o multimediálny obsah, je vhodné primárne voliť PDF formát.

Úlohou aplikačného servera je takisto zistiť a zromaždiť čo najviac informácií o archivovanom dokumente a predať ich archivačnému systému pre ďalie spracovanie. Už pri vkladaní elektronického dokumentu by mal byť klient vyzvaný na vyplnenie meta-dát.

4.1.2 Súborový server

Súborový server poskytuje v návrhu dôveryhodného dlhodobého elektronického archívu (obr. 4.1) centrálne úložisko . Jeho úlohou je ukladanie a centralizácia archivovaných dát s jednoduchým prístupom pre elektronický archív. Súborový systém má v archíve nezávislé postavenie, to znamená že pri nedostatku pamäťovej kapacity je možné pomocou migrácie premiestniť archivované dokumenty do novšieho a kapacitne väčšieho úložiska.

Súborový server býva implementovaný na fyzickom nosiči. V súčasnej dobe sa využíva pevný disk s kapacitou rádovo niekoľko TB[3]. Kedže poslaním elektronického archívu nie je ukladať obrovské množstvo elektronických dokumentov, ale ich pravidelná správa a používanie v určitých pravidelných cykloch, je takáto pamäťová kapacita plne postačujúca[4]. Z tohto dôvodu je omnoho podstatnejši parameter rýchlosti prísupu k dátam a rýchlosť zápisu dát, ktorá sa pohybuje okolo 10 000 otáčok za minútu. Najvýkonnejšie verzie využívajú vysokorýchlostné rozhranie SAS 6G pre čo najväčšiu priepustnosť dát. Formáty pevných diskov bývajú pre elektronické archívy zvyčajne 2,5", takže jeho umiestnenie je možné aj do rackovej skrine.

Pevný disk je energeticky nezávislé pamäťové médium, takže elektronický archív o svoje archivované dokumenty nepríde ani pri prerušení dodávky elektrickej energie. Dáta sú zapisované na pevný disk magnetickým záznamom.

Súborový server je spravovaný klientom (vlastníkom archívu) prostredníctvom aplikačného servera. V modeli OAIS predstavuje archivačné úložisko, pričom prijíma a odosiela archivačné balíky AIP. Uložené dáta su uchovávané v serveri až pokým klient nerozhodne o ich vymazaní. Vymazanie uložených dát môže byť nastavený aj klientom ako automatizovaný proces pri skartácii elektronických dokumentov. Práva zápisu alebo vymazávania dát sú definované vlastníkom archívu na aplikačnom serveri.

4.1.3 Databázový server

Databázový server slúži pre uloženie, modifikáciu a výber údajov v štruktúrovanej forme potrebných pre dôveryhodnú dlhodobú elektronickú archiváciu. Po vytvorení achivačného objektu sú okrem samotného elektronického dokumentu všetky entity (elektronický podpis, časová pečiatka, digitálny certifikát, meta-dáta) automaticky uložené do databázového servera. Navyše, pri vymazaní (skartácii) určitých dát, sa informácie o týchto súboroch zaznamenávaju práve do databázového servera. Pre

[3]V súčasnosti sa pamäťová kapacita súborových serverov pohybuje na úrovni 1 až 4 TB.

[4]Výber pamäťovej kapacity súborového servera závisi hlavne od množsta plánovaných elektronických dokumentov určených pre archiváciu a teda v zásade od veľkosti organizácie.

potreby klienta (napr. vyhľadávanie pomocou meta-dát) komunikuje s aplikačným serverom, ktorý prehľadáva dáta uložené v databázovom serveri.

Na databázovom serveri je spustená SQL aplikácia (Microsoft SQL, Oracle, MySQL...), ktorá slúži pre správu všetkých uložených dát. Databázové servery sú v súčasnosti založené na relačnom dátovom modeli. Jeho pamäťová kapacita nie je až taká podstatná[5], oveľa dôležitejšie je dodržať pravidlo, že operačná pamäť by nemala zaberať viac ako polovicu celkovej kapacity. Kapacita servera je teda závislá na výbere SQL aplikácie.

Fyzický prístup k serveru a jeho databázam zabezpečuje TCP/IP protokol. Databázový server je energeticky závislé médium a potrebuje neustále napájanie elektrickou energiou. Z tohto dôvodu je potrebné zaistiť vhodný a bezpečný spôsob zálohovania uložených dát. Vďaka zálohe bude potom možné v budúcnosti nahradiť databázový server novším.

