# Elektronická správa dokumentů společnosti AEV spol. s r.o., Kroměříž

Electronic document management system in AEV spol. s r.o., Kromeriz

Bc. Jiří Kubín

Diplomová práce
2007



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2006/2007

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Jiří KUBÍN** |
| Studijní program: | **N 3902 Inženýrská informatika** |
| Studijní obor: | **Informační technologie** |
| Téma práce: | **Elektronická správa dokumentů společnosti AEV spol. s r.o., Kroměříž** |

Zásady pro vypracování:

**1.Vyhledejte vhodné zdroje řešící problematiku elektronické správy dokumentů.**
**2.Analyzujte současné technologické možnosti správy dokumentů.**
**3.Navrhněte vhodné řešení pro firmu AEV s r o Kroměříž a proveďte implementaci.**
**4.Vyhodnoťte úspěšnost řešení a definujte silná a slabá místa zvoleného řešení.**

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

**1.Jašek, R.: Informační a datová bezpečnost. Skriptum UTB ve Zlíně, Zlín 2006, ISBN 80-7318-456-7**
**2.Doseděl, T.: Počítačová bezpečnost a ochrana dat. Computer Press 2004, ISBN 80-251-0106-1**
**3.PGP: Pretty Good Privacy. Computer Press 1998, ISBN 80-7226-054-5**

Vedoucí diplomové práce: **Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání diplomové práce: **13. února 2007**

Termín odevzdání diplomové práce: **28. května 2007**

Ve Zlíně dne 13. února 2007

L.S.

prof. Ing. Vladimír Vašek, CSc.
*děkan*

doc. Ing. Ivan Zelinka, Ph.D.
*ředitel ústavu*

## ABSTRAKT

V této práci se zabývám problematikou správy dokumentů – Document Management System (DMS) a jejím zavedením do praxe.

Teoretická část je zaměřena na úkoly elektronické správy dokumentů, její funkce, bezpečnost, elektronický podpis, archivaci apod.

V praktické části jde o analýzu možností DMS, rozbor situace ve firmě, návrh konkrétního řešení, implementaci a vyhodnocení.

Úkolem práce je tedy návrh vhodného řešení elektronické správy dokumentů, jejich evidenci a bezpečnou manipulaci a archivaci v rámci konkrétní středně velké výrobní firmy.


Klíčová slova: správa dokumentů, bezpečnost dat, archivace dokumentů, elektronický dokument, šifrování, elektronický podpis, autorizace, certifikát, veřejný klíč, soukromý klíč, workflow.


## ABSTRACT

This dissertation concerns problems with Document Management System (DMS) and how this can be put into practice.

The theoretical part concentrates on tasks of an electronic document management, its purpose, safeness, electronic signature, archiving and so on.

The practical part contains analysis of DMS possibilities, analysis of the company situation, concrete solution recommendation, implementation and interpretation.

The main task was to suggest a proper solution for an electronic document management, its document registration and a safe manipulation and archiving in a concrete medium-size manufacturing company.


Keywords: document management, data safeness, data archiving, electronic document, encryption, electronic signature, authorization, certificate, public key, private key, workflow.

*Poděkování:*

Na tomto místě chci poděkovat vedoucímu diplomové práce panu doc. Mgr. Romanovi Jaškovi, Ph.D. za odborné vedení, připomínky a konzultace při řešení této práce.

Dále děkuji panu Ing. Zdeňkovi Hasalovi z firmy AEV Kroměříž za podnětné rady, konzultace a připomínky ke konkrétnímu řešení ve firmě a za poskytnutí potřebných informací o firmě AEV.

*Motto:*

„Není důležité motto, nýbrž činy...“

Prohlašuji, že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně 28. května 2007

Podpis diplomanta

# OBSAH

**ÚVOD** ..... **11**

**I TEORETICKÁ ČÁST** ..... **12**

**1 SPRÁVA DOKUMENTŮ** ..... **13**

1.1 HLAVNÍ ODLIŠNOSTI DIGITÁLNÍHO A ANALOGOVÉHO DOKUMENTU ..... 13

1.2 POŽADAVKY NA SYSTÉM SPRÁVY DOKUMENTŮ ..... 14

1.3 HLAVNÍ FUNKCE SPRÁVY DOKUMENTŮ ..... 14

1.4 WORKFLOW ..... 14

1.5 DALŠÍ FUNKCE ..... 15

1.6 PŘÍNOS SYSTÉMU PRO SPRÁVU DOKUMENTŮ ..... 15

**2 BEZPEČNOST DAT** ..... **17**

2.1 HROZBY ..... 17

2.2 MOŽNOSTI OCHRANY ..... 18

2.2.1 Fyzická ochrana ..... 18
2.2.2 Přístupová práva a autentizace ..... 18
2.2.3 Technické zabezpečení ..... 19
2.2.3.1 Zálohování ..... 20
2.2.3.2 Ochrana před útoky ..... 20
2.2.3.3 Šifrování dat ..... 24

**3 KRYPTOLOGIE** ..... **25**

3.1 KRYPTOGRAFIE ..... 25

3.1.1 Základní pojmy ..... 25
3.1.2 Kryptografický algoritmus ..... 25
3.1.3 Šifrovací klíč ..... 26
3.1.4 Symetrická kryptografie ..... 26
3.1.5 Asymetrický kryptografie ..... 27
3.1.5.1 Klíčový pár ..... 28
3.1.5.2 Postup šifrování a dešifrování ..... 28
3.1.6 Hybridní kryptografie ..... 29
3.1.7 Proudové a blokové šifry ..... 29

3.2 KRYPTOANALÝZA ..... 29

3.2.1 Luštění se znalostí ..... 30
3.2.2 Útok hrubou silou ..... 30

**4 ELEKTRONICKÝ PODPIS** ..... **31**

4.1 ZÁKLADNÍ TERMINOLOGIE ..... 31

4.1.1 Certifikační autorita ..... 32
4.1.2 Certifikát ..... 32
4.1.3 Symetrická kryptografie ..... 32
4.1.4 Asymetrická kryptografie ..... 32
4.1.4.1 Klíčový pár ..... 32
4.1.5 Hash funkce a hodnota ..... 33

4.1.6 Časové razítko ..... 34
4.2 STRUKTURA ELEKTRONICKÉHO PODPISU ..... 34
4.3 ZÍSKÁNÍ ELEKTRONICKÉHO PODPISU ..... 35
4.4 ZARUČENÝ ELEKTRONICKÝ PODPIS A ELEKTRONICKÁ ZNAČKA ..... 35
4.5 VARIANTY POUŽITÍ ELEKTRONICKÉHO PODPISU ..... 35
4.6 AKREDITOVANÉ CERTIFIKAČNÍ AUTORITY ..... 36
**5 DLOUHODOBÉ UKLÁDÁNÍ A ARCHIVACE ..... 37**
5.1 NOSIČE DAT ..... 37
5.2 ČITELNOST NOSIČŮ ..... 37
5.3 INTERPRETOVATELNOST DAT ..... 37
5.3.1 Otevřené formáty ..... 38
5.3.2 Přeformátování dat ..... 38
5.4 PRÁVNÍ VALIDITA ..... 38
**6 EXISTUJÍCÍ ŘEŠENÍ ..... 39**
6.1 PGP ..... 39
6.1.1 PGP – Pretty Good Privacy ..... 39
6.1.2 Princip šifry PGP ..... 40
6.1.3 Elektronické podpisy v PGP ..... 40
6.1.4 Správa klíčů v PGP ..... 40
6.1.5 Správce veřejných klíčů v PGP ..... 41
6.1.6 Šifrování pošty v PGP ..... 42
6.1.7 Kdy šifrovat a kdy podepisovat poštu ..... 42
6.2 ADOBE ACROBAT ..... 42
6.3 VERZE ADOBE ACROBAT ..... 43
6.4 JAK ELEKTRONICKÝ PODPIS V PDF FUNGUJE ..... 43
6.4.1 Acrobat Self-Sign Security ..... 43
6.4.2 Direct-trust ..... 43
**II PRAKTICKÁ ČÁST ..... 45**
**7 CHARAKTERISTIKA FIRMY AEV ..... 46**
7.1 PŘEDMĚT PODNIKÁNÍ ..... 46
7.2 ČLENĚNÍ FIRMY A POČET ZAMĚSTNANCŮ ..... 46
7.3 CERTIFIKÁTY A OSVĚDČENÍ ..... 46
**8 SOUČASNÝ STAV SPRÁVY DOKUMENTŮ ..... 48**
8.1 POČÍTAČOVÁ SÍŤ V AEV ..... 48
8.1.1 Použité síťové prvky ..... 48
8.1.2 Umístění a fyzická ochrana ..... 49
8.2 ROUTER ..... 49
8.3 MS WINDOWS 2000 SERVER ..... 50
8.3.1 Síť Microsoft Windows ..... 50

8.3.2 Cominfo – docházkový systém ..... 51
8.4 NOVELL SERVER ..... 51
8.4.1 Síť Novell NetWare ..... 52
8.4.1.1 Struktura ..... 52
8.4.1.2 Nastavení práv ..... 52
8.4.1.3 Přihlašování do sítě Novell NetWare ..... 54
8.4.1.4 Mapování ..... 55
8.5 STANICE PC A NOTEBOOKY ..... 56
8.5.1 Kancelářské počítače ..... 56
8.5.2 Počítače ve výrobě ..... 56
8.5.3 Přenosné počítače notebooky ..... 57
8.6 POŠTOVNÍ SERVER ..... 57
8.7 TYPY POUŽÍVANÝCH DOKUMENTŮ ..... 58
8.8 ZÁLOHOVÁNÍ DOKUMENTŮ ..... 58
8.8.1 Denní záloha dokumentů ..... 59
8.8.2 Měsíční záloha dokumentů ..... 59
8.9 VYHODNOCENÍ STAVU ..... 59
8.10 DOPORUČENÍ ..... 60
**9 POŽADAVKY NA SPRÁVU DOKUMENTŮ V AEV ..... 61**
**10 MOŽNOSTI ŘEŠENÍ ..... 62**
10.1 SOVA SYSTEMS ..... 62
10.1.1 Automanager TeamWork ..... 62
10.1.2 Automanager Meridian ..... 63
10.1.3 DOCLINE ..... 64
10.1.4 xWORK ..... 64
10.2 PRINTSOFT ..... 66
10.3 XANADU ..... 67
10.3.1 iPROJECT ..... 67
10.3.2 Autodesk Vault ..... 67
10.3.3 DWF ..... 67
10.3.4 CAD Vault ..... 68
10.3.5 Automanager TeamWork ..... 68
10.3.6 CaD Manager ..... 68
10.3.7 Motiva eChange ..... 69
10.4 AUTOCONT ..... 69
10.4.1 ECM FileNET ..... 69
10.5 INFOS 2001 ..... 70
10.6 PGP – PRETTY GOOD PRIVACY ..... 71
10.6.1 PGP Desktop produkty s WholeDisk ..... 71
10.6.2 Nástroje PGP Desktop 9.x Professional ..... 71
10.6.2.1 PGP Mail ..... 71
10.6.2.2 PGP Virtual Disk ..... 71
10.6.2.3 PGP Whole Disk ..... 72

10.6.2.4 PGP ZIP ..... 72
10.6.2.5 PGP Shred ..... 72
10.6.3 Vlastnosti produktu PGP ..... 72
10.6.4 PGP Desktop - Technické údaje ..... 72
10.6.5 PGP Universal – komplexní zabezpečení emailů a disků ..... 73
10.6.6 Výhody použití PGP Desktop Professional ..... 73
10.6.7 Distribuce PGP ..... 74
10.7 ZÁLOHOVÁNÍ DAT ..... 74
10.7.1 Magnetické pásky ..... 74
10.7.2 LTO pásková technologie ..... 75
**11 NÁVRH ŘEŠENÍ ..... 76**
11.1 ÚLOŽIŠTĚ DOKUMENTŮ ..... 76
11.1.1 Požadavky na server ..... 76
11.1.2 Návrh nového serveru ..... 76
11.1.3 Operační systém a licence ..... 76
11.1.4 Cena serveru ..... 77
11.2 ZÁLOHOVACÍ ZAŘÍZENÍ ..... 78
11.3 AUTOMANAGER MERIDIAN ..... 79
11.3.1 Výhody Automanageru Meridian ..... 79
11.3.2 Licencování Automanager Meridian ..... 80
11.3.3 Cena navržených licencí ..... 81
11.3.4 Služby ..... 81
11.4 CELKOVÁ CENA INVESTICE ..... 81
11.5 KVALIFIKOVANÝ CERTIFIKÁT ..... 82
11.5.1 Výběr kvalifikované certifikační autority ..... 82
11.5.2 Vygenerování klíčů a žádosti o certifikát ..... 82
11.5.3 Vydání certifikátu ..... 83
11.5.4 Instalace vydaného certifikátu ..... 84
11.5.5 Použití elektronického podpisu ..... 85
**12 VYHODNOCENÍ ..... 86**
12.1 NÁVRH ŘEŠENÍ ..... 86
12.2 SILNÁ MÍSTA ŘEŠENÍ ..... 86
12.3 SLABÁ MÍSTA ŘEŠENÍ ..... 86
**ZÁVĚR ..... 87**
**CONCLUSION ..... 88**
**SEZNAM POUŽITÉ LITERATURY ..... 90**
**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK ..... 92**
**SEZNAM OBRÁZKŮ ..... 95**
**SEZNAM TABULEK ..... 96**
**SEZNAM PŘÍLOH ..... 97**
**PŘÍLOHA P I: CERTIFIKÁT ISO 9001: 2000 ..... 98**

**PŘÍLOHA P II: CERTIFIKÁT VDA 6.1 ..... 99**
**PŘÍLOHA P III: OSVĚDČENÍ K VÝROBĚ VOJENSKÉ LETECKÉ TECHNIKY ..... 100**
**PŘÍLOHA P IV: OPRÁVNĚNÍ K PROJEKTOVÁNÍ LETADLOVÝCH ZAŘÍZENÍ .... 101**
**PŘÍLOHA P V: HP STORAGEWORKS ULTRIUM 232 TAPE DRIVE ..... 102**
**PŘÍLOHA P VI: PŘEDSTAVENÍ SDRUŽENÍ SOVA ..... 104**
**PŘÍLOHA P VII: AUTOMANAGER MERIDIAN ..... 105**
**PŘÍLOHA P VIII: CD S PRACÍ V ELEKTRONICKÉ PODOBĚ ..... 108**

# ÚVOD

Dnes již téměř všechny dokumenty vznikají jako elektronické. Jedná se tedy o digitální datové soubory vytvořené prostřednictvím výpočetní techniky. Jsou to nejen dokumenty textové, ale i obrazové, výkresové dokumentace, elektronická pošta atd. Důvody používání elektronických dokumentů, jejich výhody i nevýhody jsou známé a mnohokrát popsané.

S těmito dokumenty – datovými soubory je třeba manipulovat obdobně jako s listinnými dokumenty a to nazýváme elektronickou správou dokumentů.

Důvody proč používat elektronickou správu a elektronický oběh těchto dokumentů, jsou zřetelné. Je to zejména zjednodušení a zrychlení realizace procesů, snadnější manipulace s dokumenty. To přináší zefektivnění práce, průhlednou kontrolu nad oběhem dokumentů a v konečném důsledku i úsporu financí. Práci s listinnými dokumenty se samozřejmě nelze zcela vyhnout, ale je možné ji podstatně minimalizovat.

Také ve firmě AEV spol. s r.o., Kroměříž, kde pracuji jako správce počítačové sítě a mám na starost hardwarové a softwarové vybavení firmy a provoz s tím spojený, vznikla potřeba uřídit stále rostoucí počet vznikajících elektronických dokumentů a efektivně je spravovat. Tento úkol jsem si vybral jako svoji diplomovou práci.

Cílem práce je vypracovat projekt pro zavedení ucelené správy elektronických dokumentů ve firmě AEV tak, aby se zefektivnila práce s dokumenty a jejich archivace.

V teoretické části práce se zabývám důvody nasazení elektronické správy dokumentů, jejími úkoly a funkcemi. Dále datovou bezpečností, která je velmi důležitá, její součástí je elektronický podpis, který rovněž budeme ve firmě používat a problematikou dlouhodobého ukládání dat a archivace dokumentů. Nakonec analýzou současných technologických možností správy dokumentů.

V praktické části krátce představuji firmu AEV a současný stav práce s elektronickými dokumenty. Dále vlastní zadání úkolu, co management od správy dokumentů očekává a které možnosti chce využívat. Hlavní význam práce spočívá v návrhu vhodného řešení pro firmu, což bylo také cílem této práce. Na závěr jsem vyhodnotil úspěšnost řešení.

# I. TEORETICKÁ ČÁST

# 1 SPRÁVA DOKUMENTŮ

Hodnota informací uložených v podobě dat na PC, serverových systémech, či sítích je pro každou firmu obrovská. Je potřeba data uschovávat, pracovat s nimi, předcházet případným ztrátám nebo zneužití.

Každá firma vytvářející a archivující větší množství elektronických dokumentů (nabídek, kalkulací, technických zpráv, výkresů v CAD systémech, předpisů, norem, apod.) musí řešit problémy s udržení pořádku v těchto dokumentech, jejich kompletní archivací, vyhledávání, přehled o jednotlivých revizích daného dokumentu, zajištěním maximální bezpečnosti dokumentů jak z hlediska přístupu tak z hlediska uchování dokumentů, toku dokumentu v rámci firmy.

## 1.1 Hlavní odlišnosti digitálního a analogového dokumentu

Analogovým dokumentem zde nemyslím pouze listinné dokumenty, ale i např. analogový záznam zvuku nebo obrazu. Analogový záznam je založen na signálu se spojitě proměnlivým průběhem.

Naproti tomu digitální záznam je tvořen posloupností znaků binární soustavy "0" a "1". Počítače umí pracovat pouze s těmito údaji tedy s čísly.

Z toho vyplývají i hlavní rozdíly uvedené v tabulce, viz Tabulka 1.

Tabulka 1 Odlišnosti dig. a analog. dokumentu

| **Digitální dokument** | **Analogový dokument** |
|---|---|
| dekódování počítačem nebo jím řízenými periférierni | dekódování strojem nebo lidskými smysly |
| proměnlivost | stálost |
| hypertextová / hypermediální struktura | lineární struktura |
| multimedialita | unimedialita |
| stavebnicový charakter | celistvost a sekvenčnost |
| neztrátová reprodukce | ztrátová reprodukce |
| snadná formální transformace | obtížná formální transformace |
| distribuovanost (možnost on-line přístupu) | lokalizovanost |
| snadná kontrola integrity záznamu | obtížná kontrola integrity dat |
| interaktivnost | jednostranné působení |

## 1.2 Požadavky na systém správy dokumentů

Systém správy elektronických dokumentů by měl kontrolovat celý životní cyklus dokumentů, který zahrnuje následující fáze:

- Vytvoření
- Posouzení
- Úpravy
- Schválení
- Publikování
- Distribuce
- Dlouhodobé uložení

Pro firmy pracující podle standardu jakostních norem IS0 9000 navíc přistupuje potřeba jednoznačně definovaných postupů a procesů práce s dokumentem a protokolování všech jeho změn (kdo, kdy, co, kdo smí, atd.). Více informací o normách ISO 9000 lze získat na stránkách CQS Sdružení pro certifikaci systémů řízení jakosti <http://www.cqs.cz>

## 1.3 Hlavní funkce správy dokumentů

- možnost snadného vytváření a správy uživatelů a uživatelských skupin
- přidělování práv a kontrola přístupu uživatelů k dokumentům
- sledování informací, které lze uložit v zabezpečeném souboru na místě, kde je zaručena jeho integrita a jsou monitorovány a zaznamenány veškeré jeho změny
- archivace dokumentů

## 1.4 Workflow

Workflow je soubor aktivit, které koordinují lidské nebo softwarové účastníky při plnění nějakého úkolu.

Zdych: „Životní cyklus objektu, jimž mohou být dokumenty, úkoly atd. Je to proces pohybu takových objektů z různých stavů za určitých podmínek a na základě nějakých událostí. Důležitou vlastností workflow je možnost definovat oprávnění na objekt v

různých stavech objektu.“[18]

Řešení pomocí workflow umožňuje:

- Správu firemní komunikace
- Efektivní využívání firemních zdrojů
- Kontrola dodržování firemního řádu
- Řešení bezpečnosti a správy dat

## 1.5 Další funkce

Dále mohou systémy správy dokumentů nabízet knihovnické služby vyzvednutí a vrácení. Když si uživatel vyzvedne dokument, systém zakáže provádění změn ostatním uživatelům. Když je dokument vrácen zpět, zpřístupní systém provádění korekcí i ostatním uživatelům s příslušným oprávněním.

Spolu se službami vyzvednutí a vrácení má systém na starosti také sledování revizí, a umožňuje tak kontrolu verze a historie dokumentu.

Systémy správy dokumentů zahrnují také funkce vyhledávání dokumentů, a to podle externích popisných dat (jméno uživatele, který dokument uložil, datum změny apod.), nebo podle obsahu, tedy fulltextové vyhledávání. Mohou být přímo napojeny nebo integrovány do procesu vytváření dokumentů.

## 1.6 Přínos systému pro správu dokumentů

Z požadavků na systém pro správu dokumentů a z jeho možností vychází jeho přínos. Dá se vyjádřit těmito body:

- zavedení určitého řádu a systému do práce s dokumenty
- urychlení vyhledávání a oběhu dokumentů
- full-textovém prohledávání a indexování dokumentů
- zabránění ztrátám dokumentů
- podpora široké množiny formátů dokumentů
- verzování dokumentů s možností návratu

- možnosti grafické definice a tvorby workflow procesních cest oběhu dokumentu nebo formuláře
- poskytnutí historie zpracování každého dokumentu
- zefektivnění archivace dokumentů

Velkým přínosem je elektronický oběh dokumentů tam, kde je nutné provádět procesy s dokumenty na dálku. Například u firem s více pobočkami vzdálenými od centrály, nebo s větším počtem často cestujících zaměstnanců.

Samostatnou kapitolu věnuji datové bezpečnosti, která se správou elektronických dokumentů souvisí.

# 2 BEZPEČNOST DAT

Bezpečnost je důležitý, ne-li nejdůležitější aspekt správy dokumentů. Mluvíme-li o elektronické správě dokumentů, jde tedy o bezpečnost elektronických dat.

Informace mají určitou hodnotu a podle jejich hodnoty s nimi musíme adekvátně zacházet, chránit je. Vznikl tak nový pojem – *informační bezpečnost*.

Bezpečnost dat představuje komplexní zajištění systému počínaje přístupem do systému, manipulací s daty, ochranou proti úniku a zneužití informací, prevencí ztráty dat (zálohování, antivirová ochrana), řešení případného bezpečnostního incidentu a minimalizace vniklých škod.

Vždy je třeba mít na vědomí, že absolutní bezpečnost neexistuje.

**Informační bezpečnost**

Co si tedy pod tímto pojmem představit?

