

## Elektronický podpis v ČR



*Analýza technického a právního stavu a související  
doporučení pro používání elektronického podpisu  
v podmínkách České republiky – říjen 2006*

Vojtěch **KMENT CONSULTING**

Revize 4.01  
Říjen 2006

---

## Obsah

---

<b>1.</b>	<b>ÚVOD</b>	<b>1-1</b>
1.1	Účel studie	1-1
1.2	Adresáti studie	1-1
1.3	Obsah studie podle hlavních struktur oblasti	1-2
1.4	Obsah studie podle kapitol	1-3
1.5	Obsah studie podle dílčích potřeb	1-5
<b>2.</b>	<b>ÚVOD DO ELEKTRONICKÉHO PODPISU</b>	<b>2-1</b>
2.1	Symetrické a asymetrické šifry	2-1
2.2	Princip šifrování a elektronického podpisu s asymetrickou šifrou	2-2
2.3	Včlenění certifikační autority a vznik PKI	2-4
2.3.1	Žádost o certifikát u certifikační autority	2-5
2.3.2	Vytvoření podpisu zprávy, přenos a ověření podpisu s PKI	2-6
2.3.3	Vytvoření podpisu s časovým razítkem	2-7
<b>3.</b>	<b>PRAKTICKÝ POSTUP PŘI POUŽITÍ ELEKTRONICKÉHO PODPISU</b>	<b>3-1</b>
3.1	Postup podpisujícího	3-1
3.1.1	Příprava platformy podpisujícího	3-1
3.1.2	Postup při vytváření podpisu	3-13
3.1.3	Bezpečnostně nežádoucí činnosti	3-14
3.1.4	Žádost o zneplatnění certifikátu podpisujícím (držitelem certifikátu)	3-14
3.1.5	Zneplatnění certifikátu certifikační autoritou	3-15
3.1.6	Seznam zneplatněných certifikátů (CRL)	3-16
3.2	Postup spoléhajícího	3-16
3.2.1	Příprava platformy spoléhajícího (ověřujícího)	3-16
3.2.2	Postup při ověřování podpisu	3-18
3.3	Použití kryptografických čipových karet / tokenů	3-20
3.3.1	Smysl použití čipové karty / tokenu	3-20
3.3.2	Formy kryptografických tokenů	3-21
3.3.3	Pravidla pro pořizování a používání čipových karet / tokenů	3-21
<b>4.</b>	<b>TRŽNÍ SUBJEKTY V OBLASTI ELEKTRONICKÉHO PODPISU V ČR</b>	<b>4-1</b>
4.1	Certifikační autority (Poskytovatelé certifikačních služeb)	4-1
4.1.1	Akreditované certifikační autority v ČR	4-1
4.1.1.i	I.CA	4-1
4.1.1.ii	PostSignum	4-4
4.1.1.iii	ACAeID	4-6
4.1.1.iv	Akreditované CA souhrnně	4-7

4.1.2	Certifikační autority v ČR vydávající kvalifikované certifikáty	4-8
4.1.3	Ostatní certifikační autority v ČR	4-9
<b>4.2</b>	<b>Dodavatelé kryptografických čipových karet/tokenů</b>	<b>4-9</b>
<b>4.3</b>	<b>Software pro čipové karty/tokeny na e-podpis</b>	<b>4-10</b>
<b>4.4</b>	<b>Dodavatelé čteček čipových karet</b>	<b>4-11</b>
<b>4.5</b>	<b>Hlavní klientské aplikace pro e-podpis</b>	<b>4-11</b>
<b>4.6</b>	<b>Příklady serverových aplikací pro e-podpis</b>	<b>4-11</b>
<b>4.7</b>	<b>Veřejně provozované aplikace</b>	<b>4-12</b>
<b>4.8</b>	<b>Vývojáři a dodavatelé elektronických podatelů</b>	<b>4-13</b>
<b>5.</b>	<b>EKONOMIE APLIKACÍ A POUŽITÍ ELEKTRONICKÉHO PODPISU</b>	<b>5-1</b>
<b>5.1</b>	<b>Co představuje elektronický podpis</b>	<b>5-1</b>
5.1.1	Hlavní druhy e-podpisu z hlediska aplikací	5-1
5.1.2	Typický elektronický podpis pro osoby	5-2
<b>5.2</b>	<b>Hlavní trhy použití elektronického podpisu</b>	<b>5-3</b>
5.2.1	Banky a finančníctví	5-3
5.2.2	Státní a veřejná správa	5-5
5.2.3	Mezifiremní datová komunikace	5-7
5.2.4	Podpisy softwarových komponent	5-8
<b>5.3</b>	<b>Hlavní ekonomické výhody elektronického podpisu a jejich měření</b>	<b>5-9</b>
5.3.1	Zefektivnění existujících procesů	5-9
5.3.1.i	Rychlost (úspory času)	5-10
5.3.1.ii	Vzdálenost (podpis na dálku)	5-10
5.3.1.iii	Pohotovost a automatizace (24/7)	5-10
5.3.1.iv	Bezpečnost	5-11
5.3.1.v	Úspory poštovního	5-11
5.3.2	Integrace s ICT (IT)	5-11
5.3.3	Nové produkty a trhy	5-12
<b>5.4</b>	<b>Typické náklady</b>	<b>5-12</b>
<b>5.5</b>	<b>Rizika falsifikace elektronického podpisu</b>	<b>5-13</b>
5.5.1	Rizika pro podpisujícího	5-13
5.5.2	Rizika pro spoléhajícího	5-15
<b>5.6</b>	<b>Odstraňování bezpečnostních hrozeb elektronickým podpisem</b>	<b>5-16</b>
<b>5.7</b>	<b>Námítky proti elektronickému podpisu a jejich řešení</b>	<b>5-17</b>
<b>6.</b>	<b>PRÁVNÍ RÁMEC ELEKTRONICKÉHO PODPISU V EVROPSKÉ UNII</b>	<b>6-1</b>
<b>6.1</b>	<b>Úvod do rámce elektronických podpisů v Evropském společenství</b>	<b>6-1</b>
6.1.1	Platné předpisy a specifikace evropského rámce	6-1
6.1.2	Povinná harmonizace podle Směrnice a navazujících předpisů	6-1
6.1.2.i	Použitelnost znalosti evropského rámce elektronických podpisů	6-2

6.1.3	Dobrovolná harmonizace	6-2
6.1.4	Pojetí Směrnice	6-3
<b>6.2</b>	<b>Hlavní pojmy Směrnice</b>	<b>6-3</b>
6.2.1	Druhy elektronických podpisů ve Směrnici	6-3
6.2.1.i	Elektronický podpis	6-3
6.2.1.ii	Zaručený elektronický podpis	6-4
6.2.1.iii	Kvalifikovaný elektronický podpis (Art. 5.1)	6-5
6.2.1.iv	Elektronický podpis s právními účinky (Art. 5.2)	6-6
6.2.1.v	Přehled druhů elektronických podpisů ze Směrnice	6-7
6.2.2	Prostředek pro bezpečné vytváření podpisu	6-7
6.2.3	Kvalifikovaný certifikát	6-10
<b>6.3</b>	<b>Poskytovatelé služeb</b>	<b>6-11</b>
6.3.1	Poskytovatelé certifikačních služeb	6-12
6.3.1.i	Obecná odpovědnost poskytovatelů certifikačních služeb	6-13
6.3.2	Poskytovatelé certifikačních služeb vydávající kvalifikované certifikáty	6-14
6.3.2.i	Odpovědnost poskytovatelů certifikačních služeb	6-16
6.3.2.ii	Dobrovolná harmonizace podle ETSI TS 101 456	6-18
6.3.3	Certifikační služby na vnitřním trhu Společenství	6-18
6.3.4	Kvalifikované certifikáty a certifikační služby mezinárodně	6-19
<b>6.4</b>	<b>Další záležitosti</b>	<b>6-20</b>
6.4.1	Ověření podpisu	6-20
6.4.2	Dodatečné požadavky pro veřejný sektor	6-21
6.4.3	Záležitosti do Směrnice záměrně nezahrnuté	6-22
6.4.4	Smluvní svoboda pravidel uznávání elektronického podpisu	6-23
6.4.5	Doba latence (grace period)	6-23
6.4.6	Certifikační politika + Prohlášení o certifikačních postupech	6-23
6.4.7	Rozšířené podpisy	6-24
6.4.8	Obecně uznávané standardy	6-24
6.4.9	Oznamovací povinnosti členských států	6-25
6.4.10	Zkratky nejpoužívanějších pojmů	6-25
6.4.11	Další používané zkratky	6-26
<b>6.5</b>	<b>Bezpečnostní služby a mechanismy v mezinárodních normách</b>	<b>6-26</b>
<b>7.</b>	<b>ELEKTRONICKÝ PODPIS V PRÁVNÍM ŘÁDU ČESKÉ REPUBLIKY</b>	<b>7-1</b>
<b>7.1</b>	<b>Úvod do výkladu českých právních předpisů</b>	<b>7-1</b>
7.1.1	Prameny práva a orgány podávající jejich výklad v ČR	7-1
7.1.2	Některé paradoxy výkladů práva	7-2
7.1.3	Charakteristika právního výkladu v této kapitole	7-3
7.1.4	Použití pojmu Elektronický podpis	7-3
<b>7.2</b>	<b>Přehled struktury hlavních platných předpisů</b>	<b>7-4</b>
7.2.1	Zamýšlená struktura předpisů	7-4
7.2.2	Skutečná struktura předpisů v ČR	7-5
<b>7.3</b>	<b>Zákon o elektronickém podpisu (227/2000 Sb.)</b>	<b>7-7</b>
7.3.1	Systematický stručný přehled ZoEP	7-7
7.3.1.i	Druhy subjektů	7-7
7.3.1.ii	Hlavní právní pojmy a jejich souvislosti v ZoEP	7-8
7.3.1.iii	Variety elektronických podpisů a ZoEP	7-9
7.3.1.iv	Veřejnoprávní význam ZoEP	7-10