Výhodou tohto riešenia je promptný prístup elektronického archívu k informáciam o archivovanom dokumente a zároveň spoľahlivé úložisko uchovávacích atribútov. Vďaka tomu, že elektronické dokumenty sú uložené separátne, je na jednej strane zaistená väčšia bezpečnosť archivovaných dát a na druhej rýchlosť vyhľadávania na základe filtračných požiadaviek[6].

4.2 Archivačný systém

Jadrom celého dôveryhodného dlhodobého elektronického archívu je **archivačný systém** (obr. 4.3). Ma za úlohu zabezpečiť integritu obsahu elektronického dokumentu, preukázať jeho časovú existenciu a legálnu nepopierateľnosť. Prináša riešenie pre vyhľadanie, vytvorenie a uchovanie dôkazových záznamov vložených elektronických dát, potrebných pre dôveryhodnosť v dlhodobom časovom období. Archivačný systém kombinuje techniky pre uloženie dát a ich správu, vytvorenie archivačného objektu spolu s uchovávacími atribútmi (tak ako to bolo popísané v kapitole 3.1), a predstavuje dôležitú funkčnú a technologickú zložku elektronického archívu.

Kľúčovou funkciou archivačného systému je prijatie a následné spracovanie vložených elektronických dokumentov, ktoré môžu byť v zásade v dvoch podobách:

- elektronicky nepodpísané,
- elektronicky podpísané.

Takisto sa môžu obidve varianty predstaviť v zašifrovanej forme (v určitých utajovaných prípadoch). To, či dokument obsahuje alebo neobsahuje elektronický podpis

[5] Odporúča sa však minimálne 10 GB voľného priestoru pre dáta.

[6] Nie je potrebné dodatočne prehľadávať elektronický dokument, čo je časovo náročnejšie.

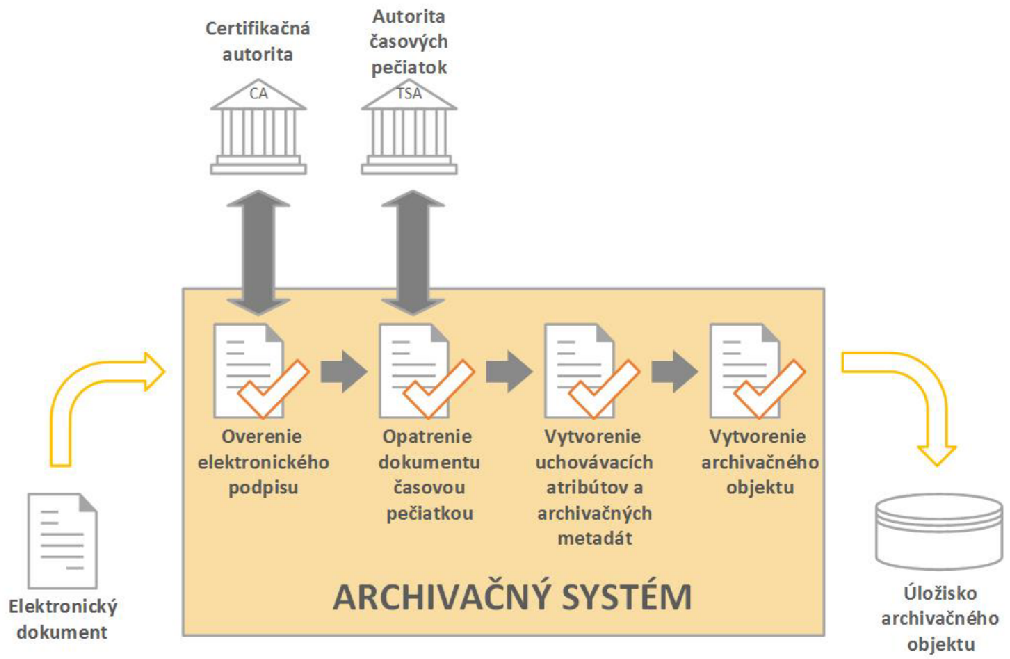
má zásadný vplyv na proces archivácie. V prípade elektronicky podpísaného dokumentu musí byť pri vstupe do archivačného systému najprv overený elektronický podpis (konkrétne či je jeho digitálny certifikát stále platný). Ak archivovaný dokument neobsahuje elektronický podpis, archivačný systém spracuje len meta-dáta dokumentu. Z hľadiska archivačného procesu, je preto jednoduchšie spracovať nepodpísaný dokument.