Jašek: „Informační bezpečnost chápeme jako zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.“[6, s. 10]

**Bezpečný informační systém**

Jak je třeba chápat bezpečný informační systém?

Jašek: „Bezpečný informační systém definujeme jako systém, který chrání informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti a při jejich likvidaci proti ztrátě důvěrnosti.“[6, s. 10]

## 2.1 Hrozby

Úkolem informační bezpečnosti je chránit data před možnými hrozbami, popř. minimalizovat jejich následky.

Datové nebezpečí můžeme dělit podle původce, od kterého hrozí. Mohou to být

- lidé - chyba, selhání, úmysl
- přírodní jevy - povětrnostní vlivy, živelné pohromy

- porucha techniky

Příklady incidentů:

- neoprávněná změna dat
- zneužití citlivých informací
- únik informací
- ztráta, zničení dat

## 2.2 Možnosti ochrany

Možnosti ochrany mají různé podoby. Jsou to:

- fyzická ochrana nosičů dat
- přístupová práva a autentizace
- technické zabezpečení - zálohování, antiviry, šifrování

Tyto metody je třeba pro zvýšení jejich účinnosti kombinovat.

### 2.2.1 Fyzická ochrana

Fyzickou ochranu nosičů dat před neoprávněnými osobami je třeba zajistit vhodnými prostředky proti neoprávněnému vniknutí. Tedy výběr místnosti, ochrana zámky, zabezpečovacím systémem, ostrahou apod. Neoprávněné osoby nemusí mít nutně zlý úmysl, ale mohou způsobit škodu i z neznalosti.

Ochrana před přírodními jevy znamená zamezení vlivu normálních povětrnostních působení jako déšť, sníh apod. Ochrana proti přírodním živlům tedy ohni, velké vodě apod. je obdobná jako ochrana ostatního majetku, např. požární hlásiče, umístění mimo záplavovou zónu.

### 2.2.2 Přístupová práva a autentizace

Nejprve je třeba nastavit uživatelům přístupová práva k jednotlivým datům. Práva se dají nastavit přímo každému uživateli zvlášť nebo skupinám uživatelů. Pokud je uživatelů větší počet, je výhodné přidělovat přístupová práva skupinám a uživatele pak do těchto skupin přiřadit. Uživatelské skupiny bývají v operačních systémech přednastavené, dají se však

podle potřeby upravovat a přidávat nové.

Přístupová práva se dají rozdělit na

- úplné řízení (administrátorské)
- přidávat
- upravovat
- mazat
- číst
- přístup zakázán

V různých systémech mohou být modifikace těchto základních přístupových práv. Kromě práva úplného řízení a zákazu všech práv se ostatní práva většinou kombinují. Práva se nastavují jednotlivým souborům nebo složkám-svazkům, ve kterých jsou umístěné.

Při vstupu do systému se uživatel musí jednoznačně identifikovat a tím vlastně získat možnosti pro manipulaci s daty, ke kterým je oprávněn. Proces, kterým systém ověří identitu uživatele je **autentizace**.

Nejrozšířenější způsob autentizace je zadávání hesel nebo PIN. V tomto případě se uživatel prokazuje určitou znalostí – *důkaz znalostí.*

Další způsobem autentizace je používání např. čipové karty. Uživatel ji musí vlastnit – *důkaz vlastnictvím.*

U těchto metod je důležité, aby si uživatelé zachovali svou jedinečnost utajením hesla resp. fyzickou ochranou své čipové karty.

Nejnovější a zatím nejméně rozšířený způsob autentizace je biometrika. Jde o ověření určité tělesné vlastnosti uživatele. Např. sejmutí otisku prstu nebo obrazu oční duhovky. Tato metoda se dá doplnit i zadáním hesla. Uživatel musí prokázat nějakou vlastnost – *důkaz vlastností.*

### 2.2.3 Technické zabezpečení

Do této podkapitoly bych zařadil zálohování dat, ochranu před útoky a šifrování dat.

#### *2.2.3.1 Zálohování*

Hlavním cílem zálohování je opětovné zpřístupnění důležitých dat ztracených nebo poškozených po nějakém incidentu. Pojem zálohování tedy není možné zaměňovat s pojmem archivace. Zálohovaná data se za normálních okolností nevyužívají. Zato je nutné pravidelně zálohy dat vytvářet. Tomuto cíli je podřízen způsob vytváření záloh, jejich čas, frekvence a média, na která se ukládají.

Pro dobré fungování zálohovacího systému je nutné zvolit optimální hardwarové a softwarové prostředky. K tomu je potřebná dobrá analýza stavu používané výpočetní techniky, struktury zálohovaných dat a aplikací, používaných pro práci s těmito daty.

Aby zálohovací systém plnil svou funkci, musím mít vyřešenou i technologii případné obnovy dat po jejich ztrátě nebo poškození.

Pravidelné denní zálohování dat bývá obvykle řešeno jako automatické s předem nadefinovanými parametry, co a jak se bude zálohovat. Půjde-li o zálohování celkové, rozdílové nebo přírůstkové apod. Naproti tomu ruční zálohování se používá např. před nějakým zásahem do hardwaru či softwaru, jako jsou výměny disků nebo updaty a upgrady softwaru.

Úplné zálohování disku se provádí tzv. **zrcadlením** (mirroring), kdy se automaticky udržuje v pravidelných intervalech přesná kopie zálohovaného disku na jiný stejně velký disk. Princip zrcadlení disku řeší nejčastější poruchu hardwaru, kterou je selhání pevného disku – harddisku.

Druhý způsob úplného zálohování disku je **vytvoření obrazu** (image) disku, ze kterého lze později pořídit kopii původního disku a to pomocí speciálního softwaru k tomu určeného. Nejznámější je Norton Ghost firmy Symantec. Společnost Symantec <www.symantec.com/cs/cz> je se svým softwarovým řešením významným pojmem v oblasti komplexní datové bezpečnosti.

Obnova dat je spíše záležitostí cílené činnosti obsluhy nebo administrátora s ohledem na rozsah ztracených dat.

#### *2.2.3.2 Ochrana před útoky*

Škodlivý software nazývaný též **malware** je počítačový program určený ke vniknutí nebo

poškození počítačového systému. Dá se rozdělit do tří základních skupin:

- viry
- trojské koně
- červi

**Virus** – Nejstarší typ škodlivého softwaru. Chová se obdobně jako biologický virus, odtud jeho označení. Šíří se internetem zejména elektronickou poštou. Napadne nějaký soubor, čeká na svou příležitost a po spuštění napadeného souboru se dál šíří a škodí. Viry mohou poškodit software, hardware i soubory. Závažnost počítačových virů se pohybuje od lehce nepříjemných až po naprosto destruktivní.

**Trojský kůň** – Tento typ malware má své pro své označení vzor ve známé lsti použité ve starověku Řeky při dobývání Tróje. A lstivě se také chová. Navenek vypadá jako nějaký užitečný nebo zábavný prográmek, kterého si uživatel sám spustí nebo nainstaluje. Ve skutečnosti provádí na pozadí nekalou činnost jako sbírání a odesílání hesel, nebo špehování, jaké internetové stránky uživatel navštěvuje apod.

**Červ** – Škodlivý samostatný program, samostatně se šíří internetem, distribuuje své kopie, rozesílá se elektronickou poštou nebo otevřenými porty. Na rozdíl od viru nepotřebuje, aby ho někdo spustil, dokáže se spustit sám. Červi mohou proniknout do systému a umožnit převzetí vzdálené kontroly jinému uživateli.

Kromě malwaru tedy škodlivého softwaru existuje ještě tzv. spyware a adware.

**Spyware** je program, který využívá Internetu k odesílání dat z počítače bez vědomí jeho uživatele.

**Adware** znepříjemňuje práci s PC reklamou. Typickým příznakem jsou vyskakující reklamní okna, společně s vnucováním komerčních stránek.

Spyware a adware není určen, aby škodil, ale přesto je pro většinu uživatelů nežádoucí a chce se proti němu bránit.

### Antiviry

Antivirové programy i přes svůj název nechrání systém pouze před viry, ale před škodlivým softwarem vůbec.

Funkce antiviru:

- rezidentní štít
- rezidentní skener
- skener úložišť
- kontrola pošty

Rezidentním štít má za úkol zachytit nežádoucí software při pokusu o vniknutí do systému z internetu nebo z místní sítě. Rezidentní skener kontroluje všechny otevírané soubory. Skener úložišť dat kontroluje v naplánovaných intervalech soubory uložené na discích. Antiviry kontrolují přílohy příchozích i ochozích emailů.

Antiviry mají schopnosti nejen identifikovat, ale i likvidovat malware a léčit napadené soubory. Pro vyhledávání virů používají metody signaturové a heuristické.

**Signaturová metoda** spočívá v databázi s názvy virů a s krátkými úseky jejich těl. Při kontrole souborů hledají signatury, které odpovídají známým virům. K této funkci antiviru je nezbytně nutná častá aktualizace jeho virové databáze.

**Heuristická analýza** používá metody spouštění programů a zkoumání jejich činnosti. K tomuto účelu antivir vytvoří tzv. virtuální počítač, na kterém je testování podezřelých programů bezpečné. Tato metoda je sice pomalejší, ale vede k odhalení dosud neznámých škodlivých programů.

Dnešní antivirové systémy využívají a vhodně kombinují obě metody. Podezřelé nebo zatím neléčitelné soubory ukládají do tzv. karantény a lze je odesílat výrobci systému k analýze. Tato zpětná vazba přispívá k rychlejšímu objevení nového malware nebo nějaké nové modifikace a jeho zavedení do databáze. Výrobci antivirových systémů vydávají aktualizační soubory a antivirové programy prostřednictvím internetu automaticky zjišťují nové aktualizace a instalují je. V podnikových sítích běží antivirový systém na k tomu určeném serveru. Toto centrální řízení umožňuje jedno nastavení aplikovat do stanic. Jednotlivé stanice si aktualizační soubory nemusí stahovat z internetu, ale prostřednictvím místní sítě se aktualizují ze serveru.

### Firewally

Firewall – protipožární zeď, má v informačních technologii význam kontrolu a omezování

provozu mezi sítěmi. Hlavním úkolem firewallu bývá chránit podnikovou síť před útoky z internetu, ale i jednotlivé stanice před vnitřními útoky resp. útoky z internetu

Základní dělení:

- hardwarové
- softwarové

Hardwarový firewall slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které spojuje. Nejčastější využití je, že router, který spojuje místní síť k internetu má vestavěný hardwarový firewall a chrání tak celou síť resp. všechny stanice a servery před útoky z internetu.

Kromě toho je třeba chránit stanice i před vnitřními útoky v místní síti. K tomu slouží programy softwarové někdy též personální firewally nainstalované v jednotlivých stanicích popř. i na serverech. Je-li počítač připojen přímo k internetu, samozřejmě ho softwarový firewall chrání i před útoky z internetu.

Základní technologie:

- jednoduchý IP filtr
- stavový IP filtr
- aplikační firewally
- hloubkové a inteligentní firewally

*Jednoduchý IP filtr* pracuje na principu pravidel, která zakazují provoz na jednotlivých portech. Nezakázané porty jsou povolené. Neanalyzuje procházející data.

*Stavový IP filtr* monitoruje síťový provoz. Podle nastavených pravidel a stavové tabulky provoz povoluje nebo zakazuje. Povolí průchod paketů z místní sítě do internetu, ale v opačném směru povolí komunikaci pouze iniciovanou zevnitř.

*Aplikační proxy* filtruje všechny pakety, jejichž propuštění není povoleno, což je zásadní rozdíl proti IP filtrům. Filtruje pakety podle toho, která aplikace na kterém portu s nimi pracuje. Každá aplikace má tedy povoleny jen určité porty, a ty jsou zakázány pro ostatní aplikace.

*Hloubkové a inteligentní firewally* jsou postavené na technologii stavové inspekce.

Kontrolují provoz na výskyt známých řetězců, ověřují dodržování standardů protokolů a standardů aplikací.

#### *2.2.3.3 Šifrování dat*

Šifrování dat neboli **kryptografii** se podrobněji věnuji v následujících kapitolách kryptologie a elektronický podpis.

Datovou bezpečností se podrobněji zabývá Doseděl Tomáš v knize Počítačová bezpečnost a ochrana dat. [2]

# 3 KRYPTOLOGIE

Jedním z důležitých způsobů zabezpečení dat je jejich šifrování, tedy **kryptografie**. Kryptografie je věda o šifrování dat pomocí matematických metod. Opačným postupem, tedy rozluštěním utajovaných dat bez znalosti klíče, se zabývá věda zvaná **kryptoanalýza.** Obě tyto vědy tvoří jeden obor s názvem **kryptologie.**

## 3.1 Kryptografie

Úkolem kryptografie je zajištění důvěrnosti dat. Kryptografie (šifrování) je převedení dat v čitelné podobě, kterým říkáme otevřený text, do nečitelné formy, tzv. šifrovaného textu.[1] Takto změněná data jsou nečitelná pro všechny nepovolané osoby a je tím zaručena jejich důvěrnost. Lze je přečíst pouze po dešifraci pomocí dešifrovacího klíče a je tedy možné je ukládat na nezabezpečená úložiště, posílat emailem apod. Toho se využívá zejména v kombinaci s tzv. elektronickým podpisem.

### 3.1.1 Základní pojmy

- Kryptografický algoritmus
- Šifrovací klíč
- Symetrická kryptografie
- Asymetrická kryptografie
- Klíčový pár

### 3.1.2 Kryptografický algoritmus

Neboli šifrovací algoritmus je matematický postup, který transformuje text do nečitelné podoby a zpět.

**Uzavřený algoritmus** – bezpečnost založena na jeho dokonalém utajení. Nevýhodou je, že často docházelo k jeho prozrazení.

[1] Pojmů otevřený text a šifrovaný text se v kryptologie používá pro všechny datové soubory, nejen pro texty.

**Veřejný algoritmus** – bezpečnost je založena na matematických vlastnostech. Je kvalitnější a důvěryhodnější než uzavřený.

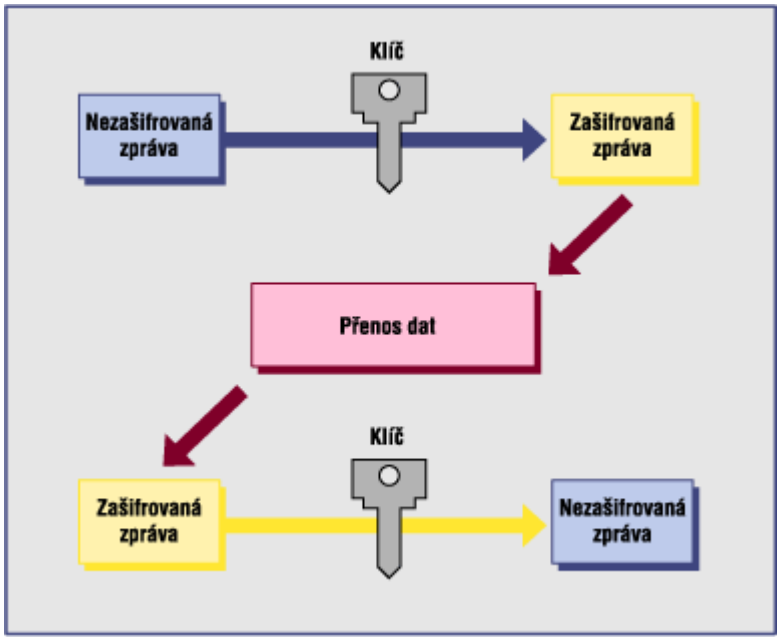
### 3.1.3 Šifrovací klíč

Je to soubor obsahující data s parametry šifrovacího algoritmu. Pomocí klíče se provádí samotné šifrování a dešifrování.

### 3.1.4 Symetrická kryptografie

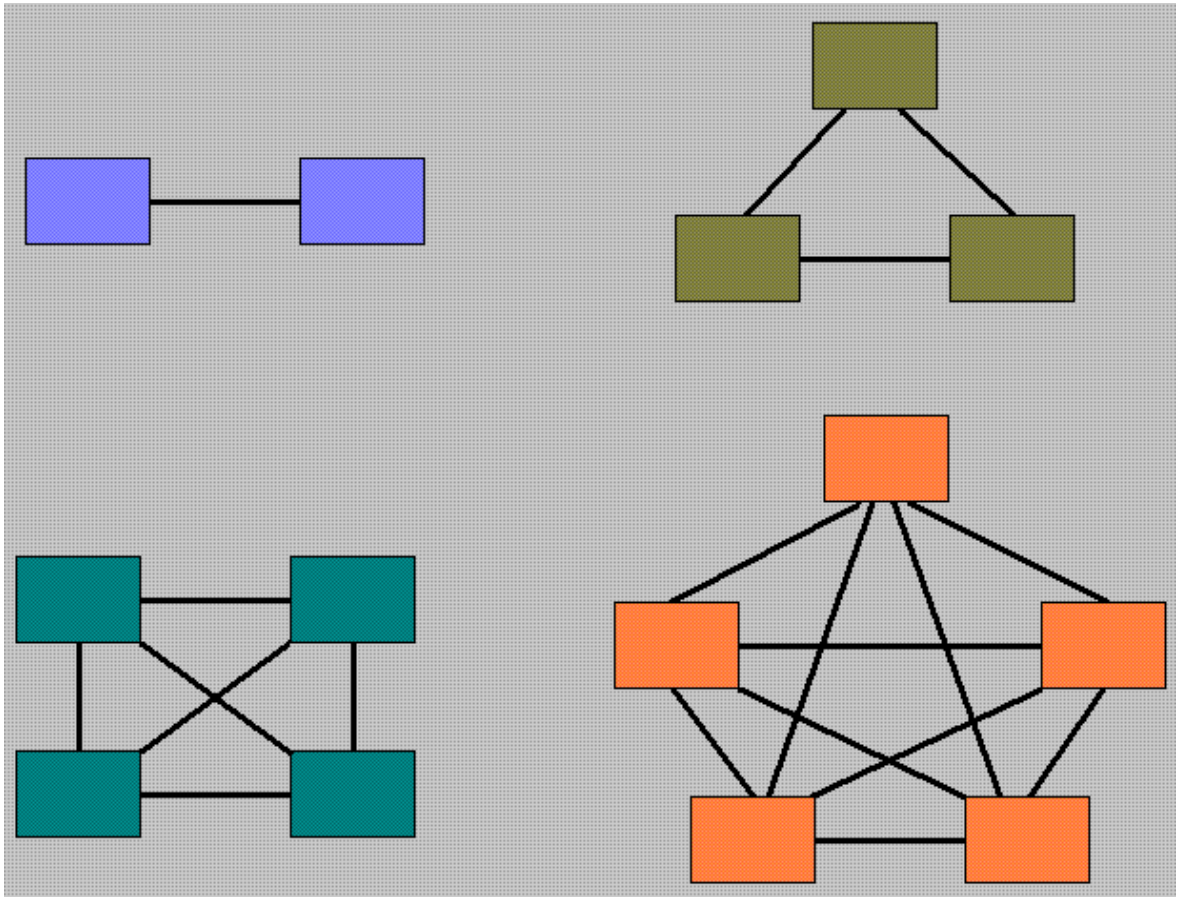
Symetrické šifrování je metoda, při které je otevřený text zašifrován s pomocí jistého klíče a může být obnoven jen se znalostí tohoto klíče. Většina moderních algoritmů je založena na matematické teorii čísel. Při symetrickém šifrování si musí autor a příjemce nějakým bezpečným způsobem vyměnit klíč.Obrázek 1. Samotné symetrické šifrování nemůže nikdy problém předání klíče vyřešit.

Rozhodujícím kritériem síly symetrické šifry je délka klíče. Zpráva totiž musí odolat tzv. útoku hrubou silou, který předpokládá prosté vyzkoušení všech možných klíčů. Délka se uvádí v počtu bitů binárního čísla. Má-li tedy šifra sílu 4 bity, je 2^4=16 možných klíčů. Je zřejmé, že tato síla neobstojí. Dnes nejčastěji používané 128 bitové klíče zaručují odolnost proti útokům hrubou silou minimálně na několik desítek let dopředu.




Obrázek 1 Symetrické šifrování

Dvě strany si bezpečným způsobem sdělí jeden tajný klíč, který nikdo jiný nezná. Tento sdílený klíč používají k šifrování a dešifrování zpráv (souborů). Pokud ovšem spolu má šifrovaně komunikovat více stran, neúměrně roste počet potřebných klíčů. Tři uživatelé – tři klíče, čtyři uživatelé – šest klíčů, pět uživatelů – deset klíčů atd. Tento nárůst je patrný z obrázku. Obrázek 2. Každý uživatel potřebuje mít totiž s každým uživatelem jeden sdílený klíč. Nevýhody jsou tedy zřejmé.



Obrázek 2 Nárůst počtu symetrických klíčů

### 3.1.5 Asymetrický kryptografie

Asymetrická kryptografie již řeší tuto problematiku daleko lépe než symetrická.

V 70. letech 20. století byl navržen první asymetrický šifrovací algoritmus. Jeho princip je jednoduchý: zpráva se zašifruje jedním klíčem, rozšifrovat se však musí jiným klíčem.

Mezi nejznámější asymetrické šifry patří RSA, Diffie-Hellman a DSS.

Délka klíče asymetrické šifry má trochu jiný význam. Asymetrické šifry jsou většinou založeny na nějakých speciálních číslech (např. prvočíslech). Při útoku hrubou silou tedy

stačí zkoumat jen tato speciální čísla. Dnes se běžně pracuje s délkou klíče 1024 bitů, avšak pro dlouhodobější použití je lépe zvolit 2048 bitů nebo více.

Hlavní výhodou asymetrického šifrování je počet klíčů. Ten totiž nenarůstá jako počet klíčů potřebný pro symetrické šifrování. Zůstává vždy pouze na dvojnásobku počtu komunikujících stran, přičemž každá strana se stará o bezpečné uložení svého soukromého klíče.

#### *3.1.5.1 Klíčový pár*

Každá komunikující strana si k tomuto účelu vygeneruje dvojici klíčů, tzv. klíčový pár:

- veřejný klíč
- soukromý klíč

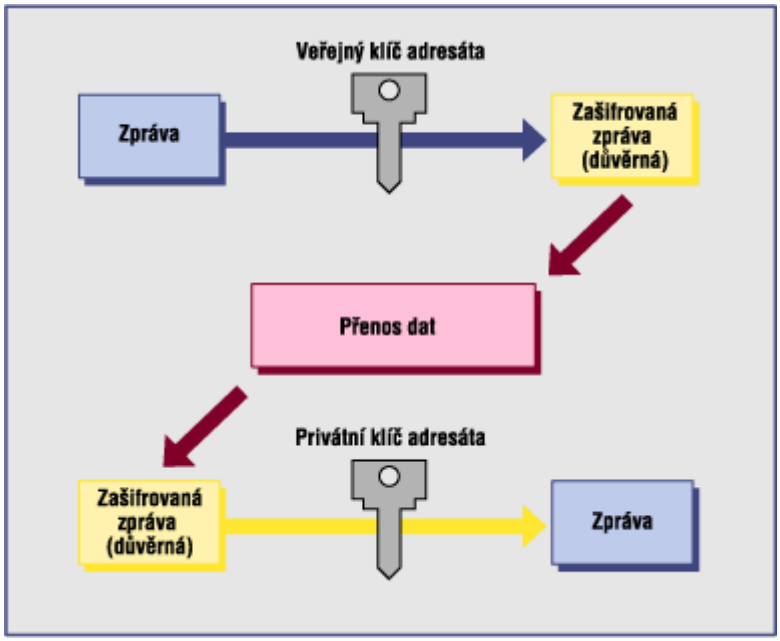
Ze znalosti prvního klíče nelze zjistit druhý. První klíč může být tedy dán ve známost komukoli (tzv. veřejný klíč nebo veřejná část klíče), zatímco druhý si uchovává vlastník v tajnosti (soukromý klíč nebo soukromá část klíče).