7.3.1.v	Soukromoprávní význam ZoEP	7-10
7.3.2	Základní pojmy v ZoEP	7-11
7.3.2.i	Datová zpráva	7-11
7.3.2.ii	Prostředek pro vytváření elektronických podpisů	7-11
7.3.2.iii	Podpisující osoba	7-11
7.3.2.iv	Data pro vytváření / ověřování elektronických podpisů	7-12
7.3.2.v	Elektronický podpis	7-12
7.3.2.vi	Zaručený elektronický podpis	7-13
7.3.2.vii	Poskytovatel certifikačních služeb	7-13
7.3.2.viii	Certifikát	7-14
7.3.2.ix	Kvalifikovaný certifikační středek	7-14
7.3.2.x	Kvalifikovaný systémový certifikační středek	7-14
7.3.2.xi	Certifikáty vydané jako kvalifikované	7-14
7.3.2.xii	Kvalifikovaný poskytovatel certifikačních služeb	7-15
7.3.2.xiii	Kvalifikované certifikační služby	7-15
7.3.2.xiv	Akreditovaný poskytovatel certifikačních služeb	7-15
7.3.2.xv	Akreditace	7-16
7.3.2.xvi	Držitel certifikátu	7-16
7.3.2.xvii	Prostředek pro vytváření elektronických značek	7-16
7.3.2.xviii	Označující osoba	7-17
7.3.2.xix	Data pro vytváření / ověřování elektronických značek	7-17
7.3.2.xx	Elektronická značka	7-17
7.3.2.xxi	Uznávaný elektronický podpis	7-18
7.3.2.xxii	Uznávaný el. podpis užívaný v oblasti orgánů veřejné moci	7-18
7.3.2.xxiii	Kvalifikované časové razítko	7-19
7.3.2.xxiv	Prostředek pro ověřování elektronických podpisů	7-20
7.3.2.xxv	Prostředek pro bezpečné vytváření elektronických podpisů	7-20
7.3.2.xxvi	Prostředek pro bezpečné ověřování elektronických podpisů	7-20
7.3.2.xxvii	Nástroj elektronického podpisu	7-20
7.3.2.xxviii	Elektronická podatelna	7-21
7.3.2.xxix	Ministerstvo	7-21
7.3.3	Kvalifikovaný poskytovatel certifikačních služeb	7-21
7.3.3.i	Povinnosti kvalifikovaného PCS obecně (§ 6)	7-22
7.3.3.ii	Povinnosti při vydávání kvalifikovaných certifikátů (§ 6a)	7-26
7.3.3.iii	Náležitosti kvalifikovaného certifikátu (§ 12)	7-28
7.3.3.iv	Zrušení kvalifikovaného certifikátu (§ 15)	7-30
7.3.3.v	Povinnosti kvalifikovaného PCS při ukončení služeb (§ 13)	7-30
7.3.3.vi	Opatření k nápravě (§ 14)	7-31
7.3.3.vii	Zahraniční kvalifikované certifikáty (§ 16)	7-32
7.3.3.viii	Průběh styku s kvalifikovaným PCS při vydání certifikátu	7-32
7.3.4	Akreditovaný poskytovatel certifikačních služeb	7-35
7.3.4.i	Akreditace a dozor (§ 9)	7-35
7.3.4.ii	Podmínky udělení akreditace (§ 10)	7-36
7.3.4.iii	Podmínky pro rozšíření služeb akreditovaného PCS (§ 10a)	7-38
7.3.5	Povinnosti a odpovědnost podepisující osoby (§ 5 ...)	7-39
7.3.5.i	Soulad s požadavky na podpis (§ 3)	7-40
7.3.5.ii	Soulad s originálem – integrita datové zprávy (§ 4)	7-41
7.3.5.iii	Vyplývající povinnosti podepisující osoby	7-41
7.3.6	Povinnosti, práva a odpovědnost držitele certifikátu (§ 5b ...)	7-42
7.3.7	Povinnosti spoléhající osoby	7-42
7.3.8	Oblast orgánů veřejné moci (§ 11)	7-44
7.3.8.i	Jednoznačná identifikace (§ 11) a obtíže zachování soukromí	7-48
7.3.8.ii	Právní účinky veřejné listiny	7-49
7.3.9	Uznávaný elektronický podpis s jednoznačnou identifikací	7-50
7.3.10	Kvalifikovaný elektronický podpis	7-51

7.3.11	Kryptografické požadavky na elektronické podpisy	7-52
7.3.11.i	Požadavky z bezpečnostních standardů a doporučení	7-53
7.3.11.ii	Použití klíčové dvojice pouze pro elektronický podpis	7-54
7.3.12	Elektronická podatelna	7-55
7.3.12.i	Předpisy v oblasti e-podatelen	7-56
7.3.12.ii	Informační povinnosti o e-podatelně dle nař. vl. č. 495/2004 Sb.	7-57
7.3.12.iii	Vedení elektronické podatelny orgány veřejné moci	7-58
7.3.12.iv	Technické funkce e-podatelny podle vyhlášky č. 496/2004 Sb.	7-59
7.3.12.v	Příjem zprávy e-podatelnou (§ 2)	7-59
7.3.12.vi	Odeslání zprávy e-podatelnou (§ 3)	7-62
7.3.12.vii	Architektura elektronické podatelny + implementační poznámky	7-64
7.3.12.viii	Druhy datových zpráv a komunikačních protokolů	7-65
7.3.12.ix	Jednoznačná identifikace osoby v kvalifikovaném certifikátu	7-65
7.3.12.x	Požadavky na kryptografické algoritmy	7-65
7.3.12.xi	E-podatelny a jiní uživatelé než orgány veřejné moci	7-66
7.3.13	Elektronická značka – automatizovaný zaručený elektronický podpis	7-66
7.3.13.i	Shrnutí odlišností elektronické značky	7-68
7.3.13.ii	Úpravy společné pro kvalifikované PCS	7-69
7.3.13.iii	Vydávání kvalifikovaných systémových certifikátů (§ 6a)	7-69
7.3.13.iv	Soulad s požadavky „na elektronickou značku“ (§ 3a)	7-69
7.3.13.v	Náležitosti kvalifikovaného systémového certifikátu (§ 12a)	7-69
7.3.13.vi	Povinnosti označující osoby (§ 5a)	7-70
7.3.13.vii	Prostředek pro bezpečné vytváření elektronických značek (§ 17a)	7-71
7.3.13.viii	Požadavky na ochranu dat pro vytváření elektronických značek	7-71
7.3.14	Kvalifikované časové razítko	7-73
7.3.14.i	Úpravy společné pro kvalifikované PCS	7-74
7.3.14.ii	Vydávání kvalifikovaných časových razítek (§ 6b)	7-74
7.3.14.iii	Náležitosti kvalifikovaného časového razítka (§ 12b)	7-75
7.3.15	Vydávání prostředku pro bezpečné vytváření elektronického podpisu	7-75
7.3.15.i	Úpravy společné pro kvalifikované PCS	7-76
7.3.15.ii	Prostředek pro bezpečné vytváření elektronických podpisů (§ 17)	7-76
7.3.15.iii	Požadavky na prostředky dle vyhlášky č. 366/2001 Sb.	7-77
7.3.15.iv	Požadavky na prostředky dle vyhlášky č. 378/2006 Sb.	7-78
7.3.16	Prostředek pro bezpečné ověřování elektronického podpisu (§ 17)	7-79
7.3.17	Ochrana osobních údajů (§ 8)	7-80
7.3.18	Odpovědnost PCS	7-80
7.3.18.i	Soukromoprávní odpovědnost kvalifikovaného PCS za škodu	7-80
7.3.18.ii	Soukromoprávní odpovědnost běžného PCS	7-83
7.3.18.iii	Odpovědnost kvalifikovaného PCS za správní delikt	7-83
7.3.18.iv	Odpovědnost kvalifikovaného PCS za přestupek	7-84
7.3.18.v	Odpovědnost zaměstnance kvalifikovaného PCS za přestupek	7-85
7.3.18.vi	K odpovědnosti PCS souhrnně	7-85
<b>7.4</b>	<b>Důležité úpravy v jiných zákonech a předpisech ČR</b>	<b>7-85</b>
7.4.1	Občanský zákoník (zákon č. 40/1964 Sb.)	7-85
7.4.1.i	Smluvní svoboda stran	7-85
7.4.1.ii	Písemná forma právního úkonu	7-86
7.4.1.iii	Občansko-právní teorie odpovědnosti za škodu	7-87
7.4.2	Správní řád „starý“ (zákon č. 71/1967 Sb.)	7-87
7.4.3	Nový správní řád (zákon č. 500/2004 Sb.) od 1.1.2006	7-90
7.4.3.i	Obecná pravidla doručování	7-91
7.4.3.ii	Oprávněné úřední osoby	7-92
7.4.3.iii	Započetí správního řízení	7-92
7.4.3.iv	Předvolání	7-94
7.4.3.v	Rozhodnutí aj. formy správních aktů	7-95

7.4.3.vi	Elektronický podpis jako důkaz a předběžné opatření	7-97
7.4.3.vii	Vedení spisu	7-100
7.4.3.viii	Změny zákonů v návaznosti na nový správní řád	7-102
7.4.4	Zákon o archivnictví a spisové službě (č. 499/2004 Sb.)	7-102
7.4.4.i	Spisová služba	7-103
7.4.4.ii	Spisová služba a elektronické podpisy	7-104
7.4.4.iii	Spisová služba a použití výpočetní techniky souhrnně	7-108
7.4.4.iv	Výjimky komunikace ze spisové služby	7-109
7.4.4.v	Spisová služba a soukromoprávní subjekty	7-110
7.4.4.vi	Archivace	7-111
7.4.5	Zákon o správě daní a poplatků (č. 337/1992 Sb.)	7-112
7.4.5.i	Podávání a doručování správci daně	7-112
7.4.5.ii	Pravidla doručování od správce daně	7-115
7.4.5.iii	Rozhodnutí	7-116
7.4.5.iv	Druhy úkonů v daňovém řízení	7-117
7.4.5.v	Vedení spisu	7-119
7.4.5.vi	Elektronický podpis jako důkaz	7-119
7.4.5.vii	Povinnost mlčenlivosti a bezpečnost IT	7-121
7.4.6	Zákon o účetnictví (č. 563/1991 Sb.)	7-121
7.4.6.i	Účetní záznam	7-122
7.4.6.ii	Podpisový záznam	7-122
7.4.6.iii	Průkaznost účetního záznamu	7-123
7.4.6.iv	Přenos účetních záznamů	7-124
7.4.6.v	Konverze mezi písemnou a technickou formou	7-124
7.4.6.vi	Čitelnost technické formy	7-125
7.4.7	Zákon o dani z přidané hodnoty (č. 235/2004 Sb.)	7-125
7.4.8	Občanský soudní řád (zákon č. 99/1963 Sb.)	7-127
7.4.8.i	Podání	7-127
7.4.8.ii	Doručování prostřednictvím veřejné datové sítě	7-128
7.4.8.iii	Úkony účastníků	7-129
7.4.8.iv	Úkony soudu	7-129
7.4.8.v	Vyvěšení na úřední desce	7-130
7.4.8.vi	Vedení spisu	7-131
7.4.8.vii	Elektronický podpis jako důkaz	7-131
7.4.8.viii	Odklad elektronických výpisů z obchodního rejstříku	7-132
7.4.8.ix	Souhrn OSŘ	7-132
7.4.9	Soudní řád správní (zákon č. 150/2002 Sb.)	7-132
7.4.9.i	Podání a úkony účastníků	7-133
7.4.9.ii	Doručování od soudu	7-134
7.4.9.iii	Předvolání	7-134
7.4.9.iv	Nahlížení do spisu	7-134
7.4.9.v	Důkazy s elektronickým podpisem, provádění a hodnocení	7-135
7.4.9.vi	Úkony soudu	7-136
7.4.9.vii	Souhrn SŘS	7-136
7.4.10	Trestní řád (zákon č. 141/1961 Sb.)	7-136
7.4.10.i	Subjekty trestního řízení	7-137
7.4.10.ii	Podání	7-137
7.4.10.iii	Doručování	7-138
7.4.10.iv	Protokol	7-138
7.4.10.v	Nahlížení do spisu	7-140
7.4.10.vi	Úkony orgánů činných v trestním řízení	7-140
7.4.10.vii	Elektronický podpis jako důkaz v trestním řízení	7-140
7.4.10.viii	Předávání osob na základě evropského zatýkacího rozkazu	7-142
7.4.10.ix	Souhrn TrŘ	7-142
7.4.11	Trestní zákon (č. 140/1961 Sb.)	7-142