Archivačný systém môže byť implementovaný na serveri podporujúcom archivačný proces.

4.2.1 Archivačný proces

Návrh archivačného systému je podriadený a prispôsobený svojmu účelu. Ako už bolo spomenuté, takýto systém aplikuje mechanizmy pre dôveryhodnú dlhodobú archiváciu. Tieto mechanizmy majú určitú následnosť, ktorú demonštruje **archivačný proces** (obr. 4.3) a sú rozdelené do štyroch základných krokov:

1. **overenie elektronického podpisu** vloženého dokumentu,
2. **opatrenie dokumentu časovou pečiatkou**,
3. **vytvorenie uchovávacích atribútov a archivačných metadát**,
4. **vytvorenie archivačného objektu**.



Obr. 4.3: Proces archivácie elektronického dokumentu v archivačnom systéme

Prvým krokom, ktorý musí archivačný systém vykonať, je kontrola elektronického podpisu (tento krok sa preskakuje, ak nie je dokument elektronicky podpísaný). Kontrola elektronického podpisu prebieha tak, ako to bolo popísané v kapitole 2.1. Certifikačná autorita má prístup do databázy CRL listov[7], ktoré sú zverejnené na webserveri a sú voľne dostupné. Tak dokáže overiť, či daný certifikát je alebo nie je platný. Existuje aj možnosť využiť internetový protokol OCSP pre získanie overenia X.509 digitálneho certifikátu. V Českej republike tento protokol poskytuje napríklad Česká pošta v rámci služby PostSignum.

Kedže samotný elektronický podpis nevypovedá o časovej existencii elektronického dokumentu (zaznamenáva iba čas kedy došlo k podpisu dokumentu), je potrebné bezprostredne po podpise pripojiť dôkaz o existencii dokumentu v konkrétnom čase. Jednou z entít uchovávacích záznamov, ktorá ma za úlohu potvrdiť existenciu dokumentu v čase, je dôkazový záznam. Najvhodnejším dôkazovým záznamom z hľadiska dlhodobej elektronickej archivácie je opatriť elektronický podpis časovou pečiatkou. Jej platnosť však môže po čase vypršať, preto je potrebné pečiatky obnovovať. Existuje aj možnosť využiť ďalšiu paralelnú autoritu časových pečiatok ako zálohu (jej časová pečiatka môže mať dlhšiu dobu expirácie). V praxi sa však využíva jednoduchšie riešenie, aj keď časovo náročnejšie – po vypršaní časovej pečiatky sa znovu odošle odtlačok dokumentu a po prijatí novej pečiatky sa pripojí k elektronickému dokumentu. Proces vytvorenia časovej pečiatky prebieha presne tak, ako to bolo definované v kapitole 2.3.

Dôveryhodná archivácia elektronických dát je proces neustáleho vytvárania a priebežnej údržby uchovávacích atribútov v štruktúre archivačného objektu. Tie sú v archíve počas celého archivačného cyklu. Tvorba uchovávacích atribútov nasleduje po overení elektronického podpisu a opatrení časovou pečiatkou a môže zabrať určitý čas. Z toho dôvodu je potrebné definovať kedy nastáva začiatok archivácie – či od okamžiku vstupu dát do archivačného systému alebo až po vytvorení dôkazových záznamov. Z hľadiska dôveryhodnosti a legálnej nepopierateľnosti elektronických dokumentov by archivačná doba mala začať až po vygenerovaní uchovávacích atribútov. Preto by mal archivačný systém generovať automatickú odpoveď s časom začiatku archivačného cyklu, ktorú pošle klientovi. V rámci uchovávacích atribútov je rovnako podstatné vytvoriť aj archivačné meta-dáta. Tie by mali byť generované na základe požiadavky vlastníka elektronického archívu. Za archivačné meta-dáta je možné považovať napríklad tvorcu dokumentu, dátum začatia archivačnej doby alebo pôvod dokumentu. Ich úlohou je pomôcť zabezpečiť vyššiu dôveryhodnosť a poskytnúť archivačnému systému čo najviac informácii o archivovanom dokumente. Logickou

[7]CRL (Certificate Revocation List) je zoznam zrušených certifikátov, ktorým už bola ukončená platnosť. Tento zoznam je pravidelne aktualizovaný, zvyčajne v 12-hodinovom intervale.

súčasťou uchovávacích atribútov je aj vygenerovaná časová pečiatka a v rámci doplnkových dát aj digitálny certifikát.