Klíčového páru se používá i při elektronickém podepisování, více v kapitole Elektronický podpis.

#### *3.1.5.2 Postup šifrování a dešifrování*

Chci-li někomu poslat zašifrovanou zprávu, vyžádám si od něj jeho veřejný klíč, nebo si ho vyhledám na veřejně dostupném místě. Tímto jeho veřejným klíčem zprávu zašifruji a odešlu. Zpráva není pro nikoho jiného čitelná a odšifrovat ji může pouze příjemce svým soukromým klíčem. Viz Obrázek 3.

Opačný postup je obdobný – Přijde-li mi zašifrovaná zpráva, musí být zašifrována mým veřejným klíčem, který jsem předem dal k dispozici. Abych tuto zprávu odšifroval, použiji k tomu svůj soukromý klíč, který si uchovávám v tajnosti. Zprávu tedy mohu považovat za důvěrnou, tzn. že ji nikdo jiný nemohl přečíst.




Obrázek 3 Asymetrické šifrování

### 3.1.6 Hybridní kryptografie

Spojuje výhody symetrické kryptografie – rychlost šifrování, rychlost dešifrování a asymetrické kryptografie – menší počet klíčů, nižší nároky na jejich správu.

Zprávy se šifrují náhodně vygenerovaným symetrickým klíčem. Tento klíč je poté zašifrován asymetrickým algoritmem a přiložen ke zprávě.

### 3.1.7 Proudové a blokové šifry

Další dělení šifrování z hlediska množství dat šifrovaných v jednom okamžiku.

**Proudové šifry** – šifrování textu probíhá po jednotlivých znacích, tedy proudem.

**Blokové šifry** – text je šifrován po větších blocích.

## 3.2 Kryptoanalýza

Kryptoanalýza se zabývá luštěním šifrovaného textu bez znalosti šifrovacího klíče. Pokus o takového luštění se též nazývá útokem, anglicky attack.

Ve většině případech má kryptoanalytik k dispozici nějaké znalosti o otevřeném nebo šifrovaném textu. Potom se jedná některou z metod luštění se znalostí. Jestliže takové znalosti nemá k dispozici, požije tzv. útok hrubou silou.

### 3.2.1 Luštění se znalostí

Rozdělené metod podle typu znalosti:

- luštění se znalostí šifrovaného textu
- luštění se znalostí otevřeného textu
- luštění se znalostí vybraných otevřených textů
- luštění se znalostí vybraných šifrovaných textů

### 3.2.2 Útok hrubou silou

Tato metoda spočívá v pokusech dešifrování všemi možnými klíči z celého prostoru klíčů. K tomu je zapotřebí výkonný výpočetní systém.

# 4 ELEKTRONICKÝ PODPIS

Elektronický podpis je kryptografická metoda zajišťující pro digitální data podobné vlastnosti jako vlastnoruční podpis u běžných papírových dokumentů. Je jedním z hlavních nástrojů identifikace a autentizace osob v prostředí elektronických dokumentů. Rozumíme jím údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě nebo dokumentu.

Elektronický podpis vytváří počítač a pro každou odesílanou zprávu je unikátní. Co je potřeba, aby elektronický podpis mohl vzniknout? Musí existovat důvěryhodná instituce, která ověří vaši totožnost a vydá certifikát, na základě kterého váš počítač generuje pro odesílané zprávy konkrétní elektronické podpisy. Těmi důvěryhodnými institucemi jsou certifikační autority (CA). Uživatel si vybere některou CA a u ní si zažádá o vystavení certifikátu. Tuto žádost lze podat prostřednictvím internetu. Výběr CA záleží na tom, k jakým účelům certifikát potřebuje. Zaručené certifikáty vydávají pouze některé CA (např. 1. certifikační autorita). Nejde-li o komunikaci se státní správou, není zapotřebí zaručený certifikát a pak je již výběr CA širší.

Elektronický podpis zajišťuje:

integritu dokumentu – lze prokázat, že po podepsání nedošlo k žádné změně, soubor není poškozen ani záměrně, ani omylem

autentizaci – lze prokázat, že autorem je skutečně ten, kdo je pod dokumentem podepsán

nepopiratelnost – autor nemůže popřít, že dokument podepsal

## 4.1 Základní terminologie

- Certifikační autorita
- Certifikát
- Klíčový pár
- Symetrická kryptografie
- Asymetrická kryptografie
- Hash funkce a hodnota

- Časové razítko

### 4.1.1 Certifikační autorita

Certifikační autorita je objekt, který vydává digitální certifikáty k použití ostatním zúčastněným.

### 4.1.2 Certifikát

Digitální certifikát je digitálně podepsaný veřejný klíč.

### 4.1.3 Symetrická kryptografie

I u elektronického podpisu lze použít symetrickou kryptografii, pak jde ovšem o arbitrovaný protokol. To je protokol, který kromě komunikujících stran potřebuje ještě třetí stranu – arbitra. Protokol je založen na důvěře obou stran arbitrovi.

### 4.1.4 Asymetrická kryptografie

Dnes se pro účely elektronického podpisu používá hlavně asymetrická kryptografie. Využívá se stejného klíčového páru jako pro šifrování, což je jeho další výhoda. Při podepisování se ale nejprve použije soukromý klíč pisatele a při ověření podpisu jeho veřejný klíč.

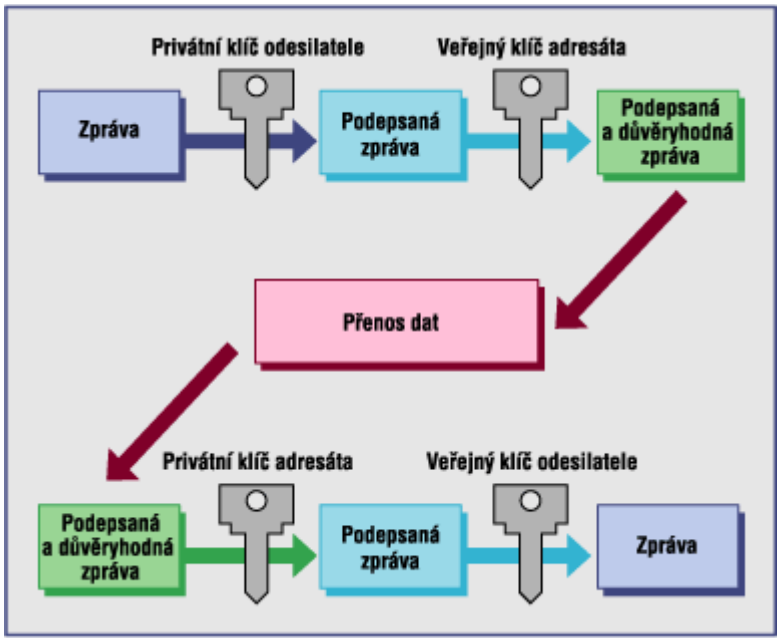
#### *4.1.4.1 Klíčový pár*

Soukromý klíč – slouží k podepisování a k dešifrování obsahu zprávy.

Veřejný klíč – slouží k ověřování podpisu a k šifrování obsahu zprávy.

Postup je znázorněn na obrázku. Viz Obrázek 4.

Je zřejmé, že elektronický podpis tedy klíčový pár musí vlastnit odesílatel podepsané zprávy. Její příjemce svůj klíčový pár pro ověření podpisu nepotřebuje. Má-li být zpráva navíc i zašifrována, potřebuje svůj klíčový pár i příjemce takové zprávy.

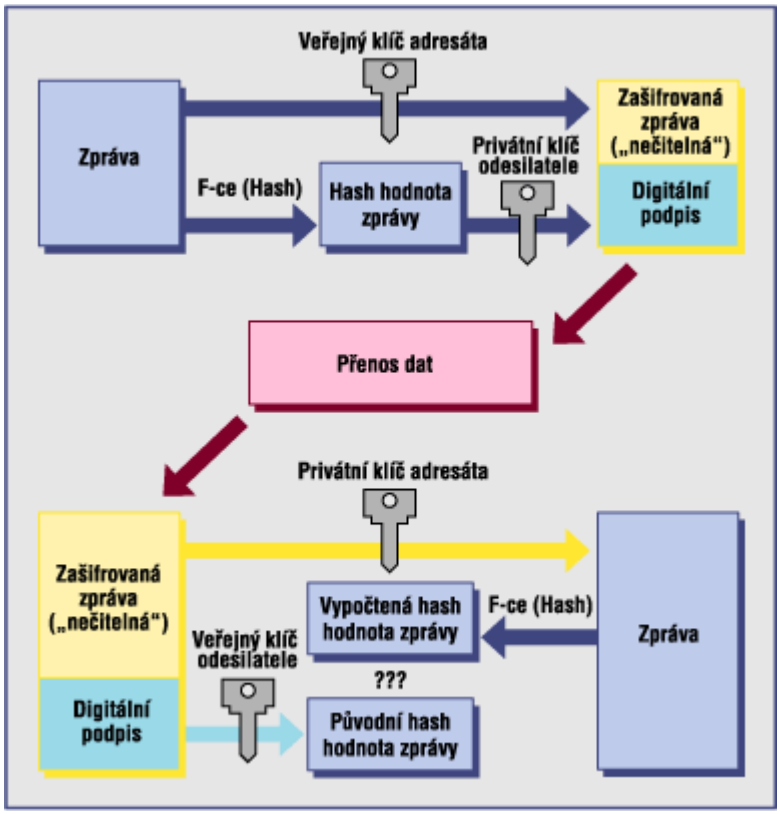



Obrázek 4 Přenos adresované, zašifrované a podepsané zprávy

### 4.1.5 Hash funkce a hodnota

Hash funkce je transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je pak řetězec znaků s pevnou délkou, tzv. hash nebo také otisk. Obrázek 5. Na její kvalitu jsou v kryptografii kladena kritéria:

- vstup může být jakékoli délky
- výstup musí mít pevnou délku
- hodnota hash musí být jednoduše vypočitatelná pro jakýkoli vstupní řetězec
- funkce je jednosměrná (irreverzibilní)
- funkce je bez kolizí




Obrázek 5 Bezpečná komunikace s využitím digitálního podpisu

### 4.1.6 Časové razítko

Kvalifikované časové razítko slouží k označení dokumentu, u kterého je nutný důkaz, že v daném čase a v dané podobě existoval. Časové razítko je dobré použít například při podpisu smlouvy v elektronické podobě, pro archivaci elektronických dokumentů, při on-line obchodování nebo kvůli případnému dokazování u soudu. Zatímco elektronický podpis je potvrzením identity autora nebo odesílatele dokumentu, časové razítko potvrzuje existenci dokumentu v čase.

## 4.2 Struktura elektronického podpisu

Jedná se o soubory veřejného a osobního klíče. Veřejný klíč slouží ke zveřejnění, a taky k ověření autenticity elektronického podpisu. Osobní klíč musí být naopak velmi pečlivě utajen, protože právě s jeho pomocí vytváří počítač unikátní elektronický podpis ke každé zprávě. Soubory certifikátu mohou být uloženy na harddisku počítače a jsou chráněny PINem. Další možnost je použít nějaké bezpečné úložiště, např. čipovou kartu nebo USB token. V okamžiku podání žádosti generuje kryptografický procesor bezpečného úložiště

dvojici klíčů (veřejný a osobní). Osobní klíč nikdy bezpečné úložiště neopustí.

## 4.3 Získání elektronického podpisu

S bezpečným úložištěm připojeným k počítači s přihlásíte na stránky CA, vyplníte příslušné údaje, kryptografický procesor bezpečného úložiště vygeneruje dvojici klíčů a vytiskne smlouvu. Smlouvu podepíšete buď u notáře nebo na matrice městského úřadu, kde váš podpis ověří. Smlouvu odešlete na adresu CA. Jedna potvrzená kopie se vám vrátí zpět a e-mailem dostanete zprávu odkud a jak si máte nainstalovat vystavený certifikát.

Toto vše platí pro získání elektronického podpisu pro komunikaci s jinými subjekty. Proto ta důvěryhodná certifikační autorita.

## 4.4 Zaručený elektronický podpis a elektronická značka

je jednoznačně spojen(a) s podepisující osobou a umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě (u el.zn. pomocí systémového certifikátu)

byl(a) vytvořen(a) a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou

je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat

## 4.5 Varianty použití elektronického podpisu

Obecně se dá říci, že elektronické podpisy jsou nejčastěji používány:

- pro vazby typu smluv v otevřených sítích (např. elektronický obchod, finanční transakce)
- v uzavřených systémech (Intranety)
- pro osobní účely
- pouze pro identifikační a autorizační účely (oprávnění přístupu do výpočetního systému)
- identifikace webového serveru
- pro oficiální komunikaci s veřejnými institucemi (daňová přiznání, přenos dokumentů s právními důsledky).

## 4.6 Akreditované certifikační autority

Akreditovaná CA je nutná pro komunikaci se státní správou.

- Česká pošta
- První certifikační autorita
- eIDENTITY

Vedle akreditovaných existuje řada neakreditovaných certifikačních autorit, které pro svou činnost akreditaci nepotřebují – např.serverové certifikáty umožňující komunikaci se „správným“, ne podvrženým serverem (pharming).

# 5 DLOUHODOBÉ UKLÁDÁNÍ A ARCHIVACE

Dlouhodobé uchovávání elektronických dokumentů se využívá pro dokumenty v původní elektronické formě nebo pro dokumenty digitalizované dodatečně.

U elektronicky uložených dokumentů potřebujeme zajistit tři hlavní body:

1) Dlouhodobou čitelnost nosičů s uloženými daty
2) Dlouhodobou interpretovatelnost dat uložených na nosičích
3) Zachování právní validity dokumentů

## 5.1 Nosiče dat

Pro archivaci dat se používají magnetické nosiče, zejména magnetické pásky.

Dnes se odborníci kloní k optickým nosičům, tedy k CD-R a CD-ROM. U CD-R jsou totiž měřitelné parametry stárnutí. Životnost dat při archivaci na kvalitních CD médiích s ochranou proti UV se uvádí až 120 let.

Je pravděpodobné, že časem bude tato technologie plně nahrazena technologií DVD-ROM., která disponuje větší kapacitou na stejně velkém disku.

## 5.2 Čitelnost nosičů

Životnost nosičů dat je vlivem působení okolních vlivů omezena. Pro magnetická média uplynula doba jejich použitelnosti a tímto nejstarším obdobím již nemá cenu se zabývat. Stejně ohroženy jsou však i novější elektronické dokumenty. Proto je nutné v určitých intervalech data přenášet na nové nosiče. Tento proces se nazývá **transference** a je třeba ho provádět pravidelně a důsledně.

## 5.3 Interpretovatelnost dat

Je třeba zajistit, aby uložená data bylo možno číst i po dlouhé době. To je ohroženo neustálým vývojem informačních technologií.

Jsou dvě možnosti jak toho dosáhnout

- otevřené formáty
- přeformátování dat

### 5.3.1 Otevřené formáty

Jsou to takové formáty, u nichž jsou známy zdrojové kódy. Příkladem jsou formáty TXT, XML (SGML), JPEG, TIFF a další.

K přečtení takových souborů je třeba vytvořit prostředí, ve kterém budou data čitelná. To se nazývá emulace. K emulaci jsou zapotřebí tzv. metadata, která poskytují informace uložených datech. To znamená, že již při vzniku formátu je třeba spolu s daty vytvořit i metadata, tedy data o datech a uložit je buď spolu s daty nebo na jiné úložiště. V tom případě musí být zajištěna pozdější možnost jednoznačně spojit správná data s příslušnými metadata.

### 5.3.2 Přeformátování dat

Druhou možností je přeformátování dat do nového čitelného formátu nazývané migrací dat. Migrace je řešením i v případě morálního zastarání nosiče. Při migraci dat dochází však ke změně struktury souboru. U elektronicky podepsaných dokumentů tak vzniká problém se ztrátou integrity.

## 5.4 Právní validita

Hobza: „Z právního hlediska je podstatná platnost elektronického podpisu pouze při jeho vytváření. Pokud byl elektronický podpis zneplatněný nebo jeho platnost uplynula až po vytvoření elektronického podpisu, nemá to vliv na právní validitu podepsaného dokumentu, a nemá tedy význam zkoumat platnost elektronického podpisu k jinému okamžiku než k okamžiku jeho vytvoření.“[5]

Z toho vyplývá možnost použití časového razítka při podepisování dokumentu.

Archivaci elektronických dokumentů se již zabývá řada zahraničních archivů. Žádný český veřejný archiv se však této problematice systematicky nevěnuje. To znamená, že u nás ještě není právní validita dlouhodobě uchovávaných elektronicky podepsaných dokumentů nijak vyřešena. Jedinou možností zatím je uchovávání takových dokumentů v listinné podobě.

# 6 EXISTUJÍCÍ ŘEŠENÍ

## 6.1 PGP

Systém bezpečné elektronická komunikace v podniku i mezi partnery

Jejím cílem je ochrana znalostí a dat. Je založena na principech symetrické a asymetrické kryptografie.

Musí splňovat následující požadavky :

**důvěrnost informací** - systém musí zabezpečit, že neautorizované subjekty nebudou mít možnost přístupu k důvěrným informacím

**integrita** - systém musí zabezpečit informace proti neautorizované modifikaci

**neodmítnutelnost odpovědnosti** - systém musí zabezpečit prevenci proti ztrátě schopnosti, přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za odeslání, případně přijetí zprávy

Podepisující strana vezme příslušný dokument v elektronické podobě a zašifruje ho svým soukromým klíčem. Vhodnou cestou přitom zveřejní (nebo již má zveřejněn) odpovídající veřejný klíč. Kdokoliv, kdo má přístup k tomuto veřejnému klíči (a ověří si, kdo je jeho skutečným majitelem), může nyní pomocí tohoto veřejného klíče dešifrovat podepsaný dokument a ověřit tak příslušný podpis tohoto dokumentu.

### 6.1.1 PGP – Pretty Good Privacy

Pro komunikaci a užití elektronického podpisu v rámci, dejme tomu, menší firmy je vhodný systém PGP, který bude ovládat vnitřní autorita firmy, zpravidla správce sítě.

PGP je kombinovaný šifrovací systém. Navenek se jeví jako program s veřejným šifrovacím klíčem, plně využívající asymetrického šifrování.

To se však ve skutečnosti používá pouze pro zakódování klíče symetrické šifry, kterou je pak zašifrována samotná zpráva. Digitálním podpisem je kontrolní součet zprávy (hash), který je zašifrován asymetrickou šifrou.

Možnosti použití (komerční i nekomerční – volné použití s omezenou funkčností)

- Elektronický podpis
- Ochrana souborů

- Ochrana disků
- Ochrana na úrovni serverů

### 6.1.2 Princip šifry PGP

PGP používá asymetrické šifry RSA.

Algoritmus je založen na jednoduché myšlence, že můžeme poměrně snadno vynásobit dvě velká čísla, je však časově velice náročné rozložit takový součin na prvočinitele.

Je známo, že klíč velikosti 384 bitů byl rozluštěn během několika měsíců neustálé práce několika desítek až stovek spolupracujících počítačů. Běžně používané velikosti klíče 1024 až 2048 bitů jsou dnes zatím bezpečné.

RSA pracuje při poměrně malém základu s vysokými čísly. Šifrování velkých zpráv s pomocí RSA by bylo časově ohromně náročné. Stejně je tomu i u jiných asymetrických algoritmů. PGP tedy kóduje text symetrickým algoritmem, jehož implementace je mnohem rychlejší. PGP nejprve vygeneruje náhodný klíč pro symetrickou šifru, tento klíč zakóduje do zprávy s pomocí veřejného RSA nebo DH klíče příjemce, a celou zprávu pak zakóduje symetrickou šifrou. Příjemce nejprve s pomocí svého soukromého RSA nebo DH klíče zjistí klíč pro symetrickou šifru, s jehož pomocí pak rozkóduje samotnou zprávu.

### 6.1.3 Elektronické podpisy v PGP

PGP řeší také problém ověření obsahu a identifikace autora zprávy tzv. elektronickými podpisy. Nejprve je nutné zvolit nějaký vzor, který umožní ověřit, že zpráva nebyla změněna poté co ji autor sestavil. K tomu slouží algoritmus MD5 nebo SHA-1 pro vytvoření kontrolního součtu zprávy. Tento kontrolní součet, který by při jakékoli změně zprávy byl porušen, se pak přidá ke zprávě, zašifrovaný autorovým soukromým klíčem. Příjemce pak s pomocí autorova veřejného klíče rozkóduje kontrolní součet zprávy a ověří, jestli zpráva nebyla pozměněna (či podvržena).

### 6.1.4 Správa klíčů v PGP

Důležitou součástí PGP je správa klíčů. Uživatel musí mít alespoň jeden pár soukromý klíč-veřejný klíč. Soukromá část zůstává na disku počítače a je zabezpečena heslem. Heslo musí být dostatečně bezpečné.

Měli byste si také zachovat kopii Vašeho soukromého klíče, protože jeho ztrátou přijdete o možnost přečíst zprávy Vám určené. Tuto kopii uložte na bezpečném místě, je ale také chráněna stejným heslem.

Při komunikaci s jinými osobami budete potřebovat jejich veřejné klíče. Tento klíč má několik atributů:

*ID - binární číslo*, jednoznačná identifikace, např. 0x59159CF1

*User ID* - identifikace osoby (skupiny osob), kterým klíč patří. Každý klíč může mít více takových uživatelských jmen.

*Signature* - podpis jiným klíčem, vyjádření jistoty jiné osoby, že klíč patří skutečně této osobě. Podpisů může být opět libovolné množství. Podepisují se jednotlivá User ID, dáváte tedy pouze najevo, že podepsané uvedené uživatelské jméno není podvrh.

*Photo* - od verze 6.0 lze do klíčů vkládat fotografie uživatele ve formátech JPEG a BMP.

*Data* - samotný klíč, obsah závisí na typu klíče.