7.4.12	Zákon o ochraně osobních údajů (č. 101/2000 Sb.)	7-144
7.4.13	Zákon o správních poplatcích (č. 368/1992 Sb.) vs. z. č. 634/2004 Sb.	7-144
7.4.14	Vyhláška č. 339/1999 Sb. NBÚ o objektové bezpečnosti	7-144
7.4.15	Vyhláška č. 528/2005 Sb. NBÚ o fyzické bezpečnosti	7-145
<b>7.5</b>	<b>Historie vývoje předpisů elektronického podpisu v ČR</b>	<b>7-145</b>
7.5.1	Vznik zákona č. 227/2000 Sb. o elektronickém podpisu	7-145
7.5.2	Vyhláška č. 366/2001 Sb. k elektronickému podpisu	7-146
7.5.3	Nařízení vlády č. 304/2001 Sb. k elektronickým podatelním	7-146
7.5.4	Zákon č. 226/2002 Sb. – novela použití e-podpisu v několika zákonech	7-146
7.5.5	Zákon č. 517/2002 Sb. (zřízení Ministerstva informatiky ČR)	7-147
7.5.6	Zákon č. 440/2004 Sb. – zásadní novela ZoEP	7-148
7.5.7	Zákon č. 501/2004 Sb. – zrušení pasáží o starém správním řádu	7-148
7.5.8	Zákon č. 635/2004 Sb. – změny k novému zákonu o správních popl.	7-148
7.5.9	Zákon č. 444/2005 Sb. – změny územních finančních orgánů	7-148
7.5.10	Vyhláška č. 378/2006 Sb. o postupech kvalifikovaných PCS	7-149
<b>7.6</b>	<b>Některé právní problémy s elektronickým podpisem v ČR</b>	<b>7-149</b>
7.6.1	Obecné potíže	7-149
7.6.2	Veřejnoprávní sféra	7-149
7.6.3	Soukromoprávní sféra	7-150
7.6.4	Uživatelské potíže	7-150
<b>7.7</b>	<b>Srovnání českého právního řádu vs. Směrnice EU</b>	<b>7-150</b>
7.7.1	Podpisy dle Art. 5.1 Směrnice	7-151
7.7.2	Podpisy dle Art. 5.2 Směrnice	7-151
7.7.3	Odpovědnost za kvalifikovaný certifikát	7-151
<b>7.8</b>	<b>Závěrečné zhodnocení</b>	<b>7-151</b>
<b>8.</b>	<b>VYBRANÉ EVROPSKÉ NORMY A DOPORUČENÍ</b>	<b>8-1</b>
<b>8.1</b>	<b>Druhy elektronického podpisu</b>	<b>8-1</b>
8.1.1	Druhy elektronického podpisu podle EESSI – fáze I.	8-1
8.1.1.i	General electronic signature (obecný elektronický podpis)	8-1
8.1.1.ii	Advanced electronic signature (zaručený elektronický podpis)	8-2
8.1.1.iii	Advanced electronic signature using qualified certificate (Zaručený elektronický podpis založený na kvalifikovaném certifikátu)	8-2
8.1.1.iv	Qualified electronic signature (Kvalifikovaný elektronický podpis)	8-3
8.1.1.v	Enhanced electronic signature (Rozšířený elektronický podpis)	8-4
8.1.1.vi	Qualified electronic signature with long-term validity (Kvalifikovaný podpis určený pro archivaci dat)	8-4
8.1.2	Druhy elektronického podpisu podle EESSI – dle DirEC	8-5
8.1.3	Druhy elektronického podpisu podle ETSI TS 101 733	8-6
8.1.3.i	Basic Electronic Signature (BES)	8-7
8.1.3.ii	Explicit policy Electronic Signatures (EPES)	8-8
8.1.3.iii	Electronic Signature with Time (ES-T)	8-8
8.1.3.iv	ES with Complete validation data references (ES-C)	8-8
8.1.3.v	EXtended Long Electronic Signature (ES-X Long)	8-9
8.1.3.vi	Extended Long ES with Time (ES-X Long Type 1 / 2)	8-10
8.1.3.vii	Archival Electronic Signature (ES-A)	8-10
8.1.3.viii	Riziko vypršení časových razítek ve formátech e-podpisu	8-10
8.1.4	Druhy elektronického podpisu podle ETSI TS 101 903	8-11
8.1.5	Druhy podpisů podle podpisových algoritmů a podpisových schemat	8-11



<b>8.2</b>	<b>Přehled hlavních evropských dokumentů EESSI + ETSI + CEN/ISSS</b>	<b>8-11</b>
<b>8.3</b>	<b>Podpisové politiky</b>	<b>8-12</b>
8.3.1	Podpisové politiky podle TR 102 041 (Signature Policies Report)	8-12
8.3.2	TR 102 045 (Podpisové politiky pro rozšířený obchodní model)	8-14
8.3.3	Kritický přístup k podpisovým politikám	8-15
<b>8.4</b>	<b>Doba latence při zneplatnění certifikátu (grace period)</b>	<b>8-15</b>
<b>8.5</b>	<b>Prostředek pro bezpečné vytváření podpisu (SSCD)</b>	<b>8-17</b>
8.5.1	Specifikace SSCD pomocí PP obecně	8-18
8.5.2	SSCD Type 1 a SSCD Type 2	8-19
8.5.3	SSCD Type 3	8-20
<b>8.6</b>	<b>Aplikace vytvářející podpis (SCA)</b>	<b>8-21</b>
8.6.1	Popis činnosti komponent SCA	8-23
8.6.2	Varianty implementace SCA	8-25
8.6.3	Rizika prostředí SCA	8-25
<b>8.7</b>	<b>Postup a systém pro ověřování podpisu (CWA 14171)</b>	<b>8-26</b>
8.7.1	Systém pro ověřování podpisů	8-27
8.7.2	Požadavky na bezpečnost systémů ověřujících podpisy	8-28
<b>9.</b>	<b>HODNOCENÍ ZÁRUKY BEZPEČNOSTI PROSTŘEDKŮ A NÁSTROJŮ</b>	<b>9-1</b>
<b>9.1</b>	<b>ISO 15408 (Common Criteria)</b>	<b>9-1</b>
9.1.1	Část 1: Úvod a všeobecný model, užívané pojmy a zkratky...	9-2
9.1.1.i	Pojmy a koncepce ISO 15408 (CC)	9-2
9.1.1.ii	Profil ochrany (PP – Protection Profile)	9-4
9.1.1.iii	Bezpečnostní cíl (ST – Security Target)	9-4
9.1.2	Bezpečnostní funkční požadavky (Část 2)	9-5
9.1.3	Požadavky na záruky bezpečnosti (Část 3)	9-6
9.1.3.i	Přehled tříd záruk bezpečnosti	9-7
9.1.3.ii	Hodnocení profilu ochrany (PP) a bezpečnostního cíle (ST)	9-7
9.1.3.iii	Úroveň míry záruky bezpečnosti (EAL 0 – EAL 7)	9-8
9.1.3.iv	Augmentace a rozšíření úrovně záruk (EAL n+)	9-10
9.1.3.v	Praktičnost indikace podle EAL	9-10
9.1.3.vi	Podpora životního cyklu (ALC – Life cycle support)	9-11
9.1.3.vii	Vývoj (ADV: Development)	9-11
9.1.3.viii	Správa konfigurace (ACM – Configuration management)	9-12
9.1.3.ix	Dodávání a provoz (ADO – Delivery and operation)	9-12
9.1.3.x	Průvodní dokumentace (AGD: Guidance documents)	9-13
9.1.3.xi	Testy (ATE – Tests)	9-13
9.1.3.xii	Ohodnocení zranitelnosti (AVA – Vulnerability assessment)	9-13
9.1.3.xiii	Údržba záruky (AMA – Maintenance of assurance)	9-14
9.1.4	Úroveň míry záruky bezpečnosti 4 (EAL 4)	9-15
<b>9.2</b>	<b>FIPS PUB 140-2 (Bezpečnostní požadavky na kryptografické moduly)</b>	<b>9-17</b>
9.2.1	Uplatnění FIPS PUB 140-1 pro elektronický podpis v ČR	9-18
<b>9.3</b>	<b>Reálná rizika chyb implementací a jejich nalézání</b>	<b>9-18</b>
9.3.1	Chyby v implementaci algoritmů nebo pojetí bezpečnostních funkcí	9-18
9.3.2	Útoky proti čipovým kartám (kryptografickým modulům)	9-18
9.3.3	Klasifikace útočníků	9-20