Posledný krok archivačného procesu spočíva vo vytvorení archivačného objektu na logickej úrovni. V štruktúre archivačného objektu by mal byť logicky spojený archivovaný elektronický dokument spolu s entitami:

- elektronický podpis,
- meta-dáta dokumentu[8],
- uchovávacie atribúty.

Takéto logické spojenie jednotlivých entít s archivovaným dokumentom je výhodné pre správu archivovaných elektronických dokumentov. Pri vyhľadávaní je pre klienta prostredníctvom prístupového systému omnoho prehľadnejšie a jednoduchšie nájsť potrebné informácie o archivovanom dokumente. Na druhej strane by elektronické dokumenty nemali byť uložené spolu s entitami archivačného objektu, pretože sú na ich uloženie kladené iné požiadavky.

4.2.2 Požiadavky na archivačný systém

V závislosti od použitia elektronického archívu na konkrétny účel, je potrebné definovať požiadavky, ktoré sú naň kladené. Systém podporujúci dôveryhodnú a dlhodobú elektronickú archiváciu musí povoliť používateľovi[9] nasledujúce základné operácie[2]:

- vložiť dáta k archivácii,
- vyhľadať archivačné dáta,
- vymazať archivačné dáta.

Zároveň musí archivačný systém z pohľadu správy elektronického archívu umožniť používateľovi povoliť prístup k operáciam ako:

- špecifikovať predpokladanú archivačnú dobu vložených dát,
- predĺžiť alebo skrátiť predpokladanú archivačnú dobu archivovaných dát,
- špecifikovať podľa seba meta-dáta spojené s archivovanými dátami,
- do istej miery špecifikovať postup ako zaobchádzať s vloženými dátami.

Navrhnutý archivačný systém musí byť schopný poskytnuť legitímny záznam[10], ktorý bude môcť byť použitý k preukázaniu celistvosti archivovaných dokumentov od momentu vloženia až po moment expirácie (konca archivačnej doby). To sa dá dosiahnuť

[8]Meta-dáta by mali byť podobne ako archivačné meta-dáta generované automaticky archivačným systémom podľa požiadavky vlastníka archívu s dôrazom na jednoduchšie vyhľadávanie archivovaných elektronických dokumentov pre používateľov archívu.

[9]Používateľom je v tomto prípade myslený vlastník elektronického archívu. Jednotlivé práva pre vlastníka, administrátora a ostatných užívateľov môžu byť však prispôsobené konkrétnemu archívu.

[10]Záznam musí byť legitímny, preto aby mohol slúžiť ako jednoznačný dôkaz aj v prípadnom súdnom konaní.

pomocou už spomenutých dôkazových záznamov v štruktúre archivačného objektu. Dôkazové záznamy udržiavajú dlhodobú nepopierateľnosť existencie archivovaných dát a demonštrujú ich integritu od konkrétneho časového okamžiku (zvyčajne sa jedná o vloženie dát do archivačného systému). K tomu potrebujú dostatok informácii získaných z archivovaných elektronických dokumentov. Riešenie vytvárania dôkazových záznamov musí byť navrhnuté tak, aby každá modifikácia v elektronickom dokumente bola detekovateľná, a to aj vrátane zmien vykonaných administrátorom archivačného systému.

Logickou súčasťou archivačného systému musí byť aj **archivačná politika**. V rámci nej je potrebné definovať už spomenuté požiadavky a nároky, ale aj napríklad určiť:

- ako zaobchádzať s dátami po ich expirácii,
- typy podporovaných formátov pre uloženie,
- typ dôkazových záznamov (napríklad časová pečiatka,)
- autoritu časových pečiatok, ktorá bude počas archivačného procesu použitá,
- aké meta-dáta by mal archivačný systém automaticky generovať,
- ako by mal prebiehať skartačný proces.