Podepsáním cizího klíče vyjádříte jistotu, že daný klíč je pravý, tj. že připojené uživatelské jméno odpovídá skutečnému vlastníkovi klíče. Při práci s každým klíčem Vás PGP upozorní, jestli jste daný klíč podepsali nebo ne a tedy jakou máte v tento klíč důvěru. Pokud klíč podepíšete, můžete dále zvolit míru Vaší důvěry v tento klíč. Podepsaný klíč lze vystavit na Internetu, aby ho mohli používat jiní partneři dané osoby a aby měli od Vás potvrzeno, že máte Vy v tento klíč důvěru.

### 6.1.5 Správce veřejných klíčů v PGP

Je to autorita v ČR nebo si klient může vybrat kteroukoliv autoritu? Filozofie užívání PGP je postavena na vzájemné důvěře konkrétních dvou komunikujících subjektů, které navzájem věří obdrženým veřejným klíčům. (Ověření může např. proběhnout telefonicky, nebo pomocí tzv. Fingerprintu - otisku veřejného klíče). PGP tedy žádnou autoritu nevyžaduje. Při tvorbě klíčů (páru) v PGP Desktop produktech máte možnost vystavit svůj veřejný klíč na PGP serveru http://keyserver.pgp.com. Tento server ověřuje, že jste k vámi vytvořenému veřejnému klíči uvedl reálné identifikační údaje (že např. uvedená emailová adresa opravdu existuje). Nejedná se v žádném případě o certifikační autoritu. Obecně však key servery toto nedělají.

### 6.1.6 Šifrování pošty v PGP

Implicitně je politika nastavena tak, že v Outlooku stačí zprávu označit jako důvěrnou a bude automaticky zašifrována, případně předmět zprávy doplníte o [PGP]. Navíc je také výchozí politika doplněna o pravidlo snažící se šifrovat komukoliv, jehož veřejný klíč se podaří získat. Toto implicitní nastavení se dá změnit deaktivací defaultních politik a vytvořením politiky vlastní. Otevřete PGP Desktop (buď přes Nabídku Start, nebo přes ikonu v Oznamovací oblasti – sys tray, kde zvolíte Open PGP Desktop). Zvolte PGP Messaging a v pravé části okna se objeví seznam politik. Klikněte na Edit policies a dostanete se do prostředí, kde lze politiky upravovat. Ty, které mají v závorce default a jsou zaškrtnuty, je třeba v tomto případě deaktivovat (dvojkliknutím na politiku zjistíte jak je nastavena). Úplně vpravo máte další možnosti: Edit nebo View Policy, New Policy, Remove Policy, Duplicate Policy a konečně šipky pro posun politiky v seznamu nahoru či dolů, čímž stanovujeme jejich prioritu. Klikněte na New Policy a vytvořte politiku šifrování dle vašich požadavků.

Analogicky je možné vytvořit politiku pro podepisování. Nezapomeňte ji pak v seznamu aktivních (zaškrtnutých) politik šipkami posunout na správné místo, aby byla zaručena její skutečná funkčnost.

### 6.1.7 Kdy šifrovat a kdy podepisovat poštu

Šifrování i podepisování pošty využívá asymetrické kryptografie. Pokud chci mail šifrovat, musím mít veřejnou část klíče příjemce. Pomocí tohoto klíče je potřeba mail zašifrovat. U podepisování zprávy je situace opačná. Mail podepíšeme svým soukromým klíčem, ověřit jeho pravost si může každý pomocí mého veřejného klíče. Tj. nemusím mít veřejnou část klíče adresáta. Šifrování zajistí, že zpráva není pro nikoho v rámci přenosu Internetem čitelná (zajistí zachování důvěrnosti), podepisování pouze zajistí, že zpráva nemůže být cestou Internetem změněna (zpráva je čitelná ve své standardní podobě, pokud by ji ale někdo cestou změnil, adresát bude informován formou „neplatnosti podpisu“). Pokud chceme zajistit zachování důvěrnosti i jistotu autentičnosti, je potřeba zprávu zašifrovat i podepsat.

## 6.2 Adobe Acrobat

Základem softwaru Adobe Acrobat je práce s formátem PDF.

## 6.3 Verze Adobe Acrobat

Řada produktů Adobe Acrobat 8 obsahuje volitelně verze Standard, Professional, 3D, Elements a bezplatný Reader.

- **Elements** je multilicenční a je určena zejména pro vytváření, sdílení a distribuci bezpečných PDF dokumentů a jejich integraci s aplikacemi MS Office a IT infrastrukturou.
- **Standard** kromě toho umožňuje kombinaci souborů z různých aplikací, využití recenzních nástrojů, digitální podpisy apod.
- **Professional** pak umožňuje i využití dalších pokročilých funkcí včetně propracovaného sběru dat.
- **3D** je určena zejména konstruktérům, projektantům a autorům technické dokumentace, umožňuje využívat dokumentů z CAD aplikací a zprostředkovat je i partnerům, kteří nemají k dispozici náročný CAD software.
- **Reader** je freeware a je určen zejména ke čtení dokumentů.

## 6.4 Jak elektronický podpis v PDF funguje

Krejčí: „Obdobně jako v případně ručního podpisu představuje i elektronický podpis prostředek autorizace stavu určitého dokumentu jednou nebo více osobami. Na rozdíl od svého klasického předchůdce přináší ovšem vedle této základní funkce řadu dalších nových možností. Při jeho nasazení lze totiž nejen ověřovat autenticitu podepisujících osob, ale rovněž trasovat změny, které byly v dokumentu provedeny od jeho podepsání. Dále může být nosičem nejrůznějších důležitých informací, jako jsou například údaje o čase, místu a důvodech podpisu či uživatelích, kteří dokument podepsali.“[9]

### 6.4.1 Acrobat Self-Sign Security

Výchozí ovladač podpisů je Acrobat Self-Sign Security, poskytovaný samotnou společností Adobe.

Systém nabízený Acrobat Self-Sign Security vychází, obdobně jako jiná řešení, z koncepce tzv. soukromého a veřejného klíče.

### 6.4.2 Direct-trust

Systém sdílení certifikátů se označuje pojmem direct-trust neboli systém přímé důvěry,

neboť nevyžaduje vstup třetí strany, tzv. certifikační autority, přidělující certifikáty a mechanismy jejich ověřování. Svým zaměřením je tedy vhodný spíše pro uzavřená workflow nežli pro veřejné transakce typu elektronického obchodování či kontaktu se státní správou.

# II. PRAKTICKÁ ČÁST

# 7 CHARAKTERISTIKA FIRMY AEV

Obchodní jméno : **AEV společnost s ručením omezeným**

Sídlo: Jožky Silného 2783, 767 01 Kroměříž

„AEV byla založena v roce 1991 se zaměřením na vývoj a výrobu technicky pokročilých produktů pro automobilní a letecký průmysl. Společnost dodává díly přímo do prvovýroby nebo nepřímo jako subdodavatel. Přes 15 let zkušeností v návrhu a výrobě automobilových a leteckých elektronických přístrojů a systémů si společnost získala pověst flexibilního a stabilního dodavatele. V úzké spolupráci se svými zákazníky jsou připravovány inovace a nové produkty. Společnost je držitelem oprávnění na výrobu elektronických přístrojů pro vojenské a civilní letectví.“[1]

Administrativní budova a výrobní haly firmy se rozkládají na ploše $7.354\,\mathrm{m}^2$. Areál firmy AEV má rozlohu $15.935\,\mathrm{m}^2$, celý pozemek $60.334\,\mathrm{m}^2$. Viz Obrázek 6.

## 7.1 Předmět podnikání

- Výrobní činnost: Výroba elektrických a elektronických přístrojů
- Obchodní činnost: Koupě zboží za účelem dalšího prodeje a prodej

## 7.2 Členění firmy a počet zaměstnanců

Firma AEV má 112 zaměstnanců, viz Tabulka 2, a je členěna na útvary:

1. Útvar prodeje – prodej, expedice

2. Útvar ekonomický – účtárna, personální

3. Útvar technický – vývoj, technologie, vývojová dílna, správce sítě, vrátní

4. Útvar výroby – mistři, dispečer, plánovači, výrobní technik, provoz

5. Útvar jakosti – kvalita, kontrola, ekolog

6. Útvar nákupu – nákup, příjem, sklad

## 7.3 Certifikáty a osvědčení

Firma AEV je v současné době držitelem těchto certifikátů a osvědčení:

- ISO 9001:2000
- VDA 6.1
- Osvědčení k výrobě výrobků vojenské letecké techniky
- Oprávnění k projektování letadlových zařízení a jejich změn

Tabulka 2 Počet zaměstnanců AEV

| | |
|---|---|
| Prodej | 7 |
| Ekonomika | 6 |
| Technický útvar | 31 |
| Výroba | 53 |
| Jakost | 8 |
| Nákup | 7 |
| CELKEM | 112 |

Obrázek 6 Areál AEV spol. s r.o., Kroměříž

# 8 SOUČASNÝ STAV SPRÁVY DOKUMENTŮ

## 8.1 Počítačová síť v AEV

Počítačová síť ve firmě je postavena na technologii Fast Ethernet o rychlosti 100 Mb/s. Základem sítě jsou router, Novell server, Windows server a 6 managementovatelných switchů HP, navzájem propojených metalickými UTP kabely resp. optickým kabelem. Switche jsou propojeny UTP kabely do strukturované kabeláže rozvedené po firmě. Router, servery, stanice a tiskárny jsou připojeny do zásuvek strukturované kabeláže.

**Úložištěm dokumentů je server se systémem Novell.**

### 8.1.1 Použité síťové prvky

- 1x router se systémem Linux
- 6x managementovatelný switch, Obrázek 7
- 2x server se systémem Windows 2000 server
- 1x server se systémem Novell
- 1x mail server se systémem Linux
- 63 PC stanic
- 12 notebooků
- 7 síťových tiskáren
- 11 jetdirectů pro tiskárny
- malé switche
- strukturovaná metalická kabeláž UTP
- optické datové vedení

Obrázek 7 Managementovatelný switch HP

### 8.1.2 Umístění a fyzická ochrana

Router, servery a 3 managementovatelné switche jsou umístěny v samostatné místnosti – serverovně, kam mají přístup pouze vybraní zaměstnanci. Elektrický zámek je napojen na systém Cominfo a otevře se jen po přiložení oprávněné karty k čtečce u dveří. Serverovna je umístěna vedle hlavní vrátnice s nepřetržitou službou, je bez oken a její vchod je tedy stále pod kontrolou. Všechna zařízení v serverovně jsou připojena na záložní zdroje UPS, Obrázek 8. Místnost je klimatizovaná.


Obrázek 8 Záložní zdroje UPS v serverovně

## 8.2 Router

Router se systémem Linux má tyto funkce:

a) spojuje síť s internetem, rychlost připojení 3 Mb/s download i upload

b) jako firewall chrání vnitřní síť před útoky z internetu

c) plní funkci DHCP serveru a DNS severu.

Na DHCP severu je nastaven rozsah dynamicky přidělovaných IP adres v rozmezí

192.168.100.220 – 192.168.100.255.

Ostatní adresy v rozmezí 192.168.100.1 – 192.168.100.219 jsou přidělovány pevně k zadaným MAC adresám síťových prvků.

Na routeru je zároveň nastaveno povolení internetu IP adresám v rozmezí 192.168.100.1 – 192.168.100.127 a zakázání internetu IP adresám ve zbylém rozmezí 192.168.100.128 – 192.168.100.255, Tabulka 3.

Tím má správce sítě při zadávání MAC adresy nového síťového zařízení možnost zvolit, zda bude mít zařízení povolení nebo zákaz internetu. Připojí-li se k síti např. počítač bez zadání MAC adresy jeho síťového adaptéru do DHCP, bude mu propůjčena IP adresa z rozmezí 192.168.100.220 – 192.168.100.255 a tím tedy zakázán přístup k internetu.

Tabulka 3 Rozmezí IP adres a jejich nastavení

| **IP nastavené k MAC adresám** | **IP dynamicky** |
|---|---|
| 192.168.100.1 - 192.168.100.219 | 192.168.100.220 - 192.168.100.255 |
| 192.168.100.1 - 192.168.100.127 | 192.168.100.128 - 192.168.100.255 |
| **Internet povolen** | **Internet zakázán** |

## 8.3 MS Windows 2000 Server

Dva servery HP se systémem MS Windows 2000 server

### 8.3.1 Síť Microsoft Windows

Síť Microsoft Windows zajišťuje HP server tc4100 - Pentium III 1400 MHz.

Na tomto serveru mají všichni uživatelé svůj účet a přihlašují se k němu do sítě Windows. Síť se skládá z pracovních skupin – workgroup, tedy bez domén. Uživatelé si mohou mezi sebou sdílet soubory, ale tato síť nemá ve správě dokumentů žádné využití. Je využita zejména pro přístup k firemnímu informačnímu systému a k síťovým tiskárnám.

Je zde nainstalován informační systém Helios Orange a běží zde databázový systém Microsoft SQL Server 2000. Server funguje i jako tiskový server – printserver. Jsou na něm nainstalovány a sdíleny všechny síťové tiskárny resp. tiskové jetdirecty.

### 8.3.2 Cominfo – docházkový systém

Druhý server se systémem Windows je HP server NetServer LC 3 - Pentium II 450 MHz.

Na serveru je systém Cominfo pro docházku a stravování a rovněž databázový systém Microsoft SQL Server 2000.

Na tomto serveru mají svůj účet pouze uživatelé pracující s docházkou a objednávkovým systémem stravy CardPay.

## 8.4 Novell server

**Novell server funguje jako úložiště všech dokumentů ve firmě.**

Systém Novell 4.11 na HP NetServer E 55 Gold - Pentium III 500MHz, Obrázek 9.

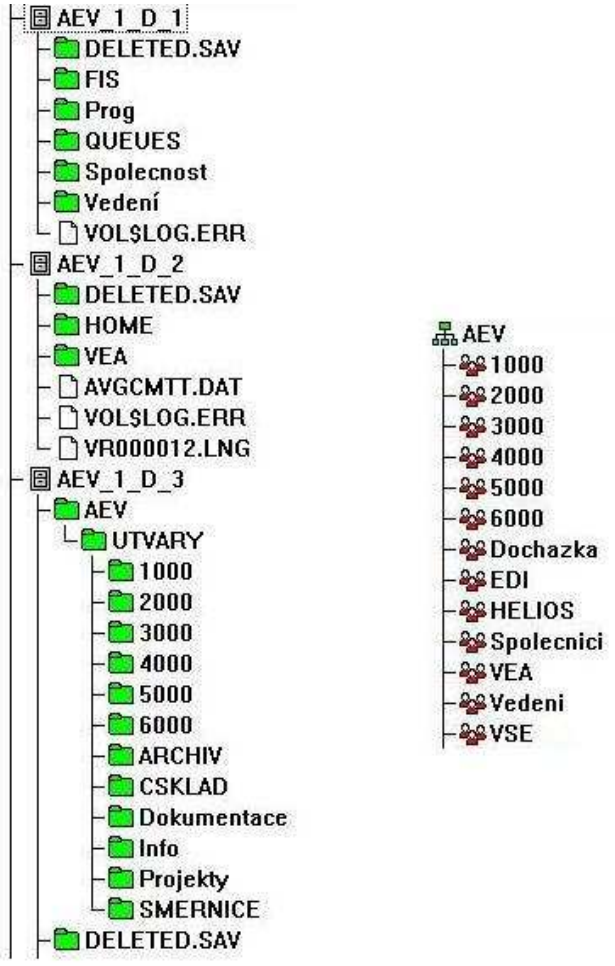
Obrázek 9 Server HP NetServer E 55 Gold

### 8.4.1 Síť Novell NetWare

Pracuje s protokolem IPX/SPX. Data proto nelze přenášet cestou, která tento protokol nepodporuje, např. přes internet, což je v našem případě žádoucí.

#### *8.4.1.1 Struktura*

V Novellu je vytvořen Tree – strom AEV, obsahuje objekty – skupiny, uživatele, svazky. Svazky obsahují kontejnery. Kontejnery jsou jako adresáře v souborovém systému, obsahují další kontejnery a soubory, viz Obrázek 10.




Obrázek 10 Novell – svazky, kontejnery, skupiny

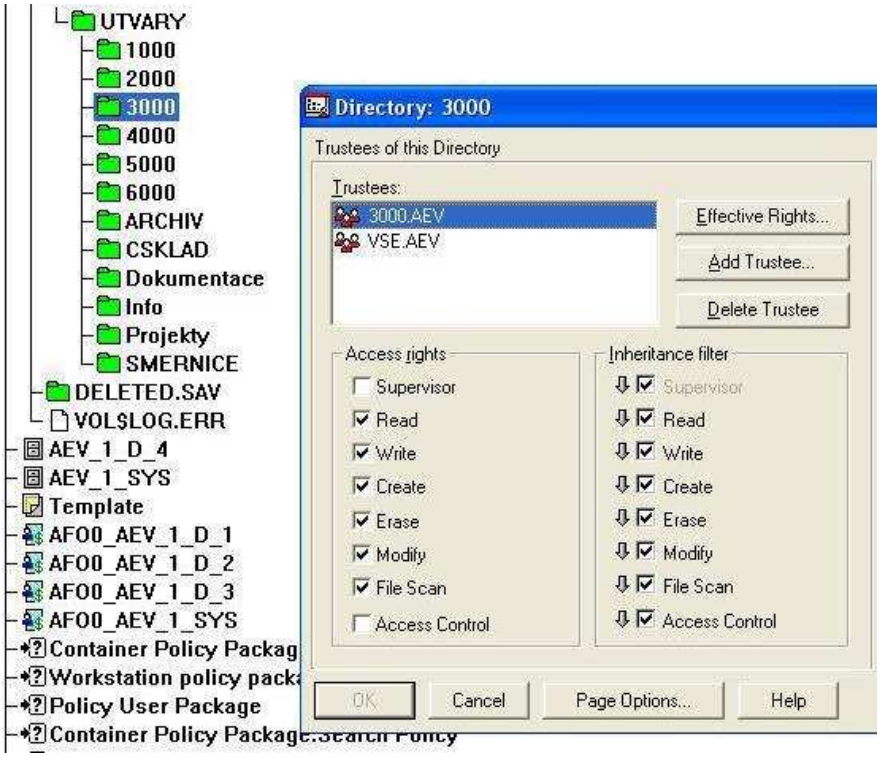
#### *8.4.1.2 Nastavení práv*

Pomocí nástroje NetWare Administrator se nastavují práva. Jsou zde vytvořeny skupiny uživatelů podle útvarů, funkcí apod. Skupiny mají přidělená práva. Ve výchozím nastavení kontejneru jsou všechna práva zakázána, tedy co není povoleno, je zakázáno. Dodatečně se

skupinám nebo jednotlivcům přidělují práva ke kontejnerům, viz Obrázek 11 a Obrázek 12. Práva se dědí v hierarchii kontejnerů směrem dolů.

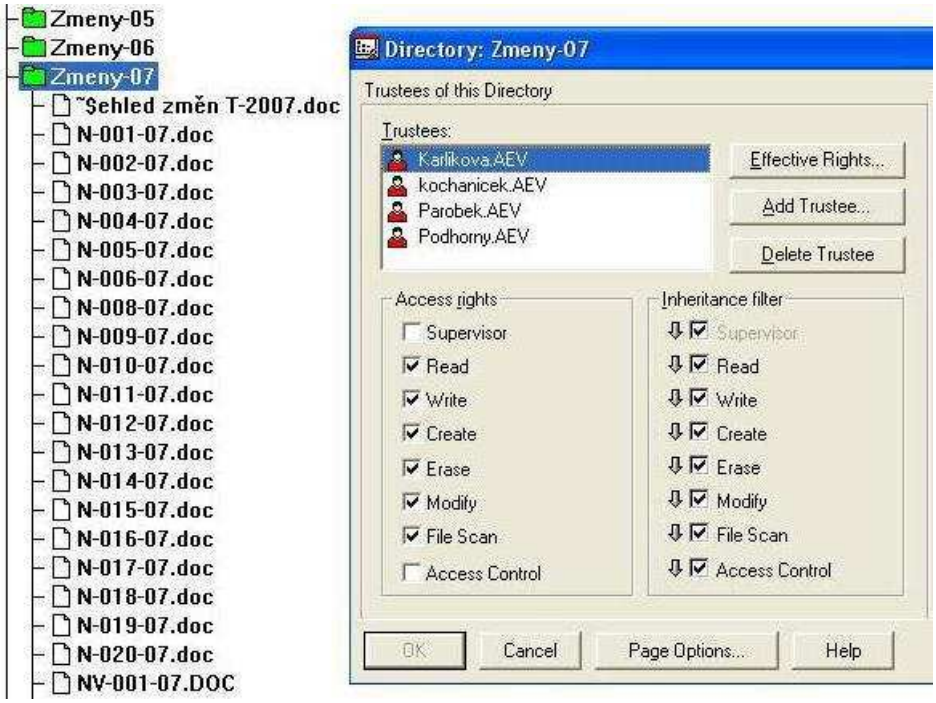
Typy práv:

- Supervisor – práva administrátora
- Read - číst
- Write - zapisovat
- Create - vytvářet
- Erase - mazat
- Modify - upravovat
- File Scan – spouštění soborů
- Access Control – řízení práv




Obrázek 11 Novell – nastavení práv skupinám

Přidá-li se nový uživatel, většinou stačí, když je zařazen do skupiny nebo skupin, aby získal příslušná práva k souborům, ke kterým bude potřebovat. V případě potřeby se práva jednotlivým uživatelům dolaďují individuelně, viz Obrázek 12. Práva nastavuje správce sítě na pokyn vedoucích útvarů.




Obrázek 12 Novell – nastavení práv jednotlivcům

#### *8.4.1.3 Přihlašování do sítě Novell NetWare*

Na uživatelských stanicích PC a notebookách je nainstalován klient pro přihlášení do sítě Novell NetWare.

Přihlašovací tabulka Novell Client, viz Obrázek 13, slouží pro

- přihlášení do sítě Novell NetWare
- přihlášení do systému Windows daného počítače
- přihlášení do sítě MS Windows

Pro zjednodušení přihlášení mají uživatelé stejná uživatelská jména a hesla do obou sítí i do „svých“ počítačů. Po zaškrtnutí okénka „Workstation only“ a kliknutí na „OK“ dojde k vynechání přihlášen do sítě NetWare a uživatel se přihlásí pouze do systému Windows počítače, resp. i do sítě MS Windows. V prostředí Windows se pomocí klienta Novell Client může přihlásit do sítě NetWare dodatečně a to i jiný uživatel, než který je přihlášen do Windows.

Příklad: Správce sítě se chce přihlásit na počítači jiného uživatele do systému Windows a nemá na něm nastaven vlastní účet. Zná jen heslo k účtu „Administrator“. Kdyby toto jméno a heslo zadal do přihlášení k síti Novell, bylo by odmítnuto jako neplatné přihlášení.

Zatrhne tedy okénko „Workstation only“ a přihlášení do Novell bude vynecháno. Proběhne pouze přihlášení do systému počítače. K síti Novell se může přihlásit dodatečně příkazem „NetWare Login“ a zadáním svých přihlašovacích údajů do NetWare.