<b>10.</b>	<b>ALGORITMY PKI PRO ELEKTRONICKÝ PODPIS V ČR</b>	<b>10-1</b>
<b>10.1</b>	<b>Teorie elektronického podpisu</b>	<b>10-1</b>
10.1.1	Podpisová schemata s dodatkem	10-2
10.1.1.i	Podpisové schema s hašovací funkcí	10-3
10.1.1.ii	Podpisová schemata a právní úprava v ČR	10-4
10.1.2	Podpisové algoritmy (asymetrické)	10-5
10.1.3	Hašovací funkce	10-5
<b>10.2</b>	<b>Algoritmy závazně používané dle VyhZoEP</b>	<b>10-8</b>
10.2.1	Specifikace algoritmů ve VyhZoEP	10-8
10.2.1.i	Příloha 1	10-8
10.2.1.ii	Příloha 2	10-9
10.2.2	Výklad příloh VyhZoEP	10-9
10.2.2.i	Vývoj podpisových algoritmů	10-9
10.2.3	Výklad příloh VyhZoEP podle EESSI	10-10
10.2.3.i	Rozdíly mezi EESSI a přílohou VyhZoEP	10-11
10.2.3.ii	Kryptografické hašovací funkce	10-11
10.2.3.iii	Doplňování (padding)	10-12
10.2.3.iv	Podpisové algoritmy	10-12
10.2.3.v	Algoritmy pro generaci klíčů podpisových algoritmů	10-13
10.2.3.vi	Generátory náhodných čísel	10-14
10.2.3.vii	Požadavky na generátor náhodných čísel trueran	10-15
10.2.3.viii	Požadavky na generátor náhodných čísel pseuran	10-15
10.2.3.ix	Generátor klíčů rsagen1	10-15
10.2.3.x	Objektové identifikátory algoritmů	10-16
<b>10.3</b>	<b>Algoritmy závazné dle vyhlášky č. 496/2004 Sb. (e-podatelný)</b>	<b>10-16</b>
<b>10.4</b>	<b>Algoritmy závazné dle vyhlášky č. 378/2006 Sb. – ETSI TS 102 176</b>	<b>10-17</b>
10.4.1	Doporučené hašovací funkce	10-18
10.4.2	Podpisové algoritmy	10-19
10.4.3	Doporučené metody generace klíčů	10-19
10.4.4	Metody doplnění	10-20
10.4.5	Doporučené metody generace náhodných čísel	10-20
10.4.6	Podpisová schémata (suity)	10-20
10.4.7	Identifikace algoritmů pomocí OID	10-21
10.4.8	Identifikace algoritmů pomocí URN	10-22
<b>10.5</b>	<b>Popis vybraných algoritmů PKI</b>	<b>10-23</b>
10.5.1	RSA	10-23
10.5.1.i	Symboly a zkratky	10-24
10.5.1.ii	Definice	10-24
10.5.1.iii	Operace šifrování/dešifrování s RSA	10-24
10.5.1.iv	Postup generování klíčů RSA	10-25
10.5.1.v	Bezpečnost RSA	10-25
10.5.1.vi	Implementace RSA	10-26
10.5.1.vii	RSA a elektronický podpis v ČR	10-27
10.5.2	DSA	10-27
10.5.2.i	Parametry DSA	10-27
10.5.2.ii	Generace podpisu DSA	10-28
10.5.2.iii	Ověření podpisu DSA	10-28
10.5.2.iv	Implementace DSA a podprahový kanál	10-29
10.5.2.v	DSA a elektronický podpis v ČR	10-29
10.5.3	SHA-1 (hašovací funkce)	10-29
10.5.3.i	Pojmy, symboly a operace v SHA-1	10-29

10.5.3.ii	Doplnění zprávy (padding)	10-31
10.5.3.iii	Výpočet otisku zprávy	10-31
10.5.3.iv	SHA-1 a elektronický podpis v ČR	10-32
10.5.4	RIPEMD-160	10-32
10.5.4.i	RIPEMD-160 a elektronický podpis v ČR	10-32
10.5.5	MD5	10-32
10.5.5.i	MD5 a elektronický podpis v ČR	10-33
10.5.6	Délka klíčů a parametry generátorů náhodných čísel	10-33
10.5.7	Odhady trvanlivosti algoritmů a délek klíče podle TS 102 176-1	10-34

## **11. ASN.1 – ABSTRAKTNÍ SYNTAXOVÁ NOTACE JEDNA** **11-1**

<b>11.1</b>	<b>Účel a smysl ASN.1</b>	<b>11-1</b>
11.1.1	Princip základních kódovacích pravidel (BER)	11-3
<b>11.2</b>	<b>Základy jazyka ASN.1</b>	<b>11-4</b>
11.2.1	Základní lexikální pravidla	11-4
11.2.2	Abstraktní typy	11-5
11.2.3	Abstraktní hodnoty	11-6
11.2.4	Základní jednoduché typy a hodnoty	11-7
11.2.4.i	INTEGER	11-7
11.2.4.ii	BOOLEAN	11-7
11.2.4.iii	ENUMERATED	11-7
11.2.4.iv	NULL	11-8
11.2.4.v	BIT STRING	11-8
11.2.4.vi	OCTET STRING	11-9
11.2.4.vii	REAL	11-9
11.2.4.viii	OBJECT IDENTIFIER	11-9
11.2.4.ix	RELATIVE OID	11-10
11.2.5	Řetězcové typy pro texty	11-11
11.2.5.i	IA5String	11-13
11.2.5.ii	PrintableString	11-13
11.2.5.iii	NumericString	11-13
11.2.5.iv	VisibleString, ISO646String	11-13
11.2.5.v	TeletextString, T61String	11-14
11.2.5.vi	VideotexString	11-14
11.2.5.vii	GraphicString	11-14
11.2.5.viii	GeneralString	11-14
11.2.5.ix	UniversalString	11-14
11.2.5.x	BMPString	11-15
11.2.5.xi	UTF8String	11-15
11.2.5.xii	CHARACTER STRING (neomezený znakový řetězcový typ)	11-15
11.2.6	Řetězcové typy pro datum-čas a popis objektů	11-15
11.2.6.i	GeneralizedTime	11-15
11.2.6.ii	UTCTime	11-16
11.2.6.iii	ObjectDescriptor	11-17
11.2.7	Ocedulkované typy (IMPLICIT, EXPLICIT)	11-17
11.2.8	Strukturované typy	11-19
11.2.8.i	SEQUENCE	11-19
11.2.8.ii	SET	11-19
11.2.8.iii	SEQUENCE OF	11-20
11.2.8.iv	SET OF	11-20
11.2.9	Omezené typy – podtypy (constrained types – subtypes)	11-20
11.2.9.i	Omezení typu uvedením hodnot	11-21
11.2.9.ii	Omezení typu jiným kompatibilním typem	11-21

11.2.9.iii	Intervalové omezení hodnot pro INTEGER a REAL	11-22
11.2.9.iv	Omezení SIZE pro řetězce, SEQUENCE OF a SET OF	11-22
11.2.9.v	Omezení abecedy FROM	11-23
11.2.9.vi	Omezení strukturovaných typů WITH COMPONENT(S)	11-23
11.2.9.vii	Další způsoby omezování	11-23
11.2.10	Ostatní typy	11-24
11.2.10.i	CHOICE	11-24
11.2.10.ii	ANY	11-24
11.2.10.iii	EXTERNAL a EMBEDDED PDV	11-25
11.2.11	Moduly ASN.1	11-25
11.2.12	Prostor pro budoucí rozšiřování definic v ASN.1	11-26
11.2.13	Objekty v ASN.1	11-26
11.2.13.i	Objektové identifikátory (OID)	11-27
11.2.13.ii	Strom objektů a pravidla registrací	11-28
<b>11.3</b>	<b>Kódovací pravidla pro ASN.1</b>	<b>11-29</b>
11.3.1	BER (Basic Encoding Rules)	11-30
11.3.2	DER (Distinguished Encoding Rules)	11-30
11.3.3	CER (Canonical Encoding Rules)	11-31
11.3.4	PER (Packet Encoding Rules)	11-31
11.3.5	XER (XML Encoding Rules)	11-31
11.3.6	SER (Signalling Encoding Rules)	11-31
11.3.7	TER (Text Encoding Rules)	11-32
<b>11.4</b>	<b>Stručná historie ASN.1 a existující standardy</b>	<b>11-32</b>
<b>11.5</b>	<b>Do jaké míry porozumět ASN.1 a jeho příslušenství</b>	<b>11-33</b>
11.5.1	Co není popsáno v tomto úvodu do ASN.1	11-34
<b>12.</b>	<b>FORMÁTY PODEPISOVANÉHO OBSAHU</b>	<b>12-1</b>
<b>12.1</b>	<b>Obecné požadavky na formáty obsahu</b>	<b>12-1</b>
<b>12.2</b>	<b>Formáty obsahu v předpisech ČR</b>	<b>12-2</b>
<b>12.3</b>	<b>Formáty obsahu v předpisech SR</b>	<b>12-3</b>
<b>12.4</b>	<b>Doporučené formáty obsahu</b>	<b>12-3</b>
<b>12.5</b>	<b>Některé formáty pro obsah</b>	<b>12-4</b>
12.5.1	TXT (prostý text)	12-5
12.5.2	MIME text/plain	12-6
12.5.2.i	text/plain ; format="Flowed"	12-6
12.5.3	RTF (Rich Text Format – obohacený text)	12-7
12.5.3.i	RTF z hlediska elektronického podpisu	12-10
12.5.4	MIME text/enriched (ETF)	12-11
12.5.5	PDF (Portable Document Format)	12-12
12.5.5.i	Software Adobe Acrobat pro práci s formátem PDF	12-14
12.5.5.ii	Jiné programy pro práci s PDF	12-15
12.5.5.iii	Intelektuální práva použití formátu PDF	12-15
12.5.5.iv	Formuláře v PDF	12-15
12.5.5.v	Bezpečnostní vlastnosti ve formátu PDF	12-15
12.5.5.vi	Elektronický podpis ve formátu PDF	12-16
12.5.5.vii	Předdefinovaná reakce na aktivní prvky při operaci e-podpisu	12-19
12.5.5.viii	Formát PDF z hlediska vhodnosti obsahu pro e-podpis	12-21