Archivačná politika by mala takisto disponovať informáciami, kto má právo vkladať, vyhľadávať a spravovať elektronické dokumenty. Úlohou archivačného systému však nie je dezignovať takéto úkony, ale ich len aplikovať v rámci archivačného procesu. Implementáciou mechanizmov v kontexte archivačnej politiky by sa mal zaoberať aplikačný server.

4.3 Výhody navrhnutého riešenia

Navrhnuté riešenie elektronického archívu je prispôsobené dvom hlavným požiadavkam – dôveryhodnosti a dlhodobému uchovaniu elektronických dát. Archivačný systém sa snaží získať čo najviac informácií o elektronickom dokumente. Preto sa predpokladá hlavne archivácia elektronicky podpísaných dokumentov, avšak je takisto možné archivovať aj elektronicky nepodpísané dokumenty.

Výsledný model (obr. 4.1) je zámerne rozdelený do viacerých celkov, aby pri modernizácii alebo údržbe bolo možné bezpečne modifikovať, resp. nahradiť konkrétny komponent v elektronickom archíve. Riešenie prináša vlastníkovi elektronického archívu rôzne možnosti ako hardwarovo a softwarovo vybaviť jednotlivé servery podľa jeho vlastných potrieb a požiadaviek.

Samozrejmosťou je zohľadnenie všetkých legislatívnych noriem týkajúcich sa elektronickej archivácie a manipulácie s elektronickými dokumentmi. Pri vytváraní návrhu slúžil ako predloha referenčný model OAIS.

Vďaka použitiu aplikačného servara môže klient pristupovať k elektronickému archívu aj cez vzdialený prístup (napríklad cez webové rozhranie), pričom je prioritou zabezpečený prístup. Vlastník archívu si môže sám definovať prístupové práva jednotlivých užívateľov.

Riešenie je vhodné aj pre rozsiahlejšie elektronické archívy vďaka použitiu viacerých serverov s voliteľnými hardwarovými parametrami. V prípade potreby je bezproblémová modernizácia alebo rozšírenie pamäťovej kapacity. Takisto odpadá závislosť na konkrétnom operačnom systéme.

5 ZÁVER

Bakalárska práca sa zameriava hlavne na elektronickú archiváciu digitalizovaných dát. Vychádza z najnovších trendov v oblasti poskytovania služieb prostredníctvom elektronických dokumentov. Pri elektronickej komunikácii je najpodstatnejšia otázka bezpečnosti dát a preto sa sústredi hlavne na zabezpečenie dokumentov v elektronickej forme pomocou kryptografických systémov a metód. Ochrana dát pred potencionálnymi hrozbami a útokmi na obsah elektronických dokumentov je eliminovaná vďaka mechanizmom, ktoré pracujú práve na princípoch symetrickej a asymetrickej kryptografie. Podstatnou súčasťou sú aj právne aspekty, ktoré definujú a usmerňujú ako majú byť elektronické dáta spravované a archivované.

Hlavnou úlohou bakalárskej práce bolo zhrnúť a zanalyzovať problematiku dôveryhodnej elektronickej archivácie najmä v dlhodobom časovom horizonte. Elektronická archivácia je z hľadiska používania a vývoja ešte stále vo svojich začiatkoch a až do nedávnej doby bola limitovaná legislatívnymi obmedzeniami. Po prijatí príslušných zákonov a noriem v Českej republike, je možné definovať požiadavky a nároky na jednotlivé technické riešenia elektronických archívov. Tie sa líšia hlavne v závislosti na plánovanej dobe archivácie. Nakoľko sa v praxi vo väčšine prípadov archivujú elektronicky podpísané dokumenty, je je nevyhnutné zabezpečiť jeho ochranu voči zneužitiu. Problémom pri dlhodobej archivácii je však práve elektronický podpis, ktorý má obmedzenú platnosť. Tá musí byť periodicky predlžovaná pomocou mechanizmu ako je elektronická časová pečiatka, ktorého funkcii sa práca podrobnejšie venuje.