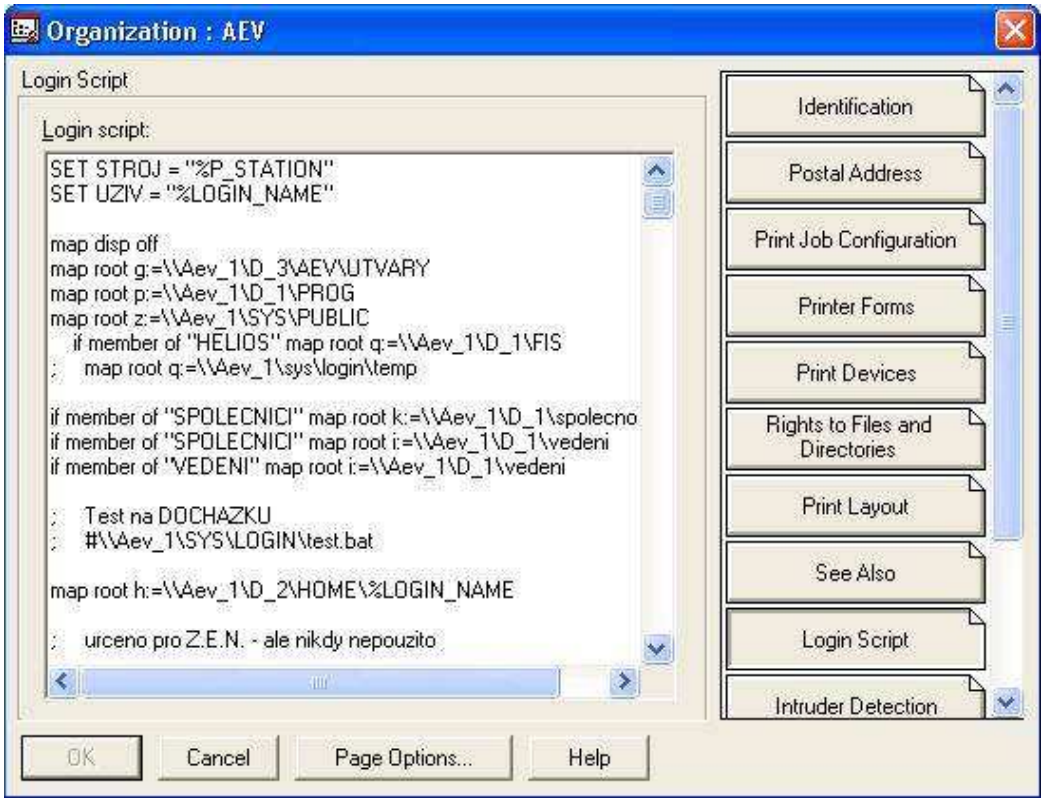

Obrázek 13 Novell klient pro prostředí Windows

#### *8.4.1.4 Mapování*

Aby uživatelé mohli v prostředí Windows pracovat se svazky a kontejnery Novell, musí se do Windows namapovat jako síťové jednotky.

Uživatelské skupiny mají v přihlašovacím skriptu zadán příkaz k mapování určitých svazků a adresářů Novellu jako na určené síťové jednotky, viz Obrázek 14. Přidá-li se tedy do systému Novell nový uživatel, stačí ho přidělit do skupiny nebo skupin a kromě práv získá i nastavené namapování svazků. Další výhodou je, že se uživatel může přihlásit do systému Novell z kteréhokoli počítače a má dostupné správné namapování a práva.

Kromě mapování pomocí Login Skriptu je možno na kterékoli stanici provézt pomocí Novell klienta ruční namapování nějakého svazku nebo kontejneru a to buď jednorázově nebo trvale pro každé přihlášení.




Obrázek 14 Novell – Login Script

## 8.5 Stanice PC a notebooky

K podnikové síti v AEV je připojeno 63 PC.

### 8.5.1 Kancelářské počítače

Většina počítačů je používána pro kancelářskou resp. konstruktérskou práci. Tyto počítače pracují s operačními systémy Microsoft Windows 2000 Professional nebo Microsoft Windows XP Professional. Aby uživatelé měli přístup k firemním dokumentům, je na počítačích nainstalován Novell Client pro přihlášení do sítě Novell NetWare. Protože síť Novell NetWare v AEV pracuje na protokolu IPX/SPX, musí být tento protokol nainstalován i na počítačích.

### 8.5.2 Počítače ve výrobě

V síti je několik počítačů používaných ve výrobním procesu. Tyto počítače poskytují data výrobním zařízením, řídí programovací a testovací zařízení apod. Pracují pod operačními systémy MS Windows 2000 Professional, Windows 98 i Windows 95. Protože se na nich

nepracuje s firemními dokumenty, není na nich nainstalovaný klient sítě NetWare ani protokol IPX/SPX.

### 8.5.3 Přenosné počítače notebooky

Kromě PC se k firemní síti připojují zaměstnanci i s notebooky, těch je celkem 12. Firemní notebooky v AEV mají operační systém MS Windows XP Professional. Je na nich rovněž nainstalován Novell Client a protokol IPX/SPX. Připojují se přípojkami UTP do zásuvek strukturované kabeláže, buď přímo nebo prostřednictvím tzv. dokovacích stanic – dock station. Bezdrátová síť není v AEV použita.

Na všech stanicích je nainstalován antivirový systém NOD32 s centrální správou.

## 8.6 Poštovní server

Poštovní server se systémem Linux běží na stroji pro běžné PC s procesorem AMD Sempron 2800+ o taktu 2000 MHz.

Systém je spuštěn z CD-ROM. Zprávy se ukládají do mail boxů na pevný disk o velikosti 200 GB. Ten se pravidelně zrcadlí na druhý pevný disk o stejné velikosti.

Uživatelský přístup k mailům je možný přes webové rozhraní SquirrelMail, viz Obrázek 15, nebo prostřednictvím nějakého běžné poštovního klienta s protokoly POP3 nebo IMAP. V AEV se jako poštovní klient používají převážně Outlook Express a MS Outlook. Někteří uživatelé dávají přednost klientům Mozilla Thunderbird nebo Netscape.

Příchozí a odchozí pošta je kontrolována antivirovým systémem NOD32 Antivirus System for Linux Mail Server.


Obrázek 15 SquirrelMail webové rozhraní mailové schránky

## 8.7 Typy používaných dokumentů

- Otevřený textový formát - TXT
- Dokumenty balíku MS Office – DOC, XLS, PPS, PPT
- Dokumenty ve formátu Adobe – PDF
- Výkresy formátu CAD – DWG, DXF
- Obrázky ve formátech – JPG, JPEG, TIF, GIF, BMP
- Soubory štítků – BTW, LBL

## 8.8 Zálohování dokumentů

Zálohování dokumentů provádí správce sítě.

- denní záloha
- měsíční záloha

Denní i měsíční zálohování se provádí ručně do archivu rar.

### 8.8.1 Denní záloha dokumentů

Pomocí softwaru WinRar vytváří správce každý den přírůstkový archiv všech dokumentů a ukládá ho do svého počítače na pevný disk. Vždy je tedy k dispozici archiv denních přírůstků aktuálního měsíce.

### 8.8.2 Měsíční záloha dokumentů

Jednou za měsíc vždy první den v měsíci vytvoří pomocí WinRar archivy kompletně všech dokumentů podle útvarů. Tyto archivy poté vypálí na nosiče DVD a označené uloží v serverovně.

## 8.9 Vyhodnocení stavu

- Přístupová práva k dokumentům zajišťuje zastaralá verze Novell NetWare 4.11
- Zabezpečení dokumentů v současné době nevyhovující
- Zálohování dokumentů nevyhovující
- Archivace v podstatě žádná, pouze ukládání měsíčních záloh, zdlouhavé vyhledávání
- Přehlednost dokumentů nedostačující
- Vyhledávání obtížné
- Kontrola změn a oběhu dokumentů žádná
- Hardware zastaralý, hrozí selhání systému
- Ochrana úložiště umístěním je dostačující
- Zajištění nepřerušitelného zdroje elektrické energie pro úložiště dat je vyhovující

## 8.10 Doporučení

Doporučuji zcela změnit systém práce s dokumenty v AEV. Navrhuji

- ✓ zavést ucelenou správu dokumentů
- ✓ nový hardware pro ukládání dokumentů
- ✓ zálohovací zařízení

# 9 POŽADAVKY NA SPRÁVU DOKUMENTŮ V AEV

Požadavek managementu firmy AEV na správu dokumentů je v podstatě shodný jako mé doporučení. To znamená zavést ucelenou správu dokumentů s důrazem na

- Zefektivnění práce s dokumenty
- Podstatné zlepšení bezpečnosti dokumentů jak z hlediska přístupu tak z hlediska uchování dokumentů a toku dokumentu v rámci firmy
- Přizpůsobení nakládání s dokumenty standardu norem ISO 9000
- Zavedení autorizace dokumentů a nepopiratelnosti autorství
- Zavést určeným pracovníkům elektronický podpis pro komunikaci s úřady státní správy

# 10 MOŽNOSTI ŘEŠENÍ

## 10.1 Sova systems

„SOVA SYSTEMS Č .R., spol. s r.o. je členem sdružení firem SOVA NET (vývoj intra/internetové technologie) a SOVA STUDIO (školící středisko).

Profiluje jako společnost se znalostí implementace informačních technologií. Zkušenost týmu pracovníků je opřena o inženýrský přístup, schopnost analýzy a komplexního řešení problémů u klienta.

Náročnost řešení je individuálně upravena dle skutečných potřeb zákazníka s respektováním jeho zaběhlých zvyklostí, popřípadě procesů popsaných normami ISO.“[14]

### 10.1.1 Automanager TeamWork

Automanager TeamWork je nástroj na správu technické dokumentace vhodný zejména pro firmy s velkými nároky na práci s výkresovou dokumentací. Je určen pro práci s dokumenty, jejich archivaci a zajištění bezpečnosti dokumentů jak z hlediska přístupu tak z hlediska uchování dokumentů.

Umožňuje přehled o jednotlivých revizích daného dokumentu, o toku dokumentu v rámci firmy a způsob schvalovacího řízení a samotné archivace.

AutoManager TeamWork plně spolupracuje s programy AutoCAD, Mechanical Desktop, Inventor a Solidworks, s náhledováním a úpravami bez nutnosti mít tyto aplikace nainstalované. Umožňuje náhled i dvou výkresů najednou a automatické vyhledání rozdílů v nich. Obsahuje přehledné reference, možnost jednoduchého workflow. Grafické workflow popisuje celou cestu dokumentu od nápadu až po realizaci, s přesně stanovenými pravidly, na první pohled je vidět kdo s dokumentem pracuje, kdo jej schvaluje a kdo za něho zodpovídá.

Pro firmy pracující dle standardu ISO 9000 řeší jednoznačnou definici postupů práce s dokumentem a protokolování všech jeho změn.

**Hlavní výhody:**

- Plná integrace do vybraných CAD aplikací.
- Řízení správy modelů, sestav výkresů a definice struktur.

- Rychlé vyhledávání modelů, sestav i jednotlivých výkresů, dílů podle zadaných atributů a šablon jako jsou: číslo výkresu, popis, jména výkresu. Je možné vyhledávat podle tzv. databázových kritérií, jako jsou revize nebo katalogové číslo.
- Zachování revizního cyklu pro všechny spravované dokumenty a soubory.
- Využití dat z konstrukčního kusovníku vytvořeného v daném CAD systému.
- Podpora vkládání křížových, externích referencí (X/REF).
- Synchronizace definovaných atributů mezi systémem AmTeam Work a rohovým razítkem daného CAD výkresu.

### 10.1.2 Automanager Meridian

AutoManager Meridian je komplexní systém správy dokumentace založený na architektuře client/server. Je dimenzovatelný na různé úrovně řešení od práce na oddělení až po divizní management v návaznosti propojení na ostatní informační systémy společnosti. Vytváří bezpečné prostředí pro dokumenty užitím "trezorového" konceptu. Zajišťuje transparentní správu dokumentace integrací do operačního systému Microsoft Windows. Tato integrace se týká také Microsoft Office aplikací (Word, Excel, Outlook...) a CAD aplikací firem Autodesk, Bentley a SolidWorks.

**Disponuje 4 druhy klientů:**

- Power User - klient s plnou integrací CAD systémů. Hlavní využití konstrukce, projekce.
- Office Client - klient bez CAD integrace systémů. Hlavní využití v oblasti editace MS Office.
- Offline Client - pro spolupráci mimo prostředí, je ovšem potřeba návaznost na Office klienta..
- Web Client - použitelný pro uživatele s možnosti vzdáleného přístupu do systému.

Systém podporuje požadavky jakostních norem třídy ISO 9000, 14 000 a dalších. Použitím ODMA technologie, mohou být produkty AutoManager Meridian integrovány do Windows, CAD a Office programů. AutoManager Meridian je možné propojit s různými ERP systémy.

### 10.1.3 DOCLINE

Originální český intranetový a internetový systém pro externí i interní komunikaci. Je zaměřen na sledování vývoje projektů a jejich dokumentů. Systém umožní oprávněným uživatelům bezpečný přístup k vedení jednotlivých projektů a ke správě dokumentů libovolného typu, které jsou součástí těchto projektů. Přístup k systému je na základě zabezpečeného protokolu www prohlížeče.

Systém umožňuje zabezpečený přístup nejen uživatelům na lokální firemní síti, ale také externím uživatelům - investoři, partneři, dodavatelé, zákazníci. K maximální bezpečnosti a ochraně dat slouží sofistikovaný šifrovaný způsob ukládání dat na diskový prostor. Licencování systému je na principu plovoucích licencí, kdy systém kontroluje počet současně připojených uživatelů do systému.

DOCLINE je vhodný právě tam, kde firma sdílí data na síťovém disku a není přitom zabezpečena integrita, bezpečnost a jednoznačná struktura takto uložených dat. Tento systém řeší sledovanost dokumentů dle autora, data vložení, aktualizace a dalších atributů definovaných na kartách dokumentů. Jednotlivé typy dokumentů mají různé karty. A je možné je uživatelsky přizpůsobit. Ke každému dokumentu se automaticky vedou revize. To znamená že je přístup vždy k aktuálním informacím sdílených celým pracovním týmem.

### 10.1.4 xWORK

Systém xWORK slouží jako prostor pro snadné vykazování činností vytvořený na základě zobrazených úkolů, aktivit, poznámek a dokumentů.

Přes rozhraní diáře si uživatel může vložit jakýkoliv možný objekt v xWORK, tzn. aktivitu v diáři, úkol, kontakt, poznámku.

Ke každému objektu je možno přiřadit dokument. Ke každé aktivitě lze přiřadit úkol, kontakt, dokument, poznámku, zdroj. A obráceně. Existují pohledy denní, týdenní a měsíční.

- úkol – objekt, který má název specifikaci, plnitele a termín plnění
- aktivita – činnost zaznamenaná mezi zákazníkem a námi
- kontakt – osoba nebo firma, která je uložena v xWORKu v modulu CRM
- poznámka – libovolná textová informace

- zdroj – je objekt v systému, u kterého se sleduje jeho čerpání, např. peníze, lidský zdroj, je využíván k vykonání aktivity, činnosti nebo úkolu
- činnost – je obecná událost, která je zaznamenána do diáře a má své trvání a termín
- projekt – je souhrn činností, úkolů a aktivit, které vedou k dosažení cíle projektu, tj. splnění do definovaného termínu za definované náklady a požadovanou kvalitou
- obchodní případ – je obchodní potenciál u zákazníka, kde je definováno co zákazník požaduje, v jakém je to předpokládaném obratu a kdy se to má realizovat

**Modul projekty/zakázky**

K zakázce se vedou informace o nákladech a výnosech. Zakázka představuje sadu aktivit, úkolů, činností a použitých zdrojů. Zakázky se mohou plánovat a později se srovnává skutečnost s plánem.

**Modul úkoly**

Slouží jako prostor pro snadné vykazování činností. Vytváří se na základě zobrazených úkolů, aktivit, poznámek, dokumentů.

**Modul docházka**

Slouží jako prostor pro snadné vykazování činností. Vytváří se na základě zobrazených úkolů, aktivit, poznámek, dokumentů.

**Modul CRM**

Slouží obchodní části firmy pro vytváření vztahů k zákazníkům, k subdodavatelům a vytváří kompletní obchodní agendu provázanou na ostatní moduly.

**Modul dokumenty**

V první fázi je nutno vybudovat pouze sklad dokumentů. Výchozí stav se bude řídit z funkčnosti stávající aplikace DOCLINE. Bude to existovat jako samostatný modul ve kterém se budou nastavovat pravidla pro práci s dokumenty.

**Modul nástěnka**

Nástroj pro podnikovou komunikaci, vyvěšování oběžníků, směrnic a pro sledování čtenářských aktivit včetně jejich logování.

**Modul notifikace**

Slouží k notifikaci pracovníků o tom, že se něco stalo, nebo nestalo. Informuje některé pracovníky (zadavatele, řešitele, nadřízeného) o stavu a událostech v úkolech, aktivitách a činnostech podle nastavení. Notifikace probíhá bud' mailem, na mobil nebo systémovým alertem. S výhodou lze uplatnit vazbu do WorkFlow.

**Modul zdroje**

Zdroje jsou interní a externí. Jsou to lidi, stroje a ostatní náklady. Vše je vyjádřeno v penězích, u každého zdroje je potřeba sledovat jeho vytíženost a celkové náklady za období , definovat kapacity zdroje

## 10.2 PrintSoft

PReS je softwarový nástroj pro návrh a publikování personalizovaných dokumentů. Umožňuje tvorbu a formátování dokumentů nebo zpráv a jejich následný tisk nebo elektronické publikování.

PReS je integrované vývojové prostředí navržené speciálně pro vývoj systémů tvorby a správy dokumentů.

Dokument může obsahovat variabilní text, obrázky, grafiku, čárové kódy a údaje pro třídění. Pomocí logických podmínek jsou vytvářeny dynamické dokumenty, kde se celé rozvržení dokumentu může různit podle údajů na vstupu. Tak lze namísto univerzálního dokumentu pro všechny vytvořit takový dynamický dokument, kdy každý jednotlivý příjemce obdrží exemplář přizpůsobený přesně jeho profilu. PReS pak může formátovat dokument pro tisk na libovolné tiskárně a pro elektronickou distribuci.

Tvorba všech typů dokumentů včetně:

- Dynamických výpisy z účtů
- Podnikových reportů
- Pojistných smluv přizpůsobených na míru
- Adresných marketingových dopisů

## 10.3 XANADU

XANADU nabízí podnikové systémy pro elektronickou správu dokumentů. kancelářských (office) i technických (CAD) v lokálních sítích i po internetu. Řešení pro správu CAD dokumentů a dat jsou postavena na technologiích Autodesk Data Management serveru.

- iPROJECT
- Autodesk Vault a Productstream
- DWF technologie
- CADVault
- AutoManager
- CAD manager
- Motiva

### 10.3.1 iPROJECT

iPROJECT je intranetový produkt určený všem kdo pracují s dokumenty a zároveň WWW služba určená projektantům, investorům, konstruktérům i všem členům kooperujících týmů. Umožňuje jednoduchou internetovou správu dokumentů, které nově vznikají a jsou průběžně aktualizovány v rámci daného projektu. Přístup z libovolného místa internetu usnadňuje spolupráci projekčních týmů nebo subdodavatelů nejen uvnitř firmy, ale i mezi vzdálenými lokalitami v republice či ve světě.

### 10.3.2 Autodesk Vault

Autodesk Vault je systém pro správu dat v pracovních skupinách integrovaný s Autodesk Inventorem, Inventorem Professional, AutoCADem Mechanical a dalšími strojírenskými produkty Autodesku. Umožňuje rychlé a přesné sdílení návrhových dat ve vašem konstrukčním týmu. Autodesk Vault představuje praktický přístup k PLM. Vault je plně integrován s produkty Inventor, AutoCAD Mechanical, AutoCAD Electrical, Civil 3D a AutoCAD.

### 10.3.3 DWF

Technologie Autodesku a otevřený formát DWF (Design Web Format) optimalizovaný pro

oblast CAD. Nabízí bezplatné nástroje pro publikování i prohlížení. Ve spolupráci s Microsoftem Autodesk vyvinul integrovanou technologii DWF a XPS (XML Paper Specification) - výsledné soubory. DWFx pak lze přímo zobrazovat ve Windows Vista a dalších OS s XPS prohlížeči.

### 10.3.4 CAD Vault

Aplikace CAD Vault for AutoCAD americké firmy CADLock Inc. je systém pro ochranu a řízení přístupu k obsahu DWG výkresů AutoCADu. Vychází z aplikace CADLock SE uvedené již v roce 1997.

CADVault umožňuje zabezpečit grafické i negrafické prvky výkresového souboru AutoCAD. Zvolené prvky vloží do elektronického objektu trezoru (vault). Ten zůstává součástí DWG souboru, ale přístup a způsob použití do tohoto trezoru je vázán na uživatelská oprávnění osoby používající daný DWG soubor. Do výkresu je také vložena nevymazatelná informace se jménem, kontaktními informacemi, apod.

Licenci CADVault potřebuje pouze autor výkresu, ostatní uživatelé mohou používat buď standardní AutoCAD nebo LT, nebo AutoCAD doplněný o bezplatný object enabler aplikace CADVault.

### 10.3.5 Automanager TeamWork

Popsaný již v nabídce Sova systems.

### 10.3.6 CaD Manager

CaD Manager je určený na správu dokumentů a technických dat. Má však širší záběr. Umožňuje spravovat v podniku data a dokumenty nejrůznějšího charakteru. Data jsou v CaD Manageru uspořádána do projektů. Projekty tvoří ucelené skupiny tematicky příbuzných dokumentů a dat, přičemž v projektu může být jeden nebo více výrobků podobného charakteru, stejně jako souhrn všech ostatních dokumentů nesouvisejících přímo s výrobkem nevázaných k položce. Datová struktura je plně přizpůsobitelná potřebám a představám uživatelů. Někdy může být projektem kusovník výrobku, jindy agenda celého oddělení. CaD Manager obsahuje i nástroje pro plánování práce a správu a plánování projektů. Součástí systému je rovněž interní pošta.

### 10.3.7 Motiva eChange

Řešení Motiva eChange umožňují firmám spravovat změny po celém dodavatelském řetězci a reagovat na ně rychlostí Internetu

## 10.4 AutoCont

### 10.4.1 ECM FileNET

Systém pro správu dokumentů postavený na platformě FileNet P8. Řešení pracují na dostupných platformách - MS Windows, HP Unix, Sun Solaris, IBM AIX, při využití architektury klient-server a moderních objektových technologií COM, ActiveX. Aplikačně je zajištěn přístup k funkcím prostřednictvím internetového prohlížeče.

Základem systému pro správu dokumentů je dokumentová knihovna. ECM FileNET používá dva typy dokumentové knihovny podle povahy dokumentů uchovávaných v knihovně. Architektura FileNet P8 poskytuje organizacím možnost rozšiřitelnosti a flexibilitu umožňující řešení komplexních úkolů týkajících se podnikového obsahu, obchodních procesů a konektivity. Využívá jednotné úložiště, jednotné uživatelské prostředí a jednotnou sadu aplikačního programovacího rozhraní (API) pro vývojáře.