12.5.6	HTML	12-22
12.5.6.i	MIME: text/html (RFC 2854)	12-22
12.5.6.ii	HTML z hlediska elektronického podpisu	12-23
12.5.7	XML	12-24
12.5.7.i	XML Document	12-25
12.5.7.ii	DTD (Document Type Definition)	12-26
12.5.7.iii	Entity XML	12-26
12.5.7.iv	Jmenné prostory XML	12-27
12.5.7.v	XLink	12-27
12.5.7.vi	XPointer	12-27
12.5.7.vii	XPath	12-27
12.5.7.viii	Styly	12-28
12.5.7.ix	CSS	12-28
12.5.7.x	XSL, XSLT	12-28
12.5.7.xi	Schémata XML	12-28
12.5.7.xii	XML z hlediska elektronického podpisu	12-29
<b>12.6</b>	<b>XML Signature</b>	<b>12-29</b>
12.6.1	Element Signature a možnosti vztahu podpisu k podepisovaným datům	12-30
12.6.2	Příklad odloučeného podpisu XML dokumentu HTML	12-31
12.6.3	Podpisované atributy (SignatureProperty)	12-32
12.6.4	Algoritmy podporované v XML Signature	12-33
12.6.5	Manifest	12-34
12.6.6	Implementační poznámky	12-35
12.6.7	XML Signature a české předpisy o e-podpisu	12-35
<b>12.7</b>	<b>Kódování znaků</b>	<b>12-36</b>
12.7.1	Přehled historicky existujících kódování češtiny	12-36
12.7.2	ASCII	12-37
12.7.3	ISO 646 (národní ASCII)	12-37
12.7.4	ISO 8859-2	12-38
12.7.5	Windows 1250	12-39
12.7.6	ISO/IEC 10646 (UCS)	12-40
12.7.6.i	UCS-4	12-41
12.7.6.ii	UCS-2 (BMP)	12-41
12.7.7	Unicode	12-41
12.7.7.i	UTF-8	12-42
12.7.8	Bezpečnostní problémy kódování znaků	12-43
<b>13.</b>	<b>STANDARDY PKCS #</b>	<b>13-1</b>
<b>13.1</b>	<b>PKCS #1 (standardní použití algoritmu RSA)</b>	<b>13-2</b>
13.1.1	Kryptografická primitiva RSAEP, RSADP, RSASP1, RSAVP1	13-3
13.1.2	Konverzní primitiva OS2IP a I2OSP	13-4
13.1.3	Masku generující funkce MGF	13-4
13.1.4	Kódovací metody pro šifrování: EME	13-5
13.1.4.i	EME-PKCS1-v1_5	13-5
13.1.4.ii	EME-OAEP (Optimal Assymmetric Encryption Padding)	13-5
13.1.5	Kódovací metody pro podpis s dodatkem: EMSA	13-6
13.1.5.i	EMSA-PKCS1-v1_5	13-7
13.1.5.ii	EMSA-PSS (Probabilistic Signature Scheme)	13-7
13.1.6	Šifrovací schémata	13-8
13.1.6.i	RSAES-PKCS1-v1_5 (Šifrovací schéma)	13-9
13.1.6.ii	RSAES-OAEP (Šifrovací schéma)	13-9
13.1.7	Podpisová schémata s dodatkem	13-10

13.1.7.i	RSASSA-PKCS1-v1_5 (Podpisové schéma)	13-11
13.1.7.ii	RSASSA-PSS (Pravděpodobnostní podpisové schéma)	13-11
13.1.8	Klíče RSA	13-12
13.1.9	Historický vývoj PKCS #1	13-12
13.1.10	Bezpečnostní rizika PKCS #1	13-12
13.1.11	Implementační záležitosti RSA neupravené v PKCS #1	13-13
<b>13.2</b>	<b>PKCS #3: Dohoda klíče algoritmem Diffie-Hellman</b>	<b>13-13</b>
<b>13.3</b>	<b>PKCS #5: Kryptografie založená na použití hesel</b>	<b>13-13</b>
<b>13.4</b>	<b>PKCS #6: Standard rozšíření certifikátu (X.509)</b>	<b>13-15</b>
<b>13.5</b>	<b>PKCS #7: Syntaxe kryptografické zprávy</b>	<b>13-16</b>
<b>13.6</b>	<b>PKCS #8: Syntaxe informace soukromého klíče</b>	<b>13-16</b>
<b>13.7</b>	<b>PKCS #9: Vybrané typy atributů (Selected Attribute Types)</b>	<b>13-16</b>
<b>13.8</b>	<b>PKCS #10: Syntaxe žádosti o certifikát</b>	<b>13-18</b>
<b>13.9</b>	<b>PKCS #11: Programovací rozhraní kryptografického tokenu (Cryptoki)</b>	<b>13-19</b>
<b>13.10</b>	<b>PKCS #12: Syntaxe výměny osobní informace</b>	<b>13-20</b>
<b>13.11</b>	<b>PKCS #13: Standard kryptografie eliptických křivek</b>	<b>13-22</b>
<b>13.12</b>	<b>PKCS #14: Generátory pseudonáhodných čísel (PRNG)</b>	<b>13-22</b>
<b>13.13</b>	<b>PKCS #15: Formát informace v kryptografickém tokenu</b>	<b>13-22</b>
<b>13.14</b>	<b>Způsoby použití standardů PKCS</b>	<b>13-24</b>
13.14.1	PKCS pro elektronický podpis	13-24
13.14.2	PKCS pro certifikační účely	13-24
13.14.3	PKCS pro digitální obálky (šifrování obsahu zpráv)	13-24
13.14.4	Trendy vývoje standardů PKCS	13-25
<b>13.15</b>	<b>PKCS a předpisy o elektronickém podpisu v ČR</b>	<b>13-25</b>
<b>14.</b>	<b>INTERNETOVÉ STANDARDY</b>	<b>14-1</b>
<b>14.1</b>	<b>Úvod do specifikací RFC</b>	<b>14-1</b>
14.1.1	Standardizační proces	14-2
14.1.2	Vývoj specifikací RFC pro elektronický podpis	14-4
<b>14.2</b>	<b>CMS (Cryptographic Message Syntax) RFC 2630</b>	<b>14-6</b>
14.2.1	CMS data	14-7
14.2.2	CMS signed-data	14-7
14.2.3	CMS enveloped-data	14-9
14.2.4	CMS digested-data	14-10
14.2.5	CMS encrypted-data	14-11
14.2.6	CMS authenticated-data	14-11
14.2.7	CMS compressed-data	14-11
<b>14.3</b>	<b>S/MIME</b>	<b>14-12</b>
14.3.1	RFC 822	14-12

14.3.1.i	Trasovací hlavičky	14-14
14.3.1.ii	Hlavičky původu zprávy	14-14
14.3.1.iii	Hlavičky příjemce	14-14
14.3.1.iv	Referenční hlavičky	14-14
14.3.1.v	Ostatní hlavičky	14-14
14.3.1.vi	Hlavičky rozšíření (EXTENSION-FIELDS)	14-15
14.3.1.vii	Uživatелеm definované hlavičky	14-15
14.3.1.viii	Specifikace data a času	14-15
14.3.1.ix	Specifikace poštovní internetové adresy	14-15
14.3.1.x	Specifikace komentáře	14-16
14.3.1.xi	Příklad zprávy dle RFC 822	14-16
14.3.2	MIME	14-16
14.3.2.i	Entita MIME	14-17
14.3.2.ii	Některé definice pojmů v MIME (RFC 2045)	14-18
14.3.2.iii	Struktura hlaviček MIME a odlišení malých a velkých písmen	14-19
14.3.3	MIME-Version	14-19
14.3.3.i	Content-Type	14-19
14.3.3.ii	Content-Transfer-Encoding	14-20
14.3.3.iii	Content-ID	14-22
14.3.3.iv	Content-Description	14-22
14.3.3.v	Content-Disposition	14-23
14.3.3.vi	Entity MIME diskrétního typu	14-23
14.3.3.vii	Entity MIME složeného typu	14-24
14.3.3.viii	Složená entita MIME multipart/...	14-24
14.3.3.ix	Složené entity MIME message/..., message/rfc822	14-25
14.3.3.x	Složená entita MIME message/partial	14-26
14.3.3.xi	Složená entita MIME message/external-body	14-27
14.3.4	S/MIME	14-27
14.3.4.i	S/MIME a CMS	14-28
14.3.4.ii	S/MIME a MIME	14-29
14.3.4.iii	application/pkcs-mime enveloped-data (pouze zaobalení)	14-30
14.3.4.iv	application/pkcs-mime signed-data (pouze podpis)	14-30
14.3.4.v	multipart/signed (pouze podpis)	14-31
14.3.4.vi	application/pkcs-mime certs-only (pouze certifikáty)	14-32
14.3.4.vii	Formát S/MIME podle přípony došlého souboru	14-33
14.3.4.viii	S/MIME a české předpisy pro e-podpis	14-33
<b>14.4</b>	<b>OpenPGP</b>	<b>14-34</b>
14.4.1	Historie programu PGP	14-34
14.4.2	Historie formátu OpenPGP	14-36
14.4.2.i	RFC 1991 (informační specifikace o programu PGP verze 2.6.x)	14-36
14.4.2.ii	RFC 2015, RFC 3156 – PGP/MIME, OpenPGP/MIME	14-37
14.4.2.iii	RFC 2440 – OpenPGP	14-38
14.4.2.iv	Ke slabině OpenPGP a PGP	14-42
14.4.3	OpenPGP a české předpisy pro e-podpis	14-42
14.4.3.i	Srovnání OpenPGP a S/MIME pro použití v ČR a SR	14-44
<b>14.5</b>	<b>PKIX (Public Key Infrastructure using X.509)</b>	<b>14-44</b>
<b>14.6</b>	<b>Privacy Enhanced Mail (PEM)</b>	<b>14-45</b>
<b>14.7</b>	<b>Časové razítko (TSP) – RFC 3161</b>	<b>14-46</b>
14.7.1	Požadavky na TSA	14-47
14.7.2	Požadavky na žadatele o časové razítko	14-48
14.7.3	Transportní protokol žádosti o razítko	14-48
14.7.4	Bezpečnostní poznámky k provozu časových razítek	14-48