Elektronická archivácia je proces, ktorý musí byť presne definovaný jeho vlastníkom, resp. musí byť prispôsobený svojej funkcii. Z časového hľadiska uloženia dát sa jednotlivé riešenia elektronických archívov líšia, pretože vyžadujú iné nároky. Pri dôveryhodnej a dlhodobej archivácii je potrebné zabezpečiť hlavné kritéria ako celistvosť obsahu, dlhodobú čitateľnosť a právnu záväznosť archivovaných dokumentov. Preto je formulovaný pojem archivačný objekt, ktorý predstavuje logickú štruktúru, v ktorej sa nachádzajú uchovávacie atribúty. Práca definuje referenčný model OAIS považovaný sa štandard v tejto oblasti a existujúce riešenia, ktoré sa s touto problematikou dokázali úspešne vysporiadať.

Výstupom bakalárskej práce je návrhnuté riešenie dôveryhodného dlhodobého elektronického archívu. Tento návrh akceptuje všetky zavedené štandardy a legislatívne požiadavky v oblasti elektronickej archivácie. Súčasťou návrhu je aj popis architektúry, ktorá sa skladá z viacerých komponentov a je navrhnutá v zmysle modernej sieťovej architektúry. Komunikácia medzi jednotlivými komponentmi a prístup zo strany klienta je ošetrený v rámci popisu jednotlivých súčasti. Navrhnutý archív spĺňa všetky kritéria pre malé aj veľké archívy a môže byť modifikovaný podľa

potrieb vlastníka alebo užíateľov. V neposlednom rade je aj predstavený archivačný systém, ktorý má na starosti prevádzku celého elektronického archívu. Archivačný proces prebiehajúci v tomto systéme je podrobne popísaný, s tým že jeho činnosť je zameraná na vytáranie uchovávacích atribútov, kontrolu platnosti elektronického podpisu a pridelovanie časových pečiatok, pričom komunikuje s príslušnými autoritami. Nakoniec sú zhrnuté všetky výhody, ktoré navrhnuté riešenie prináša.

LITERATÚRA

[1] Adobe Systems Incorporated. *The AdES family of standards: CAdES, XAdES and PAdES* [online]. 2009, [cit. 2013]. Dostupné z URL: <http://blogs.adobe.com/security/91014620_eusig_wp_ue.pdf>

[2] BLAŽIČ, A.J.; KLOBUČAR, T.; JERMAN, B.D. *Long-term trusted preservation service using service interaction protocol and evidence records* [online]. Computer Standards & Interfaces 29 (2007) 398-412, July 2006. [cit. 9. 5. 2014]. Dostupné z URL: <http://www.sciencedirect.com/science/article/pii/S0920548906000778#>.

[3] BLAŽIČ, A.J. *Long term trusted archive services* [online]. Proceedings of the First International Conference on the Digital Society, 2007. [cit. 10. 5. 2014]. Dostupné z URL: <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4063790&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F4063752%2F4063753%2F04063790.pdf%3Farnumber%3D4063790>.

[4] ČESKÁ REPUBLIKA: Vyhláška č. 191 ze dne 23. června 2009 o podrobnostech výkonu spisové služby. In *Sbírka zákonů České republiky, 2009*. Dostupné z URL:<http://www.mvcr.cz/soubor/archivnictvi-a-spisova-sluzba-dokumenty-vyhlaska-o-spisove-sluzbe-pdf.aspx>

[5] ČESKÁ REPUBLIKA: Zákon č. 227/2000 Sb., ze dne 29. června 2000 o elektronickém podpisu a změně některých dalších zákonů. In *Sbírka zákonů České republiky , 2000*. Dostupné z URL: <http://http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>

[6] ČESKÁ REPUBLIKA: Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, jak vyplývá ze změn provedených zákonem č. 413/2005 Sb., zákonem č. 444/2005 Sb., zákonem č. 112/2006 Sb., zákonem č. 181/2007 Sb., zákonem č. 296/2007 Sb., zákonem č. 32/2008 Sb., zákonem č. 190/2009 Sb., zákonem č. 227/2009 Sb., zákonem č. 424/2010 Sb. a zákonem č. 167/2012 Sb. In *Sbírka zákonů České republiky, 2004*. Dostupné z URL: <http://www.mvcr.cz/soubor/zakon-c-499-2004sb-ve-zneni-zakona-c-167-2012sb-pdf.aspx>

[7] *Digitálne certifikáty* [online]. Advanced, 2005. [cit. 4. 12. 2013]. Dostupné z URL: <http://eshop.advanced.sk/instantssl/manual/page4.aspx>.