ECM FileNET se skládá z následujících modulů:

- **Content manager -** poskytuje kontrolu, přístup a sdílení podnikového obsahu v bezpečném a vysoce škálovatelném prostředí
- **Business Process manager** - automatizuje, narovnává a optimalizuje firemní procesy prostřednictvím řízení pracovních toků mezi lidmi a podnikovými systémy
- **Forms manager -** správa a zpracování formulářů
- **Image manager** - poskytuje bezpečné a výkonné prostředí pro ukládání a řízení velkých objemů naskenovaných dokumentů, faxů, emailů, multimediálních souborů a dalšího obsahu
- **Records manager** - zpracování spisů v závislosti na definovaném procesu
- **Web Content manager -** slouží pro řízení tvorby, schvalování a publikaci webového obsahu a komplexních dokumentů

- **Team Collaboration manager**. Všechny uvedené produktové sady jsou vzájemně plně integrovány, umožňují zákazníkům zvolit si vyhovující řešení a následně podle potřeby přidávat další moduly a prvky.

Systém pro správu dokumentů FileNET splňuje všechny požadavky kladené na integrovanou správu dokumentů - vytváření dokumentů, nástroje pro jejich vyhledávání včetně full-textového, šablony pro vyhledávání, vytváření anotací, správa dokumentů, nástroje pro publikování dokumentů, správa verzí dokumentů, podpora různých formátů dokumentů, zajištění datové integrity a kompletní bezpečnosti na úrovni uživatele, skupiny, adresáře, dokumentu, verze, anotací a uložených kritérií pro vyhledávání. Součásti systému jsou nástroje, které umožňují práci se systémovými objekty a jejich vlastnostmi. Spojením dokumentové knihovny s těmito nástroji vzniká platforma pro správu obchodních procesů. Celý systém pro správu dokumentů ECM FileNET lze integrovat s dalšími systémy jako jsou např. ERP, CRM, DataWarehouse, B2B aplikace, portály aj.

## 10.5 Infos 2001

**Správa dokumentů**

- centrální ukládání dokumentů
- správa revizí dokumentů
- sledování stavů zpracování a schvalování dokumentů
- víceúrovňová kategorizace dokumentů podle funkčních a pracovních skupin
- třídění a vyhledávání dokumentů podle
  - názvu klíčových slov
  - vlastností
  - zakázky/projektu
  - organizačního zařazení
- historie zpracování dokumentů
- úzké propojení s ostatními podsystémy

## 10.6 PGP – Pretty Good Privacy

Šifrovací systém - produkt americké firmy PGP Corporation.

### 10.6.1 PGP Desktop produkty s WholeDisk

Šifrování komunikace a dat pro pracovní skupiny a jednotlivce - PGP Desktop Professional 9.x integruje PGP Mail pro zabezpečení zpráv, PGP Disk pro zajištění uložených dat a PGP Whole Disk pro zabezpečení celých disků včetně partition. Tím zajišťuje, že důvěrné informace společnosti jsou chráněny silným zabezpečením nezávisle na tom, kde jsou uloženy - při přenášení informací z počítačů odesílatelů do počítačů příjemců, při uložení na PC a ve všech bodech mezi nimi. Řešení je vhodné pro pracovní skupiny a osobní použití, které nevyžaduje centrální konfiguraci, správu či definování jednotných politik.

### 10.6.2 Nástroje PGP Desktop 9.x Professional

- PGP Mail
- PGP Virtual Disk
- PGP Whole Disk
- PGP ZIP
- PGP Shred

#### *10.6.2.1 PGP Mail*

Systém PGP desktop 9.x Professional pokročil významnou měrou v automatizaci šifrování. K dispozici již nejsou tzv. plug-iny, které se instalují přímo do poštovního klienta, ale práce s PGP probíhá na pozadí na základě předem definovaných nastavení ve zprávách. Například je -li zpráva označena jako důvěrná, je email automaticky zašifrován bez nutnosti ještě volit šifrování, obsahuje-li předmět zprávy kód PPP nebo jiný definovaný kód, je email opět automaticky šifrován.

#### *10.6.2.2 PGP Virtual Disk*

S použitím programu PGP Disk lze vytvořit zašifrovanou část disku, která je operačnímu systému prezentována jako další diskové zařízení. Na toto zařízení pak je možno běžným způsobem ukládat data. Při ztrátě kupříkladu notebooku s tímto systémem ukládání

důvěrných informací pak nehrozí jejich kompromitace.

#### *10.6.2.3 PGP Whole Disk*

PGP Whole Disk je součást PGP Desktop 9.x Professional. Tento nástroj slouží k zašifrování celého obsahu disku. Uplatňuje se zde proces nepřetržitého šifrování všech dat na pevných discích uživatelů, včetně šifrování dočasných souborů a výměnných souborů operačního systému. Šifrování celého obsahu disku může probíhat současně s objemovým šifrováním disku, případně může uživatel volit mezi oběma metodami. Dešifrování disku probíhá na základě zadání silného hesla, případně je podporována dvoufaktorová autentizace díky uložení privátních klíčů na USB eTokeny.

#### *10.6.2.4 PGP ZIP*

Možnost současného připojování nebo odstraňování několika souborů i celých adresářů v jediném komprimovaném a šifrovaném archivu PGP. Odpadá potřeba individuálního šifrování souborů, které jsou součástí vícenásobného výběru.

#### *10.6.2.5 PGP Shred*

Pokud chce mít uživatel jistotu, že data mají být nenávratně smazána, může použít nástroj PGP Shred. PGP Desktop Professional ho umožňuje po nastavení používat i automaticky.

### 10.6.3 Vlastnosti produktu PGP

**Důvěrnost** – pomocí kvalitního šifrování přenášených dat je dosaženo toho, že komunikace je srozumitelná pouze pro uživatele, jemuž je určena. Přitom lze zajistit, aby zprávu mohlo číst více adresátů zároveň.

**Integrita** – použitím vhodné hashovací funkce a následným podepsáním výsledného vzorku lze zajistit, že komunikující strany se mohou ujistit, že dokument nebyl neoprávněně změněn.

**Nepopiratelnost** – i zpětně lze prokázat, že daná osoba je skutečně autorem dokumentu, či jej četla nebo s ním jinak manipulovala.

**Autenticita a autentizace** – Na základě ověřených certifikátů veřejných klíčů lze s jistotou identifikovat (autentizovat) zdroj (odesílatele) dat.

### 10.6.4 PGP Desktop - Technické údaje

**PGP Desktop 9.x podporuje OS:**

Windows XP SP1, SP2, Windows server 2003, Windows 2000 SP3

Mac OS X (verze 10.3 a vyšší)

**PGP Mail podporuje poštovní a IM klienty:**

Microsoft Outlook 2003 SP1, Microsoft Outlook XP SP3, Microsoft Outlook 2000 SP3, Microsoft Outlook Express 6.x

Entourage 2004

Lotus Notes 6.x, Lotus Notes 5.0.11 for Windows

Mozilla Thunderbird 1.0, Qualcomm Eudora 6.2

Apple Mail 1.3.9, Apple iChat 2.1 for Mac OS X

AOL Instant Messenger 5.5-5.9 for Windows, AOL Instant Messenger 4.7 for Mac OS X

Trillian 2.2-3.0 for Windows

**PGP WholeDisk:**
Windows XP SP1, SP2

**Algoritmy symetrických klíčů:**
AES až s 256 bitovými klíči, CAST, TripleDES, IDEA, Twofish

**Hashes:**
SHA-1, MD5, RIPEMD-160

**Algoritmy veřejných klíčů:**
Diffie – Hellman, DSS, RSA až do 4096 bitů

**Formáty veřejných klíčů:**
OpenPGP RFC 2440, X.509 v.3, PGP MIME/RFC 3156, S/MIME v.3

### 10.6.5 PGP Universal – komplexní zabezpečení emailů a disků

PGP Universal Server nabízí centrální správu, nasazení, automatickou generaci a správu klíčů/certifikátů. Umožňuje nastavit politiky pro automatické šifrování, dešifrování a digitální podpisy stejně jako posílení vynucování této bezpečnostní politiky.

### 10.6.6 Výhody použití PGP Desktop Professional

Zabezpečení informačních zdrojů (mail, disk) pomáhá při dodržování interní politiky ochrany dat.

Definovaná pravidla šifrování na základě domén příjemců, nebo klíčových slov snižuje potřebu aktivního výběru způsobu šifrování ze strany uživatelů.

Kompatibilita formátů zpráv a certifikátů - Podpora a spolupráce se standardními prostředky OpenPGP, X.509 a S/MIME znamená zachování stávajících investic do zabezpečení.

Hromadná komprimace a kryptování - díky možnosti současného připojování nebo odstraňování několika souborů i celých adresářů v jediném komprimovaném a šifrovaném archivu PGP odpadá potřeba individuálního šifrování souborů, které jsou součástí vícenásobného výběru.

Podpora aplikace Microsoft Word jako editoru textů zpráv elektronické pošty poskytuje uživatelům možnost rozšířeného výběru textových formátů při psaní zpráv.

Podpora zašifrování celého disku „Whole disk“ před zavedením OS.

K zašifrovaným diskovým jednotkám může mít přístup více uživatelů, což umožňuje sdílení pracovních stanic několika zaměstnanci.

Kompatibilita s „volume based“ šifrováním disku omezuje přístup zaměstnanců ke konkrétním logickým diskům šifrovaných dat uloženým na zašifrovaném pevném disku.

Automatická deaktivace a trvalé blokování režimu spánku před a po instalaci chrání soubory před poškozením.

Integrace s prostředím PGP Universal 2.5 – Administrátoři mohou spravovat jak aplikaci PGP Universal tak aplikaci PGP Desktop ze stejné administrativní konzole.

### 10.6.7 Distribuce PGP

Distributorem PGP je společnost SkyNet, a.s. K dispozici je 30 denní doba na zkoušku, časově omezená licence na 1 rok + podpora na 1 rok stojí 3.249 Kč.

## 10.7 Zálohování dat

### 10.7.1 Magnetické pásky

Jiskra: „Význam pásek jako média pro ukládání dat je stále obrovský. Je třeba si uvědomit, že v současné době je asi 89 % všech digitálně uchovávaných dat uloženo právě na páskách. Magnetické pásky se díky technologickým omezením hodí především k uchovávání neměnného obsahu. Sekvenční způsob přístupu k médiu pro čtení i zápis předurčuje tuto technologii k vytváření archivů s nízkou frekvencí přístupu, ale také pro tvorbu datových záloh a obnovu dat. Výhodou těchto médií je především vysoká úroveň spolehlivosti a bezpečnosti uchovávaných dat, stejně tak jako nízká cena za GB informace

a vysoká kapacita. Další výhodou je pak snadná výměna a převoz médií včetně možnosti jejich úschovy v jiné lokalitě, což zvyšuje bezpečnost datových záloh pro případ disaster recovery.“[7]

### 10.7.2 LTO pásková technologie

LTO je průmyslový standard digitálních páskových pamětí. Je určeno především pro zálohování a archivaci velkého množství dat s velkou přenosovou rychlostí.

LTO je výsledkem spolupráce společností IBM, HP, Seagate a Tandberg.

Tabulka 4 Specifikace LTO

| | **LTO-1** | **LTO-2HH** | **LTO-2FH** | **LTO-3** |
|---|---|---|---|---|
| kapacita s kompresí | 200GB | 400GB | 400GB | 800GB |
| kapacita nativní | 100GB | 200GB | 200GB | 400GB |
| rychlost bez komprese | 15MB/s | 24MB/s | 35MB/s | 80MB/s |
| velikost cache | 32MB | 64MB | 64MB | 128MB |
| média | LTO-1 | LTO-2 | LTO-2 | LTO-3 |

# 11 NÁVRH ŘEŠENÍ

Po analýze současného stavu práce s dokumenty ve firmě AEV, stavu a stáří HW a SW Novell serveru, současných technologických možností řešení správy dokumentů a požadavků managementu firmy navrhuji pro firmu AEV toto řešení:

- Zakoupit nový server jako úložiště dokumentů
- Zakoupit zálohovací zařízení
- Zavést nový systém správy dokumentů **Automanager Meridian**
- Požádat o vydání certifikátu vybraným zaměstnancům pro elektronický podpis u kvalifikované certifikační autority.

## 11.1 Úložiště dokumentů

### 11.1.1 Požadavky na server

- ✓ Intel Pentium 4 frekvence 2 GHz nebo vyšší
- ✓ RAM 2 GB (minimum)
- ✓ Windows 2003 server, Windows 2000 server, Windows NT 4 (SP4, SP6a)

### 11.1.2 Návrh nového serveru

Nový server HP s operačním systémem Windows 2003 server.

Server HP řady ProLiant – konkrétní typ upřesnit v době nákupu podle aktuální nabídky.

- provedení: Tower, viz Obrázek 16
- procesor: Intel Xeon 3 GHz
- paměť RAM: 4 GB
- mechanika pevného disku: 500 GB

### 11.1.3 Operační systém a licence

**Microsoft Windows Server 2003 R2 Standard**

Wikipedie: „Windows Server 2003, Standard Edition je spolehlivý síťový operační systém

pro rychlé a snadné řešení podnikových úkolů. Tento flexibilní server je ideální volbou pro zajištění každodenních potřeb v organizacích všech velikostí. Windows Server 2003, Standard Edition nabízí řešení pro sdílení souborů a tiskáren, bezpečné připojení k Internetu, centralizované zavádění osobních aplikací a hodnotnou spolupráci mezi zaměstnanci, partnery a zákazníky. Windows Server 2003, Standard Edition podporuje symetrické zpracování dvěma procesory a až 4 GB paměti.“[16]

**Windows Server Device CAL**

Windows Server Device CAL je klientská přístupová licence k serverům Windows 2003. Tato přístupová licence pokrývá počítače - Device, které budou přistupovat k souborovým nebo tiskovým službám Windows Server 2003. Alternativou k Device CAL je User CAL, které slouží pro pokrytí přístupu uživatelů k serveru.

Obrázek 16 Server HP ProLiant v provedení Tower

### 11.1.4 Cena serveru

Orientační cena serveru včetně pevného disku, OS a licencí - cena bez DPH: **101.900 Kč**, viz Tabulka 5. Orientační ceny jsou označeny *.

Tabulka 5 Cena serveru

| | |
|---|---|
| Server HP ProLiant | *48.000 Kč |
| Mechanika pevného disku 500 GB | *15.000 Kč |
| Windows Server 2003 R2 Standard | 19.200 Kč |
| Windows Server Device CAL pro 25 počítačů | 19.050 Kč |
| Instalační médium | 650 Kč |
| CELKEM bez DPH | ***101.900 Kč** |

Není vybrán konkrétní typ serveru, ceny za hardware jsou vyhodnocené podle ceníku z webových stránek HP. Ceny za operační systém a licence byly nabídnuty prodejcem softwaru e-software.cz.

## 11.2 Zálohovací zařízení

### HP StorageWorks Ultrium 232i (AE304A)

Interní zálohovací mechanika formátu LTO Ultrium dodávána se zálohovacím softwarem a s 5 kusy medií. Možná doba archivace dat na médiích je uváděna 30 let. Technické parametry viz Tabulka 6

Cena bez DPH: **28.000 Kč**


Obrázek 17 Interní zálohovací mechanika HP

### Spotřební materiál

Datová kazeta HP Ultrium 200 GB stojí 1.100 Kč bez DPH.

Tabulka 6 Technické parametry HP StorageWorks Ultrium 232i

| | |
|---|---|
| Přenosová rychlost trvale | nativní 16 MB/s, komprimovaná 32MB/s |
| Přenosová rychlost (výkon) | 160 MB/s (Ultra3 SCSI) |
| Vyhledávací čas | 64 s pro 100 GB pásku (nativní) |
| Střední doba mezi poruchami | 250 000 hodin |
| Vyrovnávací paměť | 64 MB |
| Rozhraní SCSI | Wide Ultra3 SCSI (LVDS) |
| Kompatibilní operační systémy | MS Windows, Novell NetWare, HP-UX, Red Hat Linux, United Linux, IBM-AIX, Sun Solaris |
| Typ skříně | 5,25" half-height |
| Software pro správu | HP Library a Tape Tools |
| Komprimovaná kapacita media | 200 GB |
| Základní kapacita media | 100 GB |
| Typ jednotky | LTO-1 |
| Obnovení dat při nehodě | stisknutím jednoho tlačítka |
| Technologie zápisu | 8-channel linear serpentine |
| Rozměry | 145 x 206 x 41 mm |
| Hmotnost | 1,45 kg |

## 11.3 Automanager Meridian

Automanager Meridian nizozemské firmy CYCO Software B.V. u nás distribuuje a podporu poskytuje firma SOVA NET, s r. o.

Navrhuji kontaktovat obchodního konzultanta Sova Net, pozvat ho do firmy AEV, aby nezávazně prezentoval možnosti využití produktu.

### 11.3.1 Výhody Automanageru Meridian

- Komplexní systém DMS
- Rychlý přístup k dokumentům

- Dimenzovatelnost na různé úrovně řešení
- Trezorový koncept (bezpečnost dokumentů)
- Integrace do MS Windows, MS Office a CAD aplikací
- Možnost propojení s podnikovým IS
- Podpora norem třídy ISO 9000

### 11.3.2 Licencování Automanager Meridian

Licence Automanager Meridian jsou plovoucí. To znamená, že po zakoupení několika licencí je možné nainstalovat zakoupené klienty do všech počítačů ve firmě. Systém nainstalovaný na serveru hlídá, aby počet přihlášených klientů nepřekročil v každý okamžik počet zakoupených licencí. Jinak řečeno počet najednou přihlášených klientů k systému nesmí překročit počet zakoupených licencí pro daného klienta.

Ze čtyř nabízených klientů Power User, Office Client, Offline Client a Web Client navrhuji dva:

- **Power User** - klient s plnou integrací CAD systémů – **3 licence**
- **Office Client** - klient bez CAD integrace systémů – **12 licencí**

Ke každé licenci klienta je nutné zakoupit i licenci pro některou z nabídnutých databází:

- HyperTrieve
- MS SQL
- ORACLE

Sova Net doporučuje databázi HyperTrieve.

K cenám za licence je účtován poplatek za užívání tzv. subscription na 1 rok ve výši 20% z celkové ceny licencí.

### 11.3.3 Cena navržených licencí

V tabulce, viz Tabulka 7, jsou ceny za licence, které jsem navrhnul a roční subscription.

Tabulka 7 Ceny licencí Automanager Meridian

| ks | Produkt | Jednotková cena | Cena pro množství |
|---|---|---|---|
| 1 | Media Kit, CD, manuál | 1.670 Kč | 1.670 Kč |
| 3 | Automanager Meridian Power User Client | 24.310 Kč | 72.930 Kč |
| 12 | Automanager Meridian Office Client | 7.047 Kč | 84.564 Kč |
| 15 | *Databáze HyperTrieve | 21.763 Kč | 326.445 Kč |
| 0 | *Databáze MS SQL | 31.102 Kč | - |
| 0 | *Databáze ORACLE | 34.668 Kč | - |
| 1 | Subscription na 1 rok | 20% z ceny licencí | 96.788 Kč |
| **CELKEM bez DPH** | | | **582.397 Kč** |

* Výběr jedné z databází

### 11.3.4 Služby

Při zavádění systému je možné využít placených služeb firmy Sova Net, viz Tabulka 8.

Tabulka 8 Ceny za služby

| Činnost | Cena za hodinu bez DPH |
|---|---|
| Technická analýza stavu dokumentace | 950 Kč |
| Implementace systému + úpravy | 950 Kč |
| Školení administrátora, uživatelů | 500 Kč |

## 11.4 Celková cena investice

Tabulka 9 Celková cena investice

| | |
|---|---|
| Server + OS s licencemi | 101.900 Kč |
| Zálohovací zřízení | 28.000 Kč |
| Automanager Meridian licence, roční subscription | 582.397 Kč |
| **CELKEM bez DPH** | **712.297 Kč** |

## 11.5 Kvalifikovaný certifikát

Pro komunikaci s úřady státní správy je nutný kvalifikovaný certifikát, tedy certifikát získaný od kvalifikované certifikační autority.

### 11.5.1 Výběr kvalifikované certifikační autority

Jak jsem již zmínil v teoretické části, jsou u nás tři kvalifikované certifikační autority:

- Česká pošta: PostSignum QCA
- První certifikační autorita
- eIDENTITY

V tabulce, viz Tabulka 10, jsou ceny za kvalifikované certifikáty pro zaměstnance.

Tabulka 10 Ceny kvalifikovaných certifikátů

| Certifikační autorita | Doba platnosti certifikátu | Cena s DPH |
|---|---|---|
| Česká pošta | 1 rok | 190 Kč |
| První certifikační autorita | 1 rok | 752 Kč |
| eIDENTITY | 1 rok | 702 Kč |

Jako kvalifikovanou certifikační autoritu navrhuji **PostSignum QCA**, která je rozšířením obchodní aktivity České pošty, s.p. Pro účel, který firma potřebuje, je cena nejpříznivější a navíc kontaktní místo pro identifikaci uživatele je na každé větší poště.

