

# OBSAH

Předmluva.....	6
Úvod .....	7
<b>1. Elektronická komunikace v praxi.....</b>	<b>10</b>
1.1 Aplikace B2B .....	12
1.2 Aplikace B2C.....	16
1.3 e-Government .....	20
1.3.1 Elektronické podatelny .....	21
1.3.2 Datové schránky a konverze dokumentů.....	25
<b>2. Bezpečná komunikace – základy kryptografie .....</b>	<b>27</b>
2.1 Symetrická kryptografie .....	28
2.2 Asymetrická kryptografie, kryptografie s veřejným klíčem .....	30
2.3 Praktické využití.....	33
2.4 Správa kryptografických klíčů .....	38
<b>3. Certifikáty .....</b>	<b>39</b>
3.1 Struktura certifikátu .....	40
3.2 Typy certifikátů .....	44
3.2.1 Certifikáty CA .....	44
3.2.2 Klientské certifikáty.....	52
3.3 Životní cyklus certifikátu.....	63
3.3.1 Zneplatnění certifikátu – CRL.....	63
3.3.2 Obnova certifikátu .....	67
<b>4. Certifikační autority .....</b>	<b>70</b>
4.1 Autentizační funkce CA.....	70
4.1.1 Mechanismus propojení CA .....	71
4.1.2 Autentizace uživatelů.....	72
4.2 Uložení a distribuce dat .....	72
4.2.1 Uložení a ochrana dat CA.....	72
4.2.2 Zveřejňování dat CA.....	77
4.3 Vydávání certifikátů a certifikačně správní funkce .....	77

---

4.4	Notářské funkce .....	78
4.4.1	Časová razítka .....	79
4.4.2	Atributová autorita .....	89
4.4.3	DVC server .....	90
4.5	Bezpečnost CA .....	91
4.6	Kritéria hodnocení CA .....	92
<b>5.</b>	<b>Legislativa a elektronický podpis .....</b>	<b>99</b>
5.1	Standardizace elektronického podpisu .....	99
5.2	Směrnice EU .....	102
5.3	Směrnice EU v legislativě .....	107
5.4	Zákon o elektronickém podpisu .....	111
5.4.1	Základní pojmy zákona o elektronickém podpisu .....	112
5.4.2	Povinnosti podepisující osoby a osoby spoléhající se na elektronický podpis .....	118
5.4.3	Poskytovatelé certifikačních služeb .....	121
5.4.4	Povinnosti kvalifikovaného poskytovatele certifikačních služeb .....	125
5.4.5	Použití zaručeného elektronického podpisu v praxi .....	129
<b>6.</b>	<b>Elektronický podpis v aplikacích .....</b>	<b>131</b>
6.1	Bezpečný e-mail .....	131
6.2	Bezpečný web .....	139
<b>7.</b>	<b>Potenciální problémy spojené s elektronickým podpisem .....</b>	<b>144</b>
7.1	Archivace dokumentů opatřených elektronickým podpisem .....	144
7.2	Průkaznost provedené operace .....	146
7.3	Mezinárodní uznatelnost elektronického podpisu .....	147
<b>8.</b>	<b>Vybrané klíčové pojmy .....</b>	<b>148</b>
	Použité zdroje .....	152