[8] DOLEŽAL, D. *Co to je digitálni certifikát*. In: www.interval.cz [online]. ZONER sotware. 2003, [cit. 1. 12. 2013]. Dostupné z URL: <http://www.interval.cz/clanky/co-to-je-digitalni-certifikat/#zacatek-clanku>.

[9] DOSTÁLEK, L.; VOHNOUTOVÁ, M.; KNOTEK, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu* [online]. 2001, poslední aktualizace 11. 11. 2004. [cit. 17. 2. 2005]. Dostupné z URL:

[10] *eKeeper product brochure* [online]. SETCCE, 2010. [cit. 19. 5. 2014]. Dostupné z URL: <http://www.setcce.si/images/download/eKeeper_brochure_eng.pdf>.

[11] HÖNIG, P. *Důvěryhodný elektronický archiv pro dlouhodobou archivaci, požadavky a jejich řešení*. Liberec:AKP 2007, 16.- 17. 5. 2007. 11. ročník semináru.

[12] HUBLER, V. *Budúcnosť archivácie je digitálna.* In: IT NEWS [online]. PC Revue, 2012. [cit. 31. 12. 2013]. Dostupné z URL: <http://www.itnews.sk/2012-06-01/c149133-buducnost-archivacie-je-digitalna>.

[13] KREJČÍ, R. *PDF/A – nový formát pro archivaci a publikování nastupuje* In: Svět tisku [online]. Vydavatelství Svět tisku, 2006. [cit. 12. 5. 2014]. Dostupné z URL: <http://www.svettisku.cz/buxus/generate_page.php?page_id=2969&buxus_svettisku=0df7e4d387774e6542462440d24111e2>.

[14] KUNSTOVÁ, R. *Efektivní správa dokumentů*. Praha: Grada, 2009. 204s. ISBN 978-80-247-3257-2.

[15] LECHNER, T. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013. 256s. ISBN 978-80-87576-41-0.

[16] PIPER, F., MURPHY, S. *Kryptografie*. Praha: Dokořán, 2006. 157s. ISBN 80-7363-074-5.

[17] PODSTRELENEC, J. *DIP: Elektronická archivácia papierových dokumentov.* In: Trend [online]. Trend Holding, 1998. [cit. 31. 12. 2013]. Dostupné z URL: <http://www.etrend.sk/trend-archiv/rok-/cislo-Apríl/dip-elektronicka-archivacia-papierovych-dokumentov.html>.

[18] *SETCCE* [online]. SETCCE, 2010. [cit. 19. 5. 2014]. Dostupné z URL: <http://www.setcce.si/item.php?catId=14&itemId=138&section=4&lang=eng>.

[19] *Software602* [online]. Software602, a.s., 1991. [cit. 26. 5. 2014]. Dostupné z URL: <http://www.602.cz/produkty/digitalni-archiv-elektronicka-spisovna>.

[20] VRABEC, V. *Elektronické časové razítko, doplněk elektronického podpisu.* In: www.interval.cz [online]. ZONER sotware. 2003, [cit. 11. 12. 2013]. Dostupné z URL: <http://www.interval.cz/clanky/elektronicke-casove-razitko-doplnek-elektronickeho-podpisu>.

[21] *White Paper: Trusted electronic archive* [online]. SETCCE, 2005. [cit. 19. 5. 2014]. Dostupné z URL:<http://www.setcce.si/images/download/Trusted_Electronic_Archives_-_White_Paper.pdf>.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

AIP	Archive Information Package
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DEA	Dôveryhodný elektronický archív
DIP	Dissemination Information Package
DMS	Document Management System
ECM	Enterprise Content Management
ETSI	European Telecommunications Standards Institute
GB	GigaByte
ISO	International Organization for Standardization
LTAP	Long Term Archive Protocol
OAIS	Open Archival Information System
OCSP	Online Certificate Status Protocol
PDF/A	Portable Document Format/Archive
PDF	Portable Document Format
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adlemanov algoritmus
SHA	Secure Hash Algorithm
SIP	Submission Information Package
SOA	Service Oriented Architecture
TAA	Trusted archive authority
TB	TeraByte
TSA	Time Stamp Authority
URL	Uniform Resource Locator