### 11.5.2 Vygenerování klíčů a žádosti o certifikát

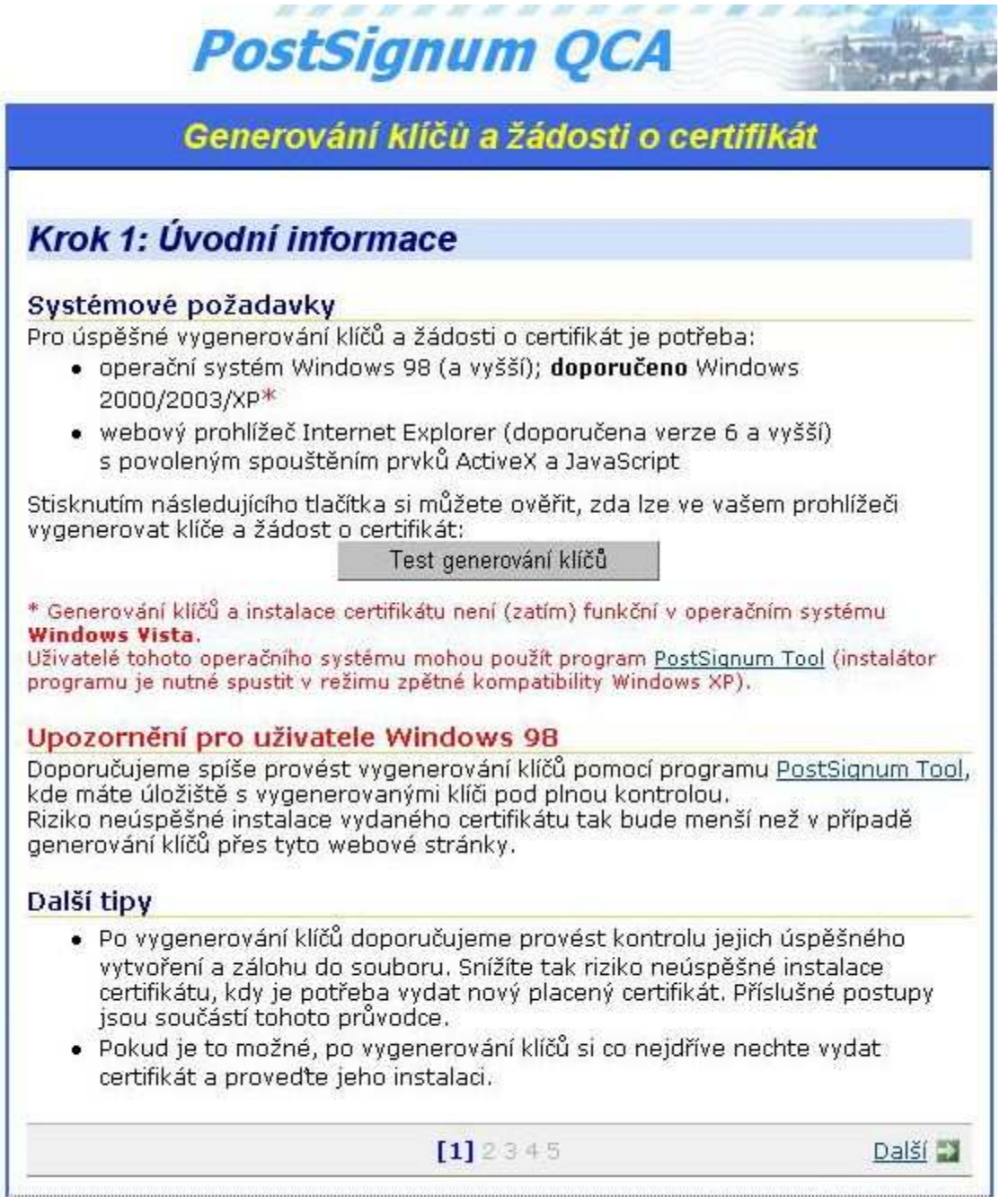
Před vydáním certifikátu je nutné vygenerovat klíče a žádost o certifikát. Na základě žádosti o certifikát bude pak vydán kvalifikovaný certifikát.

PostSignum QCA nabízí tyto možnosti vygenerování klíčů a žádosti o certifikát:

- on-line generování přes webové stránky
- off-line generování pomocí PostSignum Tool

Počítače žadatelů o vydání certifikátů jsou trvale připojeny k internetu, proto zvolíme metodu on-line generování pomocí webových stránek PostSignum www.postsignum.cz, viz Obrázek 18.

Vygenerované klíče se uloží do profilu aktuálně přihlášeného uživatele ve Windows a žádost o certifikát se uloží do souboru. Proto je nutné generování provádět na počítači žadatele a pod jeho přihlášením. V žádosti musí být uvedena emailová adresa, která bude k podpisu přiřazena. Soubor s vygenerovanou žádostí zkopírujeme žadateli na disketu.




Obrázek 18 Generování klíčů a žádosti na PostSignum on-line

### 11.5.3 Vydání certifikátu

Žadatel o certifikát přinese osobně na kontaktní místo České pošty vygenerovanou žádost

o certifikát na disketě a doklad totožnosti (občanský průkaz nebo pas).

Pracovník České pošty provede kontrolu totožnosti žadatele oproti předloženému dokladu. Osobní doklad žadatele je poté zkopírován. Tuto povinnost ukládá zákon o elektronickém podpisu - § 6 odst. 5 písm. c). Vytiskne se písemná žádost o certifikát. Žadatel si zvolí heslo pro zneplatnění certifikátu, které se doplní do žádosti, a podpisem odsouhlasí vydání certifikátu s údaji uvedenými na žádosti.

Dojde k vydání certifikátu. Certifikát se uloží na disketu k elektronické žádosti o certifikát, kterou si žadatel přinesl. Pracovník České pošty vytiskne protokol o vydání certifikátu a předá jej žadateli ke kontrole a k podpisu. Na disketu budou nakopírovány další soubory potřebné pro instalaci certifikátu.

### 11.5.4 Instalace vydaného certifikátu

Instalace certifikátu musí být provedena na tomtéž počítači a pod tímž uživatelským účtem, pod kterým bylo provedeno vygenerování klíčů a žádosti o certifikát. Proces instalace certifikátu závisí na způsobu vygenerování klíčů a žádosti o certifikát, podle které byl certifikát vystaven. Jelikož byly vygenerovány přes webové stránky PostSignum QCA, provedeme instalaci certifikátu z těchto web stránek pomocí průvodce instalací certifikátu. Viz Obrázek 19.


Obrázek 19 Průvodce instalací certifikátu

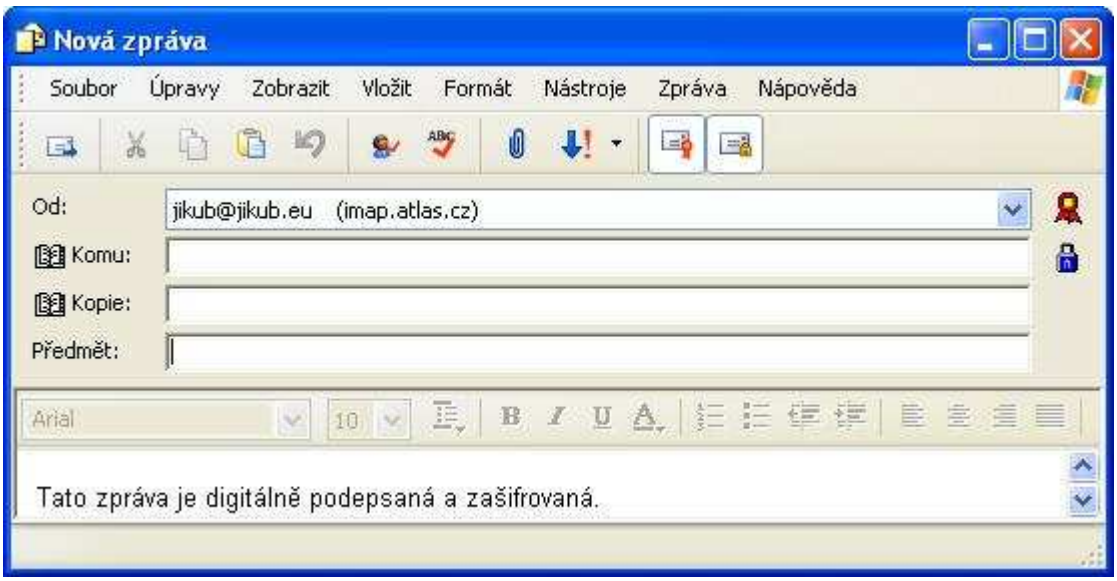
Instalaci certifikátu lze provést i bez webového průvodce. V možnostech internetu, kam se dostaneme např. přes ovládací panely, otevřeme záložku obsah. Po kliknutí na tlačítko

„Certifikát“, viz Obrázek 20, provedeme instalaci certifikátů z diskety.


Obrázek 20 Instalace certifikátu

### 11.5.5 Použití elektronického podpisu

Před odesláním zprávy pomocí emailového klienta je možné zprávu podepsat, zašifrovat nebo podepsat i zašifrovat, viz Obrázek 21.




Obrázek 21 Digitální podpis v Outlook Express

Zprávu odesílatel podepisuje svým soukromým klíčem, tzn. že podepsanou zprávu může odeslat komukoli. Příjemce si podpis ověří pomocí veřejného klíče odesílatele.

Zatímco zašifrovanou zprávu lze odeslat pouze tomu, kdo vlastní svůj klíčový pár. Zpráva se šifruje veřejným klíčem příjemce.

# 12 VYHODNOCENÍ

## 12.1 Návrh řešení

- Nový server HP řady ProLiant s operačním systémem Windows 2003 server
- Automanager Meridian od Cyco software
- Zálohovací zřízení HP StorageWorks Ultrium 232i (AE304A)

Předpokládaná investice cca 712.000 Kč bez DPH

Investice do správy dokumentů, tak jak jsem ji navrhl, se může zdát vysoká. Je ale třeba si uvědomit, jaká nebezpečí hrozí, pokud by se neudělala změna, jaký bude přínos pro bezpečnost a efektivitu práce s dokumenty. Také je třeba mít na vědomí, že toto řešení má dlouhodobý význam. Při rozhodování bude užitečná prezentace produktu Automanager Meridian zástupcem firmy Sova Net.

Zatím byl v AEV realizován pouze ten bod požadavku, který se týká kvalifikovaných certifikátů elektronického podpisu pro komunikaci s úřady státní správy.

## 12.2 Silná místa řešení

- ucelená správa dokumentů v jednom produktu
- zefektivnění práce s dokumenty
- bezpečnost dokumentů
- zálohování a archivace
- podpora norem třídy ISO 9000 a VDA 6.1
- integrace s IS

## 12.3 Slabá místa řešení

Slabá místa jsem nenašel.

# ZÁVĚR

V této práci jsem se zabýval problematikou elektronické správy dokumentů a jejím použitím v praxi. Kromě pohodlí a efektivity jsem se zaměřil zejména na datovou bezpečnost, kterou považuji při zacházení s dokumenty za velmi důležitou.

Cílem mé diplomové práce bylo navrhnout vhodné řešení správy elektronických dokumentů, jejich evidence a bezpečné manipulaci a archivace. Práce je určena pro firmu AEV, spol. s r.o., Kroměříž. Je to středně velká výrobní firma, jejímž předmětem činnosti je výroba elektronických přístrojů pro automobilní a letecký průmysl, osvětlovací a speciální techniku.

V teoretické části jsem se zabýval přínosem elektronické správy dokumentů a jejími úkoly. Hlavní důraz jsem kladl na bezpečnost dat, šifrování a elektronický podpis. K řešení úkolu v teoretické části, jsem využíval znalostí nabytých studiem na Fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně zejména v předmětech datová bezpečnost, počítačové sítě a provoz počítačových sítí. Dále studiem problematiky z uvedené literatury a z internetu. Teoretické části práce je možno využít pro seznámení s problematikou. Z teoretických poznatků jsem dále vycházel v praktické části diplomové práce.

V praktické části krátce představuji firmu AEV a charakteristiku její činnosti. Po té analyzuji současný stavu práce s dokumenty v AEV a uvádím svá doporučení. Dále je analýza možnosti řešení, návrh řešení a jeho vyhodnocení.

K vyhodnocení současného stavu a návrhu řešení pro firmu AEV jsem využil praktických znalostí problematiky a situace ve firmě z pozice správce počítačové sítě v AEV Kroměříž.

Při hledávání zdrojů řešící problematiku elektronické správy dokumentů a analýze současných technologických možností, licenčních a cenových nabídek jsem využíval vyhledávání v internetu a komunikace se zástupci firem nabízejících tato řešení.

Dospěl jsem k závěru, že v AEV je nutné změnit současný stav práce s dokumenty a zavést ucelenou správu dokumentů.

Svůj návrh předkládám managementu firmy AEV ke zvážení investice do správy firemních dokumentů.

# CONCLUSION

Text In this dissertation I was engaged in problems concerning electronic data management and its usage in practice. Besides a convenience and effectiveness I focused especially on data safety which I consider very important while managing data.

The aim of my thesis was to suggest a proper solution for an electronic data managing, its filing and safe manipulation and archiving. This work is intended for a company called AEV, spol. s r.o., Kromeriz. It's a medium-size firm which specializes in electronic gadgets manufacturing designed for automotive and air industry, illumination and special technology.

In the theoretical part I dealt with a contribution of electronic data management and its main tasks. The main emphasis was put on data safeness, encryption and electronic signature. For a problem solving in a theoretical part of this work I used my knowledge gained during my studies at the Faculty of applied informatics at Tomas Bata University in Zlin especially in subjects like data safety, PC networks and PC network operating. I also used knowledge acquired in the literature which I mention as the used literature in the end and the internet. The theoretical part of my dissertation is possible to use for familiarizing with the problems. These theoretical findings also served me as a base for the practical part of my work.

In the practical part the company called AEV is shortly introduced and its activity characterized. After that I analyze a current state of work with data in this firm and I bring in my recommendations. The other section contains a solving possibilities analysis, suggestion for solution and its interpretation.

For the interpretation of the current state and a suggestion for resolution for the company AEV I used practical knowledge of the problems and the situation in the company from a network administrator position in AEV Kromeriz.

During a search for sources which solve the problems with electronic data management and the analyse of current technical possibilities, licence and price offers I put in use internet searching and communication with representatives of companies offering these solutions.

I came to the conclusion that the current state of work with documents in AEV is needed to be changed and a comprehensive document administration should also be established. I

suggested the solution, too.

I am bringing my suggestion forward to the management of the AEV for an investment consideration into the company data management.

# SEZNAM POUŽITÉ LITERATURY

[1] AEV spol. s r.o. [online]. [cit. 2007-04-27]. Dostupné na WWW: http://www.aev.cz/html/onas.htm

[2] DOSEDĚL, T.: *Počítačová bezpečnost a ochrana dat*. 1. vyd. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1

[3] FRONĚK, M.: Elektronický oběh dokumentů. *IT Systems*, 2006, roč. 8, č. 12, s. 20-21.

[4] GARFINKEL, S.: *PGP: Pretty Good Privacy*. 1. vyd. Praha: Computer Press, 1998. 373 s. ISBN 80-7226-054-5

[5] HOBZA, J.: Dlouhodobé ukládání a archivace elektronických dokumentů. *IT Systems*, 2006, roč. 8, č. 3, s. 18-19.

[6] JAŠEK, R.: *Informační a datová bezpečnost*. 1. vyd. Zlín: UTB, 2006. 140 s. Fakulta managementu a ekonomiky. ISBN 80-7318-456-7

[7] JISKRA, J. *Moderní prostředky pro ukládání dat(část 2: Možné technologie (2))* [online]. Poslední změna: 7.12.2006. [cit. 2007-05-16]. Dostupné na WWW: http://www.computerworld.cz/cw.nsf/id/storage_moderni_prostredky_pro_ukladani_dat?OpenDocument&cast=2

[8] KLABALOVÁ, S. : *Projekt zvýšení konkurenceschopnosti firmy AEV s.r.o. využitím nástrojů marketingového mixu.* Zlín, 2006. 93 s. Diplomová práce na Fakultě managementu a ekonomiky Univerzity Tomáše Bati ve Zlíně na Ústavu managementu. Vedoucí diplomové práce Vratislav Kozák.

[9] KREJČÍ, R.: *Elektronický podpis v PDF* [online]. Poslední úpravy 19.6.2002. [cit. 2007-04-06] Dostupné na WWW: http://www.grafika.cz/art/pdf/pdfpodmis.html

[10] PostSignum [online]. Dostupné na WWW: http://www.postsignum.cz

[11] První certifikační autorita, a.s. [online]. Dostupné na WWW: http://www.ica.cz

[12] QCS Sdružení pro certifikaci systémů řízení jakosti [online]. Dostupné na WWW: http://www.cqs.cz

[13] SkyNet a.s. [online]. Dostupné na WWW: http://www.skynet.cz

[14] Sova systems Č.R. s.r.o. [online]. [cit. 2007-05-06]. Dostupné na WWW: http://www.sovasystems.cz/o-spolecnosti/

[15] Sova systems Č.R. s.r.o. [online]. Dostupné na WWW: http://www.sovasystems.cz

[16] Wikipedie, otevřená encyklopedie [online]. [cit. 2007-05-06]. Dostupné na WWW: http://cs.wikipedia.org/wiki/Windows_Server_2003#Windows_Server_2003.2C_Standard_Edition

[17] Wikipedie, otevřená encyklopedie [online]. Dostupné na WWW: http://cs.wikipedia.org

[18] ZDYCH, L. *Workflow* [online]. Poslední změna: 11.1.2007. [cit. 2007-04-04]. Dostupné na WWW: http://cms4u.cz/resources/rejstrik-pojmu/workflow

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| 3D | Trojdimenzionální - trojrozměrný |
| AEV | Společnost AEV spol. s r.o. - zkratka pro automobilní elektronika výroba |
| AFPDS | Advanced Function Printing Data Stream – pokročilé funkce PDS |
| AMD | Advanced Micro Device – výrobce procesorů |
| CA | certifikační autorita |
| CAD | Computer Aided Design – počítačem podporované navrhování |
| CAL | Client Access Licence – klientská přístupová licence u produktů Microsoft Windows Server |
| CD | Compact Disc – kompaktní disk |
| CDL | Podnikatelská skupina se zaměřením na CAD - DTP - LAN |
| CD-R | Compact Disc Recordable – kompaktní disk zapisovatelný |
| CD-ROM | CD – Read Only Memory – kompaktní disk pouze ke čtení |
| CRM | Customer Relationship Management - systémy podporující řízení vztahů se zákazníky. |
| DH klíč | Diffie-Hellman - šifrovací algoritmus |
| DHCP | Dynamic Host Configuration Protocol – konfigurace TCP/IP klientům |
| Diffie-Hellman | kryptografická metoda výměnou klíčů |
| DMS | Document Management System – systém správy dokumentů |
| DNS | Domain Name System – systém doménových jmen |
| DSS | Digital Signature Standard - asymetrická šifra |
| DTP | Desktop Publishing - tvorba tištěného dokumentu za pomoci počítače neboli elektronická sazba |
| DVD | Digital Versatile Disc – digitální víceúčelový disk |
| DVD-R | Digital Versatile Disc Recordable – digitální víceúčelový disk zapisovatelný |
| DVD-ROM | DVD – Read Only Memory – digitální víceúčelový disk pouze ke čtení |
| DWF | Design Web Format – needitovatelný bezpečný souborový formát |
| DWG | DraWinG - nativní formát výkresů programu AutoCAD |
| ECM | Enterprise Content Management - správa firemního obsahu, neboli správa veškerých informací a dokumentů a na ně navázaných procesů |
| ERP | Enterprise ressource planning - podnikový informační systém |
| HP | Hewlett Packard – výrobce výpočetní a kancelářské techniky |
| IBM | International Business Machines Corporation – přední světová společnost v oboru informačních technologií |

| | |
|---|---|
| IM | Instant Messaging – snadná online komunikace prostřednictvím počítačové sítě resp. internetu |
| IMAP | Internet Message Access Protocol – protokol pro práci s emailovou schránkou |
| IP | Internet Protocol – komunikační síťový protokol |
| IPDS | Intelligent Printer Data Stream - protokol pro přenos dat mezi hostitelským počítačem a tiskárnou |
| IPX | Internet Packet Exchange – komunikační síťový protokol |
| IPX/SPX | síťový protokol systému Novell NetWare |
| ISO | International Standardization Organizatoin – Mezinárodní organizace pro normalizaci |
| LAN | Local Area Network – místní počítačová síť |
| LTO | Linear Tape-Open – technologie ukládání digitálních dat na magnetické pásky |
| LVDS | Low Voltage Differential Signaling – metoda nízkonapěťového signálu |
| MD5 | Message-Digest algorithm 5 - šifrovací algoritmus |
| NOD32 | Antivirový systém firmy ESET |
| ODMA | Open Document Management Architecture - Aplikační programové rozhraní pro správu otevřených dokumentů |
| OS | operační systém počítače |
| PC | Personal Computer – osobní počítač |
| PCL | Printer Command Language - jazyk tiskových příkazů tiskáren HP |
| PDF | Portable Dokument Format - formát dokumentů firmy Adobe |
| PDS | Printing Data Stream – tok tiskových dat |
| PGP | Pretty Good Privacy – Báječné soukromí – systém šifrování a bezpečné elektronické komunikace |
| PIN | Personal Identification Number - osobní identifikační číslo |
| PLM | Product Lifecycle Management - komplexní popis správy životního cyklu výrobku v produkční sféře |
| POP3 | Post Office Protocol verze 3 – protokol pro stahování emailových zpráv |
| QCA | Kvalifikovaná certifikační autorita |
| RSA | Rivest, Shamir, Adlemann - kryptografický systém |
| SCSI | Small Computer System Interface – standardní rozhraní mezi počítačovými zařízeními a počítačovou sběrnicí |
| SHA-1 | Secure Hash Algoritm - šifrovací algoritmus |
| SMTP | Simple Mail Transfer Protocol – protokol pro přenos emailů mezi stanicemi |

| | |
|---|---|
| SPX | Sequenced Packet Exchange – síťový protokol na transportní vrstvě |
| SQL | Structured Query Language – strukturovaný dotazovací jazyk |
| STP | Shielded Twisted Pair – stíněná kroucená dvoulinka |
| TCP | Transmission Control Protocol – síťový protokol na transportní vrstvě |
| TCP/IP | sada protokolů pro komunikaci v počítačové síti zejména v internetu |
| UPS | Uninterruptible Power Supply – nepřerušitelný zdroj energie |
| USB | Universal Series Bus - univerzální sériová sběrnice |
| UTP | Unshielded Twisted Pair – nestíněná kroucená dvoulinka |
| UV | Ultraviolet – ultrafialové záření |
| VDA | Verband der Automobilindustrie – německý systém managementu kvality pro automobilový průmysl |
| WWW | World Wide Web – celosvětová „pavučina“ – síť hypertextových dokumentů |
| XML | eXtensible Markup Language – rozšiřitelný značkovací jazyk |
| XPS | XML Paper Specification - otevřený formát Microsoftu určený k archivaci, ukládání a univerzální tisk dokumentů |
| ZIP | souborový formát pro kompresi a archivaci dat |

# SEZNAM OBRÁZKŮ

Obrázek 1 Symetrické šifrování ..... 26
Obrázek 2 Nárůst počtu symetrických klíčů ..... 27
Obrázek 3 Asymetrické šifrování ..... 29
Obrázek 4 Přenos adresované, zašifrované a podepsané zprávy ..... 33
Obrázek 5 Bezpečná komunikace s využitím digitálního podpisu ..... 34
Obrázek 6 Areál AEV spol. s r.o., Kroměříž ..... 47
Obrázek 7 Managementovatelný switch HP ..... 48
Obrázek 8 Záložní zdroje UPS v serverovně ..... 49
Obrázek 9 Server HP NetServer E 55 Gold ..... 51
Obrázek 10 Novell – svazky, kontejnery, skupiny ..... 52
Obrázek 11 Novell – nastavení práv skupinám ..... 53
Obrázek 12 Novell – nastavení práv jednotlivcům ..... 54
Obrázek 13 Novell klient pro prostředí Windows ..... 55
Obrázek 14 Novell – Login Script ..... 56
Obrázek 15 SquirrelMail webové rozhraní mailové schránky ..... 58
Obrázek 16 Server HP ProLiant v provedení Tower ..... 77
Obrázek 17 Interní zálohovací mechanika HP ..... 78
Obrázek 18 Generování klíčů a žádosti na PostSignum on-line ..... 83
Obrázek 19 Průvodce instalací certifikátu ..... 84
Obrázek 20 Instalace certifikátu ..... 85
Obrázek 21 Digitální podpis v Outlook Express ..... 85

# SEZNAM TABULEK

Tabulka 1 Odlišnosti dig. a analog. dokumentu ..... 13
Tabulka 2 Počet zaměstnanců AEV ..... 47
Tabulka 3 Rozmezí IP adres a jejich nastavení ..... 50
Tabulka 4 Specifikace LTO ..... 75
Tabulka 5 Cena serveru ..... 78
Tabulka 6 Technické parametry HP StorageWorks Ultrium 232i ..... 79
Tabulka 7 Ceny licencí Automanager Meridian ..... 81
Tabulka 8 Ceny za služby ..... 81
Tabulka 9 Celková cena investice ..... 81
Tabulka 10 Ceny kvalifikovaných certifikátů ..... 82

# SEZNAM PŘÍLOH

P I: Certifikát ISO 9001: 2000

P II: Certifikát VDA 6.1

P III: Osvědčení k výrobě vojenské letecké techniky

P IV: Oprávnění k projektování letadlových zařízení

P V: HP StorageWorks Ultrium 232 Tape Drive

P VI: Představení sdružení SOVA

P VII: Automanager Meridian

P VIII: CD s prací v elektronické podobě

# PŘÍLOHA P I: CERTIFIKÁT ISO 9001: 2000

TÜV CERT

# ZERTIFIKAT

**Die TÜV CERT-Zertifizierungsstelle**
**der TÜV SÜD Management Service GmbH**

bescheinigt gemäß
TÜV CERT-Verfahren, dass das Unternehmen

**AEV spol. s r.o.**
**Jožky Silného 2783**
**CZ - 767 01 Kroměříž**

für den Geltungsbereich

**Entwicklung, Konstruktion, Produktion**
**und Vertrieb von elektronischen Geräten**

ein Qualitätsmanagementsystem
eingeführt hat und anwendet.