<b>15.</b>	<b>CERTIFIKÁTY X.509</b>	<b>15-1</b>
<b>15.1</b>	<b>Účel certifikátů pro e-podpis</b>	<b>15-1</b>
<b>15.2</b>	<b>Varianty X.509</b>	<b>15-2</b>
15.2.1	Původ X.509 v ITU-T	15-2
15.2.2	Verze X.509 v ISO/IEC	15-3
15.2.3	Profil versus standard	15-3
15.2.4	Internetové profily X.509 (PKIX)	15-4
15.2.5	Varianty DER, TXT, PEM, ...	15-4
15.2.6	Jaké X.509 si sehnat?	15-4
<b>15.3</b>	<b>Příprava pro výklad X.509</b>	<b>15-5</b>
15.3.1	ASN.1 a volba jejího provedení pro zápisy syntaxe	15-5
15.3.2	Objekty a OID	15-5
15.3.3	URI (URL, URN)	15-6
15.3.4	Adresář X.500 a pojmy DIB, DIT	15-6
15.3.4.i	Jména položek adresáře DN, RDN	15-8
15.3.4.ii	Stav rozvoje a rozšíření adresáře X.500	15-9
15.3.5	Subjekty a entity vyskytující se při certifikaci	15-9
15.3.6	Vývoj verzí formátů v1, v2, v3	15-9
15.3.6.i	Certifikační cesta a důvěra (PEM versus X.509v3)	15-10
15.3.7	Protokoly pro správu certifikátů	15-11
15.3.8	Zneplatnění certifikátu (revokace)	15-11
<b>15.4</b>	<b>Formát X.509 v3</b>	<b>15-12</b>
15.4.1	signatureAlgorithm (podpisové schéma podpisu certifikátu)	15-13
15.4.2	signatureValue (hodnota podpisu certifikátu)	15-14
15.4.3	version (verze formátu certifikátu)	15-14
15.4.4	serialNumber (sériové číslo certifikátu)	15-15
15.4.5	signature (podpisové schéma podpisu certifikátu)	15-15
15.4.6	issuer (vydavatel certifikátu – certifikační autorita)	15-15
15.4.6.i	Podporované typy atributů podle RFC 3280	15-16
15.4.6.ii	Možné typy atributů uvedené v X.520 (1997)	15-17
15.4.6.iii	Možné typy atributů RDN podle X.521 pro adresář X.500	15-18
15.4.6.iv	Význam nejčastěji používaných atributů	15-18
15.4.6.v	Atribut emailAddress z PKCS #9	15-20
15.4.6.vi	Atributy používané I.CA	15-20
15.4.6.vii	Jaké atributy tedy používat	15-20
15.4.7	validity (období předpokládané platnosti certifikátu)	15-21
15.4.8	subject (certifikovaný subjekt)	15-21
15.4.9	subjectPublicKeyInfo (informace o veřejném klíči subjektu)	15-21
15.4.10	issuerUniqueID, subjectUniqueID	15-22
15.4.11	extensions (rozšíření)	15-22
15.4.12	Standardní rozšíření pro prostředí internetu	15-23
15.4.12.i	authorityKeyIdentifier (identifikátor klíče certifikační autority)	15-23
15.4.12.ii	subjectKeyIdentifier (identifikátor klíče subjektu)	15-23
15.4.12.iii	keyUsage (použitelnost klíče)	15-24
15.4.12.iv	privateKeyUsagePeriod (doba použitelnosti klíče subjektu)	15-25
15.4.12.v	certificatePolicies (certifikátové politiky)	15-25
15.4.12.vi	policyMappings (mapování politik)	15-26
15.4.12.vii	subjectAltName (alternativní jméno subjektu)	15-26
15.4.12.viii	issuerAltName (alternativní jméno vydavatele)	15-27
15.4.12.ix	subjectDirectoryAttributes (adresářové atributy subjektu)	15-27
15.4.12.x	basicConstraints (základní vymezení)	15-27



15.4.12.xi	nameConstraints (vymezení jmen)	15-28
15.4.12.xii	policyConstraints (vymezení politik)	15-28
15.4.12.xiii	extKeyUsage (použitelnost klíče – rozšíření)	15-29
15.4.12.xiv	cRLDistributionPoints (distribuční body CRL)	15-29
15.4.12.xv	inhibitAnyPolicy (potlačení použití anyPolicy)	15-30
15.4.12.xvi	freshestCRL (též známo jako Delta CRL Distribution Point)	15-31
15.4.13	Soukromá rozšíření pro prostředí internetu	15-31
15.4.13.i	authorityInfoAccess (Authority Information Access)	15-31
15.4.13.ii	subjectInfoAccess (Subject Information Access)	15-32
<b>15.5</b>	<b>Formát CRL v2 (Seznam zneplatněných certifikátů)</b>	<b>15-32</b>
15.5.1	signatureValue	15-34
15.5.2	issuer (jméno vydavatele)	15-34
15.5.3	thisUpdate (čas vydání CRL)	15-34
15.5.4	nextUpdate (nejpozdější čas vydání příštího CRL)	15-34
15.5.5	revokedCertificates (zneplatněné certifikáty)	15-34
15.5.6	Rozšíření	15-34
15.5.7	crlExtensions	15-35
15.5.7.i	authorityKeyIdentifier (identifikátor klíče vydavatele CRL)	15-35
15.5.7.ii	issuerAltName (alternativní jméno vydavatele CRL)	15-35
15.5.7.iii	cRLNumber (pořadové číslo CRL)	15-35
15.5.7.iv	deltaCRLIndicator (indikátor rozdílového CRL)	15-36
15.5.7.v	issuingDistributionPoint (distribuční bod CRL)	15-36
15.5.7.vi	freshestCRL (též známo jako Delta CRL Distribution Point)	15-36
15.5.8	crlEntryExtensions	15-36
15.5.8.i	cRLReason (důvod zneplatnění certifikátu)	15-36
15.5.8.ii	holdInstructionCode (kód instrukce při pozdržení certifikátu)	15-37
15.5.8.iii	invalidityDate (čas pravděpodobné kompromitace klíče)	15-37
15.5.8.iv	certificateIssuer (vydavatel certifikátu)	15-37
<b>15.6</b>	<b>OCSP (Online Certificate Status Protocol)</b>	<b>15-38</b>
15.6.1	Žádost OCSP	15-38
15.6.1.i	Nonce	15-39
15.6.1.ii	Acceptable Responses	15-39
15.6.1.iii	Service Locator (Vyhledávač odpovídacích služby)	15-39
15.6.2	Odpověď OCSP	15-39
15.6.2.i	Nonce	15-41
15.6.2.ii	CRL References (odkazy na CRL)	15-41
15.6.2.iii	Archive Cutoff (stáří archivu)	15-41
15.6.2.iv	CRL Entry Extensions	15-42
<b>15.7</b>	<b>Atributové certifikáty X.509 v2</b>	<b>15-42</b>
15.7.1	holder (držitel atributového certifikátu)	15-43
15.7.2	attributes (atributy)	15-45
15.7.3	Příklad možného použití atributových certifikátů v podmínkách ČR	15-45
<b>15.8</b>	<b>X.509 v provedení I.CA</b>	<b>15-46</b>
<b>16.</b>	<b>PRŮMYSLOVÉ STANDARDY</b>	<b>16-1</b>
<b>16.1</b>	<b>Microsoft Windows</b>	<b>16-1</b>
16.1.1	CryptoAPI (Kryptografie v MS Windows)	16-2
16.1.1.i	CSP (Cryptographic Service Provider)	16-3
16.1.1.ii	CryptoAPI: Funkce úložiště certifikátů	16-4
16.1.1.iii	CryptoAPI: Funkce kódování/dekódování certifikátů	16-4

16.1.1.iv	CryptoAPI: Základní kryptografické funkce	16-4
16.1.1.v	CryptoAPI: Funkce pro nízkoúrovňové zpracování zpráv	16-4
16.1.1.vi	CryptoAPI: Funkce pro zjednodušené zpracování zpráv	16-4
16.1.1.vii	Implementace CSP	16-5
16.1.2	Subsystem čipových karet ve Windows	16-5
16.1.2.i	Správce zdrojů (Smart Card Resource Manager)	16-6
16.1.2.ii	Servisní poskytovatelé čipových karet (COM přístup)	16-7
16.1.2.iii	Rozhraní čipových karet (Smart Card Interfaces)	16-7
16.1.2.iv	Čipová karta	16-8
16.1.2.v	Ovladače čteček čipových karet	16-8
16.1.2.vi	Čtečky čipových karet	16-8
16.1.2.vii	Uživatelské rozhraní	16-8
16.1.3	CAPICOM	16-8
16.1.4	Alternativy ke standardní architektuře ve Windows	16-9
<b>16.2</b>	<b>SET</b>	<b>16-9</b>
<b>16.3</b>	<b>SSL</b>	<b>16-11</b>
<b>16.4</b>	<b>EMV</b>	<b>16-12</b>
16.4.1	EMV a elektronický podpis	16-13
<b>16.5</b>	<b>CEPS</b>	<b>16-14</b>
<b>16.6</b>	<b>Java Card</b>	<b>16-14</b>
16.6.1	Bezpečnost Java Card	16-16
16.6.2	Java Card a elektronický podpis v ČR	16-17
<b>16.7</b>	<b>MULTOS</b>	<b>16-17</b>
<b>16.8</b>	<b>Windows for Smart Cards</b>	<b>16-18</b>
<b>16.9</b>	<b>OpenCard Framework (OCF)</b>	<b>16-18</b>
<b>16.10</b>	<b>ISO 7816 – standardizace čipových karet</b>	<b>16-19</b>
<b>17.</b>	<b>PC/SC – PERSONAL COMPUTER / SMART CARD</b>	<b>17-1</b>
<b>17.1</b>	<b>Úvod a přehled architektury PC/SC</b>	<b>17-2</b>
17.1.1	Pro koho je určeno PC/SC, pro koho a jak tato kapitola o PC/SC	17-2
17.1.2	PC/SC Workgroup	17-2
17.1.3	Přínos PC/SC pro (budoucího) uživatele čipové karty	17-2
17.1.4	Vztah PC/SC a zmiňovaných norem	17-2
17.1.5	Slovník PC/SC	17-3
17.1.6	Cíle a motivace PC/SC – výhody uživatele	17-3
17.1.7	Popis architektury PC/SC	17-4
17.1.7.i	ICC (čipová karta)	17-4
17.1.7.ii	IFD (čtečky)	17-5
17.1.7.iii	IFD Handler	17-5
17.1.7.iv	ICC Resource Manager – správce čipových zdrojů	17-5
17.1.7.v	Service Provider	17-6
17.1.7.vi	ICC Aware Application – Aplikace pracující s čipovou kartou	17-7
17.1.7.vii	Hostitelské prostředí PC	17-7
17.1.8	Stanovení výrobce součásti a odpovědnosti	17-7
17.1.9	Oblast soustředění zájmu různých druhů čtenářů	17-8