Durch ein Audit, Bericht-Nr. **70010091**

wurde der Nachweis erbracht, dass die Forderungen der

**ISO 9001: 2000**

erfüllt sind. Dieses Zertifikat ist gültig bis **2010-02-01**

Zertifikat-Registrier-Nr. **12 100 12095**

Deutscher Akkreditierungs Rat
DAR
TGA-ZM-18-96

München, 2007-02-02

TÜV SÜD
Management Service

TÜV CERT-Zertifizierungsstelle
der TÜV SÜD Management Service GmbH
Ridlerstraße 65
D-80339 München

Cert04.02.99

# PŘÍLOHA P II: CERTIFIKÁT VDA 6.1

VDA QMC TÜV CERT

TÜV SÜD Management Service

## ZERTIFIKATSERGÄNZUNG

**Die TÜV CERT-Zertifizierungsstelle der**
**TÜV SÜD Management Service GmbH**
**VERBAND DER AUTOMOBILINDUSTRIE E.V. (VDA) / Z. Nr. 10/97**

bescheinigt hiermit entsprechend dem
TÜV CERT-Regelwerk, dass das Unternehmen

**AEV spol. s r.o.**
**Jožky Silného 2783**
**CZ - 767 01 Kroměříž**

Standort: CZ-767 01 Kroměříž

für den Geltungsbereich:
Entwicklung, Konstruktion, Produktion und Vertrieb
von elektronischen Geräten für die Automobilindustrie

**ein Qualitätsmanagementsystem nach VDA 6.1: 2003**
**- Materielle Produkte -**
**(mit Produktentwicklung)**

anwendet.

Diese Zertifikatsergänzung ist nur gültig in Verbindung mit dem ISO 9001-Zertifikat, Registrier-Nr.: 12 100 12095. Sie bestätigt, dass das QM-System durch Erfüllung der in VDA 6.1: 2003, gegenüber ISO 9001: 2000 erweiterten Forderungen zusätzlich qualifiziert ist. Der Nachweis wurde im Rahmen des Zertifizierungsaudits, Bericht Nr. 70010091, erbracht.

Diese Zertifikatsergänzung ist gültig bis **2010-02-01**

TMS-Registrier-Nr.: **12 107 12095**

Ausstellungsdatum: 2007-02-02

KBA-ZM-A22001-95

M. Vogel

TÜV CERT-Zertifizierungsstelle
der TÜV SÜD Management Service GmbH
Ridlerstraße 65
D-80339 München

# PŘÍLOHA P III: OSVĚDČENÍ K VÝROBĚ VOJENSKÉ LETECKÉ TECHNIKY

**MINISTERSTVO OBRANY**
**MINISTRY OF DEFENCE**

**ČESKÁ REPUBLIKA** — **CZECH REPUBLIC**

## OSVĚDČENÍ
## APPROVAL CERTIFICATE

**Č. / No: MAA 018**

Tímto dokumentem se na základě splnění požadavků vojenských leteckých předpisů Armády České republiky a příslušných postupů OVL MO platných v České republice
This document on the basis of compliance with requirements of the Czech Army Military Aviation Regulations and with the pertinent MAD Procedures valid in the Czech Republic

| | |
|---|---|
| Opravňuje<br>Approves | **AEV spol. s r.o.** |
| Se sídlem<br>Whose business address is | **Jožky Silného 2783, 767 01 Kroměříž** |
| Pracoviště<br>Workplace | **Jožky Silného 2783, 767 01 Kroměříž** |
| Jako organizace schválená<br>Approved organization | **k výrobě výrobků vojenské letecké techniky** |

Podmínky – Conditions:

1. Osvědčení je omezeno na rozsah činností a typy nebo druhy výrobků uvedených v části 5. tohoto osvědčení.
   This Approval Certificate is limited to the scope of the activities and to the types and/or to the sorts of articles listed in the Annex of the Approval Certifcate.
2. Držitel Osvědčení provádí činnost za podmínek a v souladu s dokumenty, které schválil OVL MO při vydání Osvědčení.
   The Approval Certificate holder shall perform these activities according to conditions and documents approved by the MAA when issueing this Approval Certificate.
3. Držitel osvědčení je povinen dodržovat předpisy vydané Ministerstvem obrany ČR.
   Approval Certificate holder shall comply with the regulations issued by Ministry of Defence of the Czech Republic.
4. Osvědčení je platné dokud se jej jmenovaný nevzdá, dokud není OVL MO jeho platnost pozastavena, odvolána nebo ukončena, dokud neuplyne doba jeho platnosti stanovena OVL MO, nebo pokud se změní místo nebo obor činnosti pro něž bylo Osvědčení vydáno. Toto Osvědčení je nepřenosné.
   The Approval Certificate is valid until surrendered, suspended, revoked or termination date otherwise establishedby the MAA until the end of a MAA specified duration or until the location or the branch of the activity, for which the Approval Certificate was issued, is changed. This document is not transferable.

**2006-09-04**
Datum vydání - Date of issue
(rr-mm-dd) - (yy-mm-dd)

MINISTERSTVO OBRANY
219

Podpis - Signature

Státní tiskárna cenin, s.p.

# PŘÍLOHA P IV: OPRÁVNĚNÍ K PROJEKTOVÁNÍ LETADLOVÝCH ZAŘÍZENÍ

ÚŘAD PRO CIVILNÍ LETECTVÍ
CIVIL AVIATION AUTHORITY

ČESKÁ REPUBLIKA — CZECH REPUBLIC

# OPRÁVNĚNÍ
## APPROVAL CERTIFICATE

Č. / No: **L-NP 033**

Tímto dokumentem se na základě splnění požadavků civilních leteckých předpisů České republiky a příslušných „Postupů ÚCL" platných v České republice

This document on the basis of compliance with requirements of the Czech Republic Civil Aviation Regulations and with the pertinent CAA Procedures valid in the Czech Republic

| | |
|---|---|
| Opravňuje<br>Approves | **AEV, spol. s r.o.** |
| se sídlem<br>whose business address is | **Jožky Silného 2783, 767 01 Kroměříž** |
| Pracoviště<br>Workplace | **Jožky Silného 2783, 767 01 Kroměříž** |

**v souladu s Postupy CAA - TI - 026 - n/ 01 k projektování letadlových zařízení a jejich změn**

**in accordance with the National Procedures CAA - TI- 026 - n/01 to design appliances or their changes**

Podmínky - Conditions:

1. Oprávnění je omezeno na rozsah činností a typy a/nebo druhy výrobků uvedených v příloze tohoto Oprávnění.
   This Approval Certificate is limited to the scope of the activities and to the types and/or to the sorts of articles listed in the Annex of this Approval Certificate.
2. Držitel Oprávnění provádí činnosti za podmínek a v souladu s dokumenty, které schválil ÚCL při vydání Oprávnění.
   The Approval Certificate holder shall perform these activities according to conditions and documents approved by the CAA at issueing this Approval Certificate.
3. Držitel Oprávnění je povinen dodržovat předpisy vydané Ministerstvem dopravy a spojů ČR.
   Approval Certificate Holder shall comply with the regulations issued by Ministry of Transport and Communication of the Czech Republic.
4. Oprávnění je platné dokud se jej jmenovaný nevzdá, dokud není ÚCL jeho platnost pozastavena, odvolána nebo ukončena dokud neuplyne doba jeho platnosti stanovená ÚCL, nebo dokud se nezmění místo nebo obor činnosti, pro něž bylo Oprávnění vydáno. Toto oprávnění je nepřenosné.
   The Approval Certificate is valid until surrendered, suspended, revoked or termination date otherwise established by the CAA, until the end of a CAA specified duration or until the location or the branch of the activity, for which the Approval Certificate was issued, is changed. This document is not transferable.

**12.9.2005**

Datum vydání – Date of issue

ÚŘAD PRO CIVILNÍ LETECTVÍ ČESKÁ REPUBLIKA -1-

Podpis – Signature

# PŘÍLOHA P V: HP STORAGEWORKS ULTRIUM 232 TAPE DRIVE



## HP StorageWorks Ultrium 232 Tape Drive (AE304A) - Specifikace

» Return to original page

**Chcete koupit tento produkt?**

» Technická podpora
» Dokumentace k produktu

Cena
**26458 Kč**
bez DPH

**Zákaz. centrum: 261 108 108**

**Vyberte si dodavatele zboží HP dle názvu, specializace či produktu.**

Výběr HP partnera »

**Specifikace** » Doplňky a příslušenství

**Technická specifikace**

| | |
|---|---|
| Obsah krabice | HP StorageWorks Ultrium 232 Internal Tape Drive; HP StorageWorks Tape CD-ROM (contains HP StorageWorks Library and Tape Tools utilities and localised user manuals); HP OpenView Storage Data Protector for Windows (SSE) license-to-use (installation via download); 5 x HP Ultrium Data Cartridge (200 GB); internal SCSI cable; documentation |
| Rozsah provozní teploty | 10°to 35°C |
| Rozsah provozní vlhkosti | 20 to 80% RH |
| Vlhkost, mimo provoz | 10 to 95% RH |
| Rozměry (šířka x hloubka x výška) | 14.5 x 20.6 x 4.1 cm |
| Rozměry balení (š x h x v) | 45.0 x 31.0 x 29.0 cm |
| Hmotnost | 1.45 kg |
| Hmotnost balení | 3.6 kg |
| Typ skříně | 5¼ inch half-height |
| Střední doba mezi selháním | 250,000 hours at 100% duty cycle |
| Komprimovaná kapacita | 200 GB per cartridge with 2:1 compression |
| Původní kapacita | 100 GB |
| Vyhledávací čas | 64 seconds typical for a 100 GB tape (native) |
| Vyrovnávací paměť | 64 MB |
| Dlouhodobá přenosová rychlost | 16 MB/s native; 32 MB/s with 2:1 compression |
| Přenosová rychlost (výkon) | 160 MB/s (with Ultra3 SCSI wide) |
| Typ jednotky | LTO-1 |
| Vstupní/Výstupní konektory modulu | 68-pin LVDS |
| Možnosti upgradu | HP StorageWorks Library and Tape Tools (L&TT) enables firmware downloads |
| Podpora výměny za provozu (Hot-Plug support) | No |

| | |
|---|---|
| Obnovení dat v případě nehody stisknutím jediného tlačítka | Yes |
| Technologie zápisu | 8-channel linear serpentine |
| Rozhraní SCSI | Wide Ultra3 SCSI (LVDS) |
| Četnost výskytu nezjištěných chyb | 1 × 10(17) bits read |
| Software pro správu | HP Library and Tape Tools |
| Kompatibilní operační systémy | Microsoft® Windows®, Novell NetWare, HP-UX, Red Hat Linux, United Linux, IBM-AIX, Sun Solaris and other operating systems |
| Prohlášení o standardní záruce | Hewlett-Packard provides a 3-year, next-day, product exchange, limited warranty for all the StorageWorks Ultrium Tape Drives, plus 9x5 phone support for the duration of the warranty |

» Return to original page

# PŘÍLOHA P VI: PŘEDSTAVENÍ SDRUŽENÍ SOVA

## Představení sdružení společností pod značkou SOVA®

Registrovaná značka SOVA® sdružuje dvě firmy a jednu divizi se společným cílem dosáhnout kvalitních služeb v oblasti implementace a integrace informačních technologií a školení. Zkušenosti sdružení datují deset let práce v oboru a stálé udržování pozice odborného řešitele s certifikací Autodesk Authorised Reseller, CYCO dealer, IBM dealer, HP, COMPAQ reseller. V oblasti školení udržuje těsnou spolupráci se státní správou.

Sdružení společností nabízí svým partnerům zajištění komplexních služeb z portfolia činností následujících subjektů:

SovA SYSTEMS je nejdéle působící firmou sdružení, stavící na systémově inženýrském přístupu, schopnosti analýzy a řešení požadavků klienta v oblasti informačních technologií. Díky autorizaci společnosti Autodesk je firma schopna implementace a optimalizace systémů CAD v návaznosti na správu dokumentace DMS/PDM systémy a jiné podnikové informační systémy. Servis u zákazníka je komplexní i ve výběru a pravidelné údržbě hardware pracovních stanic a technologií pro zálohu dat. Řešení firemních sítí je prováděno v součinnosti s divizí firmy SOVA NET.

SovA NET je dceřiná společnost firmy SOVA® SYSTEMS, která po svém vzniku kompletně převzala její aktivity v oblasti Internetu, intranetu a eBusiness. Mezi hlavní činnosti divize patří poskytování služeb spojených s vytvářením a provozováním internetových aplikací, určených pro publikování a obchodování v prostředí Internetu a programátorské aktivity na zakázku, zaměřené na práci s databázemi. Nosnou aktivitou společnosti je vývoj a prodej informačního systému xWORK, obsahující mimo jiné moduly CRM, Project a Time management.

SovA STUDIO je divizí zaměřenou na vzdělání a zvyšování pracovních dovedností. Pravidelně připravuje široce orientovanou nabídku školení v oblastech: organizační management, sekretářky, marketing, obchodní dovednosti, obchodní právo, zahraniční obchod, zásobování, skladování, obaly, výroba, nemovitosti, personalistika, pracovní právo, mzdy, ekonomika, finanční účetnictví, daně, kurzy práce na PC, a to formou otevřených nebo zakázkových kurzů, seminářů, přednášek, aktivních tréninků a workshopů. Divize úzce spolupracuje ve školících a konzultačních službách s ostatními subjekty sdružení SOVA® .

**Vybrané reference:**

Dopravoprojekt Brno, a.s.
Unistav a.s.
UNIS, spol. s r.o.
ZS Brno, a.s.
B-projekting, s.r.o.
První brněnská strojírna Brno DIZ, a.s.
CETOS, a.s.
Dynasig, spol s r.o.
S.O.K. stavební, s.r.o.
Jihomoravská plynárenská a.s.
Česká pošta, s.p., JM
Magistrát města Brna
Moravské naftové doly, a.s. Hodonín
Hartmann Rico, a.s
PBS Turbo, s.r.o.
Siemens Automobilové systémy s.r.o., Frenštát p. R.
Siemens VDO Automotive s.r.o., Horní Adršpach

autodesk authorized dealer architecture and building design

cyco software

IBM Business Partner

hp invent

TANDBERG DATA Securing your information

## SOVA® - pro Vaši práci

Adresa: Křenová 52, 602 00 Brno

www.sovasystems.cz
Tel/fax: 543 256 250

www.sovanet.cz
Tel/fax: 543 256 251

www.sovastudio.cz
Tel/fax: 543 254 037

# PŘÍLOHA P VII: AUTOMANAGER MERIDIAN

SovA NET — The core of your business


## AutoManager® Meridian

**Jednoduchost, dostupnost, kompletnost – s AutoManager® Meridian bude vaše pracovní skupina výkonnější a silnější**

**Správa dokumentace nebyla nikdy tak snadná. Cyco software Vám představuje nový AutoManager Meridian – jednoduchý, dostupný a kompletní inženýrský systém pro správu dokumentace. S AMM budete schopni neuvěřitelně rychle ovládat, sdílet, tisknout a prohlížet všechny vaše dokumenty. Buďte rychlí a vždy v předstihu! Předefinované šablony a průvodci Vám pomohou software lehce nakonfigurovat dle Vašich potřeb.**


**Jako jeden z čelních představitelů správy dokumentace firma Cyco připustila, že dnešní manažer je konfrontován velkou časovou náročností obsahující: provádění schvalovacích, komplexní kontrolu dat, on-line spolupráci, redukci životního cyklu atd.**

**Nový AMM poskytuje jednoduchou, spolehlivou a úplnou správu dokumentace, protože má vlastnosti, které nejvíce potřebujete. Pomocí následujících nástrojů posílíte vaši pracovní skupinu :**

- **rychlý přístup k dokumentům**
- **opravy a kontroly**
- **tisk a náhledy pro rychlé reference**
- **integrace s kancelářskými aplikacemi pro snazší spolupráci**

**Jako další generace AutoManager WorkFlow, rozšířeného systému pro správu dokumentace, AMM přejímá víc než 10 let zkušeností s podporou pracovních skupin a jejich každodenních úkolů.**


| Název společnosti: | Sídlo: | TEL, FAX: | IČ, DIČ: | E-mail, web: | Bankovní spojení: |
|---|---|---|---|---|---|
| SOVA NET, s. r. o. | Křenová 52 | +420 543 255 536 | 26281813 | info@sovanet.cz | HVB Bank |
| | 602 00 Brno | +420 543 255 853 | CZ26281813 | www.sovanet.cz | č. ú: 303034005/2700 |
| Spisová značka: | C.41708 vedená u Krajského soudu v Brně | | | | |

**Staví na prokázaných schopnostech AutoManager WorkFlow s pokročilou technologií Cyco softwaru vycházejícího z AutoManager Meridian. AutoManager Meridian zlepšuje práci Vašeho týmu s ohledem na vzrůstající produktivitu, rychlost a úspěch všech projektů dnes i v budoucnu.**

## Charakteristika AutoManager Meridian

| AutoManager Meridian | |
|---|---|
| Hlavní charakteristika | snadný a bezpečný přístup k firemní dokumentaci z inter. i exter. prostředí |
| Cílová skupina | Středně velké a velké společnosti |
| Uživatelé | správci objektů, vedoucí projektů a zakázek, manažeři i řadoví zaměstnanci |
| Organizační struktura | Divize s týmy pracovníků |
| Počet uživatelů | 30 – 100 a více |
| Druhy databází | HyperTrieve, SQL, Oracle |
| Uživatelské úpravy | - přizpůsobení<br>- příklady aplikací<br>- plně přizpůsobitelné pomocí Visual Basic |
| Hlavní rysy | - rychlý přístup k dokumentům<br>- prohlížení, editace a rychlý tisk<br>- řízení revizí, workflow<br>- rychlé vyhledávací nástroje |
| Hlavní výhody | - zlepšení koordinace firemních procesů<br>- optimalizace toku dokumentů z různých oddělení<br>- zajištění bezpečnosti dokumentů- z hlediska archivace i přístupu<br>- podrobné nastavení rolí a práv pro jednotlivé uživatele<br>- integrace se společným informačním systémem |

## Technické požadavky

**AutoManager Meridian je klasická aplikace klient - server se všemi výhodami této architektury. Aplikační a souborový server systému je možno provozovat na platformě WindowsNT/2000/2003 pro procesor Intel. Databázový server může běžet na kterémkoliv operačním systému pro který je určen.**

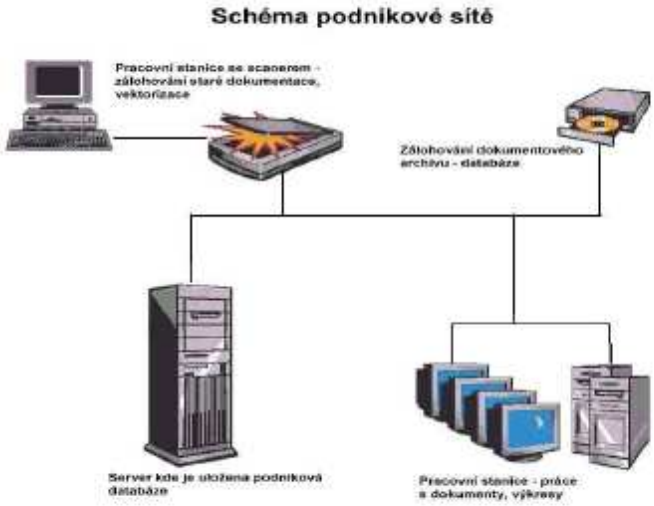
| Požadavky na server | Požadavky na klienta |
|---|---|
| Intel Pentium IV 2 GHz nebo vyšší<br>2GB RAM (minimum)<br>Windows 2003 Server, Windows 2000 Server, nebo Microsoft Windows NT 4 (SP4, SP6a)<br>síťový protokol TCP/IP<br>Microsoft Internet Explorer 5.5 nebo vyšší<br>zálohovací zařízení (doporučeno) | Intel Pentium III nebo vyšší<br>cca 70 MB volného místa na disku<br>128 MB RAM pro Windows 98,NT4, 2000<br>256 MB RAM pro Windows XP Professional<br>Network připojení: TCP/IP<br>Microsoft Internet Explorer 5.5 nebo vyšší |

**AMM disponuje 4 druhy klientů:**

1. **AMM Power User – klient s plnou integrací CAD systémů. Hlavní využití je pro projekci a konstrukci.**
2. **AMM Office klient – klient bez CAD integrace systémů. Hlavní využití v oblasti editace MS Office.**
3. **AMM Offline klient – pro spolupráci mimo prostředí**
4. **Web klient – použitelný pro uživatele s možnostmi vzdáleného přístupu do systému.**

**Systém podporuje požadavky jakostních norem třídy ISO 9000, 14000, VDA 6.1 a dalších. Použitím ODMA (Open Dokument Management Architecture) technologie, mohou být produkty AMM integrovány do jádra Windows, CAD a Office software programu.**
**AMM obsahuje integrace do vybraných systémů ERP. Jedná se o výměnu kusovníků z prostředí CAD systémů do AMM, odkud je možné veškeré výrobní informace o produktu přesunout pomocí modulu worfflow do vybraného ERP systému.**

*Ukázka možného využití databázového systému v podniku*



# PŘÍLOHA P VIII: CD S PRACÍ V ELEKTRONICKÉ PODOBĚ