<b>17.2</b>	<b>Stručný obsah dílů specifikace PC/SC</b>	<b>17-8</b>
17.2.1	Díl 1 – Úvod a přehled architektury PC/SC	17-8
17.2.2	Díl 2 – Požadavky na rozhraní mezi čipovými kartami a čtečkami	17-8
17.2.3	Díl 3 – Požadavky na realizaci IFD připojeného k PC	17-8
17.2.4	Díl 4 – Požadavky na konstrukci IFD a referenční konstrukce	17-9
17.2.5	Díl 5 – Definice modulu ICC Resource Manager	17-9
17.2.6	Díl 6 – Definice rozhraní poskytovatele služeb (ICC Service Provider)	17-9
17.2.7	Díl 7 – Aplikační doména a požadavky na vývoj aplikací	17-10
17.2.8	Díl 8 – Doporučení pro bezpečnost ICC a soukromá zařízení	17-10
<b>17.3</b>	<b>Revize PC/SC v2.0</b>	<b>17-11</b>
17.3.1	Dynamické přiřazování ICC Service Provider a rozšířené rozeznávání čipových karet	17-11
17.3.2	Díl 9 – IFD s rozšířenými schopnostmi	17-12
17.3.3	Podpora synchronních komunikačních protokolů	17-14
17.3.4	Podpora bezkontaktních čipových karet	17-14
<b>18.</b>	<b>VÝZNAMNÉ ORGANIZACE V OBLASTI E-PODPISU</b>	<b>18-1</b>
<b>18.1</b>	<b>Evropská unie</b>	<b>18-1</b>
18.1.1	Hlavní zúčastněné organizace v EU	18-2
18.1.1.i	EESSI --> NISSG	18-2
18.1.1.ii	CEN	18-3
18.1.1.iii	CEN/ISSS (CWA)	18-3
18.1.1.iv	CENELEC	18-3
18.1.1.v	ETSI	18-3
18.1.1.vi	ETSI TC ESI	18-4
18.1.1.vii	ICT Standards Board (ICTSB)	18-6
18.1.2	Zkušebny aj. významné bezpečnostní organizace v ICT	18-7
18.1.2.i	TÜVIT (Seculab)	18-7
18.1.2.ii	BSI (Německo)	18-7
18.1.2.iii	BSI (Spojené království)	18-7
<b>18.2</b>	<b>Česká republika</b>	<b>18-7</b>
18.2.1	ÚOOÚ	18-7
18.2.2	ÚVIS	18-8
18.2.3	Ministerstvo informatiky ČR	18-8
18.2.4	ČSNI	18-8
18.2.5	SPIS	18-9
18.2.6	První certifikační autorita, a.s.	18-9
<b>18.3</b>	<b>Slovenská republika</b>	<b>18-9</b>
18.3.1	Národní bezpečnostný úrad SR	18-9
<b>18.4</b>	<b>Spojené státy americké</b>	<b>18-9</b>
18.4.1	NIST	18-9
18.4.2	NSA	18-10
18.4.3	ANSI	18-10
18.4.4	Americký patentový a značkový úřad	18-11
18.4.5	RSA Security Inc. (RSAS)	18-11
<b>18.5</b>	<b>Mezinárodně působící standardizační instituce a organizace</b>	<b>18-12</b>
18.5.1	ISO	18-12
18.5.2	IEC	18-12
18.5.3	ITU (ITU-T)	18-12
18.5.4	CC (Common Criteria)	18-14

18.5.5	SCSUG	18-15
18.5.6	IEEE	18-15
18.5.7	IETF	18-16
18.5.8	W3C	18-16
18.5.9	Oasis	18-16
18.5.10	ebXML	18-17
18.5.11	PC/SC Workgroup	18-17
18.5.12	SETCo (SET)	18-18
18.5.13	EMVCo (EMV)	18-18
18.5.14	CEPSCo (CEPS)	18-18
18.5.15	Java Card Forum	18-18

**A. SEZNAM POUŽITÝCH ZKRATEK 1**

**B. LITERATURA 1**

## Seznam tabulek

Tab. 4-1 Akreditované certifikační autority v ČR (10/2006) .....	4-1
Tab. 4-2 Certifikační politiky v2.1 pro kvalifikované (systémové) certifikáty vydané I.CA - QRC ..	4-3
Tab. 4-3 Certifikační politika pro sebezodpovědný kořenový certifikát I.CA - QRC .....	4-3
Tab. 4-4 Certifikační politika 1.04 pro komerční certifikáty vydané I.CA - QRC .....	4-3
Tab. 4-5 Certifikační politiky pro autoritu časových razítek vydaných I.CA - TSA .....	4-3
Tab. 4-6 Druhy kvalifikovaných certifikátů vydaných kvalifikovaným PCS „PostSignum Qualified CA“ .....	4-5
Tab. 4-7 Druhy certifikátů vydaných veřejným PCS „PostSignum VCA“ .....	4-5
Tab. 4-8 Druhy certifikátů vydaných kořenovou autoritou PostSignum Root QCA .....	4-5
Tab. 4-9 Certifikační politiky v2.1 pro kvalifikované (systémové) certifikáty vydané ACAeID - QCA .....	4-7
Tab. 4-10 Ostatní veřejné certifikační autority v ČR .....	4-9
Tab. 4-11 Kryptografické čipové karty/tokeny .....	4-9
Tab. 4-12 Integrovaný software čipových karet/tokenů .....	4-10
Tab. 4-13 Čtečky pro čipové karty .....	4-11
Tab. 4-14 Klientské aplikace pro e-podpis .....	4-11
Tab. 4-15 Příklady serverových aplikací pro e-podpis .....	4-12
Tab. 4-16 Aplikace e-podpisu provozované orgány veřejné moci .....	4-13
Tab. 4-17 Vývojáři a dodavatelé elektronických podatelů .....	4-14
Tab. 5-1 Cenové relace součástí aplikací s elektronickým podpisem .....	5-13
Tab. 5-2 Rizika podpisujícího a jeho vhodná protipatření .....	5-14
Tab. 5-3 Rizika spoléhajícího a jeho vhodná protipatření .....	5-16
Tab. 5-4 Teoretické hrozby při komunikaci a vliv e-podpisu na jejich eliminaci .....	5-17
Tab. 6-1 Bezpečnostní služby a mechanismy v mezinárodních normách .....	6-27
Tab. 6-2 Bity rozšíření KeyUsage v certifikátech X.509 podle X.509v3 a RFC 3280 .....	6-27
Tab. 7-1 Zákon o elektronickém podpisu a na něj přímo navazující předpisy platné v 5/2006 .....	7-6
Tab. 7-2 Další zákony s významnou složkou úpravy použití elektronického podpisu .....	7-6
Tab. 7-3 Druhy subjektů v ZoEP .....	7-8
Tab. 7-4 Varianty elektronického podpisu přípustné v ZoEP .....	7-9
Tab. 7-5 Příklady veřejných listin z českého právního řádu (r.2004) .....	7-50
Tab. 8-1 Přehled tříd elektronického podpisu z hlediska DirEC .....	8-5
Tab. 8-2 Druhy účelů podpisu indikované atributem Commitment-type-indication .....	8-7
Tab. 9-1 Přehled tříd bezpečnostních funkcí (třídy v Části 2) .....	9-5
Tab. 9-2 Přehled tříd požadavků na záruky bezpečnosti (třídy v Části 3) .....	9-7
Tab. 9-3 Přehled úrovní míry záruky bezpečnosti (EAL) 0-7 .....	9-8
Tab. 9-4 Stručná charakteristika úrovní míry záruky bezpečnosti (EAL 0 - 7) .....	9-9
Tab. 9-5 Přibližné srovnání úrovní záruk mezi ISO 15408 (CC) – ITSEC – TCSEC .....	9-10
Tab. 9-6 Požadavky pro úroveň míry záruky bezpečnosti EAL 4 .....	9-15
Tab. 10-1 Protokoly a parametry z přílohy 1 VyhZoEP .....	10-8
Tab. 10-2 Protokoly a parametry z přílohy 2 VyhZoEP .....	10-9
Tab. 10-3 Odlišný protokol generování klíčů oproti VyhZoEP .....	10-11
Tab. 10-4 Protokoly uváděné navíc k VyhZoEP .....	10-11
Tab. 10-5 Algoritmy kryptografických hašovacích funkcí podle EESSI .....	10-12
Tab. 10-6 Metody doplnění výsledku před výkonem asymetrického podpisového algoritmus dle EESSI .....	10-12
Tab. 10-7 Podpisové asymetrické algoritmy podle EESSI .....	10-13
Tab. 10-8 Metody generování klíčů pro podpisové algoritmy dle EESSI .....	10-14
Tab. 10-9 Generátory náhodných čísel dle EESSI .....	10-14
Tab. 10-10 Tabulka objektových identifikátorů algoritmů používaných dle metodiky EESSI .....	10-16
Tab. 10-11 „Tabulka č.1 z vyhlášky č. 496/2004 Sb.“ .....	10-17
Tab. 10-12 „Tabulka č.2 z vyhlášky č. 496/2004 Sb.“ .....	10-17
Tab. 10-13 Tabulka doporučených hašovacích funkcí .....	10-18
Tab. 10-14 Podpisové asymetrické algoritmy podle EESSI .....	10-19
Tab. 10-15 Doporučené metody generování klíčů .....	10-19

Tab. 10-16 Metody doplnění.....	10-20
Tab. 10-17 Metody generace náhodných čísel.....	10-20
Tab. 10-18 Podpisová schémata.....	10-21
Tab. 10-19 OID hašovacích algoritmů.....	10-21
Tab. 10-20 OID asymetrických podpisových algoritmů.....	10-21
Tab. 10-21 OID podpisových schémat (suit).....	10-22
Tab. 10-22 URN hašovacích funkcí.....	10-22
Tab. 10-23 URN podpisových schémat (suit).....	10-22
Tab. 10-24 Srovnání délek klíče s podobnou odolností.....	10-33
Tab. 10-25 Odhad použitelnosti hašovacích funkcí (z r. 2005).....	10-34
Tab. 10-26 Odhad použitelných délek klíčů v podpisových schématech (z r. 2005).....	10-34
Tab. 11-1 Příklad tří různých celých čísel v kódování BER (DER zde totožné).....	11-4
Tab. 11-2 Výčet omezených znakových řetězcových typů (pro texty).....	11-12
Tab. 11-3 Přehled typů třídy UNIVERSAL a jejich čísel cedulek.....	11-18
Tab. 11-4 Kombinace omezení použitím více typů či hodnot.....	11-22
Tab. 11-5 Povolené hodnoty identifikátorů kořenových hran ASN.1 typu OBJECT IDENTIFIER.....	11-28
Tab. 11-6 Standardy ITU-T a ISO/IEC pro registraci objektů (OID).....	11-29
Tab. 11-7 Aktuální standardy ITU-T definující ASN.1 a kódovací pravidla.....	11-32
Tab. 12-1 Přehled rozvoje verzí formátu RTF.....	12-7
Tab. 12-2 Přehled rozvoje formátu PDF se zaměřením na e-podpis.....	12-16
Tab. 12-3 Položky tabulky specifické pro políčka signature (tab 7.53 z [PDF13]).....	12-17
Tab. 12-4 Příklad volitelných položek tabulky políčka signature.....	12-17
Tab. 12-5 Nové položky tabulky signature v PDF 1.5.....	12-18
Tab. 12-6 Obsah tabulky právní atestace (legal attestation dictionary) dokumentu PDF v1.6.....	12-21
Tab. 12-7 Způsoby zachycení nebo odkazu na veřejný klíč použitelný pro ověření podpisu.....	12-32
Tab. 12-8 Algoritmy podporované v XML Signature.....	12-34
Tab. 12-9 Kódování znaků v ISO 8859-2 (včetně kódů UCS/Unicode), zdroj: Microsoft Corporation.....	12-38
Tab. 12-10 Kódování znaků ve Windows-1250 (včetně kódů UCS/Unicode), zdroj: Microsoft Corporation.....	12-39
Tab. 12-11 Kódování znaků Unicode ve formátu UTF-8.....	12-43
Tab. 13-1 Přehled standardů PKCS (#1 až #15).....	13-1
Tab. 13-2 Atributy objektové třídy pkcsEntity.....	13-17
Tab. 13-3 Atributy objektové třídy naturalPerson (přirozená osoba).....	13-17
Tab. 13-4 Atributy používané pro podepsovaná data v PKCS #7 (CMS).....	13-17
Tab. 13-5 Atributy používané pro data v PKCS #10.....	13-17
Tab. 13-6 Atributy používané pro „PFX“ PDU v PKCS #12 a tokeny PKCS #15.....	13-18
Tab. 13-7 Atributy definované v S/MIME (pouze pro přehled).....	13-18
Tab. 13-8 Druhy základních informací uložených v PKCS #12.....	13-21
Tab. 13-9 Objektová hierarchie PKCS #15.....	13-23
Tab. 13-10 Druhy a obsah souborů EF podle PKCS #15.....	13-23
Tab. 13-11 Standardy PKCS používané pro elektronický podpis.....	13-24
Tab. 13-12 Standardy PKCS používané pro digitální certifikáty.....	13-24
Tab. 13-13 Standardy PKCS používané pro digitální obálky (šifrování obsahu zpráv).....	13-25
Tab. 14-1 Typy datových obsahů definovaných v CMS.....	14-6
Tab. 14-2 Obsah souborů S/MIME podle typu přípony souboru v poštovní zprávě.....	14-33
Tab. 14-3 Typy podpisu určené ve složce (2) Signature type.....	14-40
Tab. 14-4 Typy podpaketů, pro použití mezi hašovanými podpaky.....	14-41
Tab. 15-1 Přehled objektových (položkových) tříd a jejich povinných atributů.....	15-7
Tab. 15-2 Typy atributů pro složky issuer a subject zmiňované v RFC 3280.....	15-16
Tab. 15-3 Seznam možných atributů dle X.520 (08/97).....	15-17
Tab. 15-4 Atributy určené pro RDN v definicích NAME-FORM podle OBJECT-CLASS položky.....	15-18
Tab. 15-5 Význam nejčastěji používaných atributů z PKIX (RFC 3280) a kvalifikovaných certifikátů I.CA.....	15-19
Tab. 15-6 Význam bitů KeyUsage.....	15-24

Tab. 15-7 Atributy typu IetfAttrSyntax v RFC 3281 .....	15-45
Tab. 16-1 Podpisové algoritmy v balíčku javacard.security z Java Card API 2.2 .....	16-17
Tab. 17-1 Vztah součástí architektury PC/SC - odpovědný výrobce .....	17-7
Tab. 17-2 Na které díly se mají soustředit uvedené druhy čtenářů .....	17-8

## Seznam obrázků

Obr. 1-1 Elektronický podpis: doména mezi více obory a více subjekty .....	1-2
Obr. 2-1 Symetrické šifrování .....	2-1
Obr. 2-2 Asymetrické šifrování .....	2-2
Obr. 2-3 Šifrování s veřejným klíčem (pro Bedřicha) .....	2-2
Obr. 2-4 Digitální podpis (šifrování) s veřejným klíčem (od Adama) .....	2-3
Obr. 2-5 Operace digitální podpisu (od Adama): vytvoření a ověření podpisu .....	2-4
Obr. 2-6 Žádost a získání (kvalifikovaného) certifikátu od certifikační autority .....	2-5
Obr. 2-7 Vytvoření a ověření elektronicky podepsané zprávy s připojeným certifikátem .....	2-6
Obr. 2-8 Vytvoření a ověření elektronicky podepsané zprávy s připojeným časovým razítkem .....	2-7
Obr. 3-1 Příklad vyplnění žádosti pro „zaměstnance“ .....	3-7
Obr. 3-2 Výběr „Poskytovatele certifikačních služeb“ .....	3-8
Obr. 3-3 Výřez ze správce souborů (I.CA Cryptoplus) po dokončení importu certifikátu .....	3-12
Obr. 4-1 Struktura podpisujících klíčů v I.CA (10/2006) .....	4-2
Obr. 4-2 Struktura podpisujících klíčů v PostSignum (9/2006) .....	4-4
Obr. 4-3 Struktura podpisujících klíčů v eIdentity (9/2006) .....	4-6
Obr. 6-1 Druhy elektronického podpisu zavedené Směrnicí .....	6-7
Obr. 7-1 Zamýšlená koncepce struktury legislativy a standardů v roce 1999 .....	7-4
Obr. 7-2 Výsledná struktura legislativy a standardů v ČR v roce 2006 .....	7-5
Obr. 7-3 Příjem zprávy v elektronické podatelně .....	7-60
Obr. 7-4 Odeslání zprávy v elektronické podatelně .....	7-63
Obr. 7-5 Nejjednodušší použití e-značky .....	7-67
Obr. 7-6 Použití e-značky pro automatické výpisy v typickém úřadě .....	7-67
Obr. 8-1 General electronic signature (elektronický podpis) .....	8-1
Obr. 8-2 Advanced electronic signature (zaručený elektronický podpis) .....	8-2
Obr. 8-3 Advanced electronic signature using qualified certificate (Zaručený elektronický podpis založený na kvalifikovaném certifikátu) .....	8-2
Obr. 8-4 Qualified electronic signature (Kvalifikovaný elektronický podpis) .....	8-3
Obr. 8-5 Enhanced electronic signature (Vylepšený elektronický podpis) .....	8-4
Obr. 8-6 Qualified electronic signature with long-term validity (Kvalifikovaný podpis určený pro archivaci dat) .....	8-5
Obr. 8-7 Předpokládaný přenosový formát dat s podpisem .....	8-6
Obr. 8-8 Základní elektronický podpis (BES) .....	8-7
Obr. 8-9 Elektronický podpis s časem (ES-T) .....	8-8
Obr. 8-10 Elektronický podpis s úplnými odkazy na validační data (ES-C) .....	8-9
Obr. 8-11 Rozšířený dlouhý elektronický podpis (ES-X Long) .....	8-9
Obr. 8-12 Rozšířený dlouhý elektronický podpis s časem (ES-X Long Type 1 / 2) .....	8-10
Obr. 8-13 Archivní elektronický podpis (ES-A) .....	8-10
Obr. 8-14 Přehled dokumentů EESSI + ETSI + CEN/ISSS .....	8-11
Obr. 8-15 Doba latence (Grace period) .....	8-16
Obr. 8-16 SSCD Type 1 a SSCD Type 2 .....	8-19
Obr. 8-17 SSCD Type 3 .....	8-20
Obr. 8-18 Aplikace vytvářející podpis (SCA) ve funkčním modelu vytváření podpisu .....	8-21
Obr. 8-19 Informační model vytváření podepsaného datového objektu .....	8-22
Obr. 9-1 Odvození požadavků a specifikace .....	9-3
Obr. 10-1 Podpisové schema s obnovou zprávy .....	10-2
Obr. 10-2 Podpisové schema s dodatkem .....	10-2
Obr. 10-3 Podpisové schema s hašovací funkcí .....	10-3

Obr. 10-4 Podpisové schema s hašovací funkcí při použití algoritmu s obnovou zprávy .....	10-4
Obr. 10-5 Kompresní vlastnost všech hašovacích funkcí.....	10-6
Obr. 10-6 Kryptografické jednosměrné hašovací funkce odolné proti kolizím .....	10-7
Obr. 10-7 Jeden průchod jádra algoritmu SHA-1 (krok 4) .....	10-32
Obr. 11-1 Vlevo: komunikace každý s každým. Vpravo: komunikace prostřednictvím syntaxe ASN.1 .....	11-1
Obr. 11-2 Syntaxová triáda: abstraktní syntaxe, konkrétní syntaxe, přenosová syntaxe.....	11-2
Obr. 11-3 Kódování BER pro strukturovanou hodnotu (např. typu SEQUENCE se třemi jednoduchými složkami).....	11-4
Obr. 11-4 Kódování ocedulkovaných typů v BER pro kvalifikátory IMPLICIT a EXPLICIT s cedulkou Tc .....	11-17
Obr. 11-5 Strom registrovaných objektů.....	11-28
Obr. 12-1 Základní struktura XML Signature.....	12-30
Obr. 13-1 Kódovací metoda pro šifrování EME-PKCS1-v1_5.....	13-5
Obr. 13-2 Kódovací metoda pro šifrování EME-OAEP .....	13-6
Obr. 13-3 Kódovací metoda pro podpis s dodatkem EMSA-PKCS1-v1_5 .....	13-7
Obr. 13-4 Kódovací metoda pro podpis s dodatkem EMSA-PSS.....	13-8
Obr. 14-1 Varianty standardizačního procesu a možné typy/stavy RFC specifikací .....	14-2
Obr. 14-2 Přehled vývoje RFC standardů v oblasti poštovních zpráv, elektronického podpisu, důvěrnosti obsahu, certifikátů a certifikačních služeb .....	14-5
Obr. 14-3 Podepsaná data CMS v případě bez podepisovaných atributů .....	14-8
Obr. 14-4 Podepsaná data CMS v případě s podepisovanými atributy.....	14-8
Obr. 14-5 Podpisový strom CMS.....	14-9
Obr. 14-6 Struktura CMS enveloped-data a postup rozšifrování obsahu.....	14-10
Obr. 14-7 Zpráva ve formátu dle RFC 822 a s omezeními z RFC 821 (SMTP).....	14-12
Obr. 14-8 Entita MIME.....	14-17
Obr. 14-9 Složená entita MIME Multipart.....	14-24
Obr. 14-10 Složená entita MIME message/rfc822.....	14-26
Obr. 14-11 Složená entita MIME message/partial .....	14-27
Obr. 14-12 Oblast specifikace S/MIME.....	14-29
Obr. 14-13 S/MIME - zaobalený zašifrovaný obsah v application/pkcs-mime .....	14-30
Obr. 14-14 S/MIME - podepsaný obsah v application/pkcs-mime .....	14-31
Obr. 14-15 S/MIME - Podepsaný odloučený obsah multipart/signed .....	14-32
Obr. 14-16 S/MIME - samostatné certifikáty a/nebo CRL .....	14-32
Obr. 14-17 Formátování PGP dat programu PGP 2.6.x.....	14-36
Obr. 15-1 "Obecná" struktura certifikátů veřejného klíče.....	15-1
Obr. 15-2 Adresář (DIB) a jeho stromová struktura DIT, a struktura položek DIB/DIT.....	15-7
Obr. 15-3 Vytváření jmen položek RDN a DN.....	15-8
Obr. 15-4 Struktura certifikátu X.509 v3 .....	15-13
Obr. 15-5 Struktura seznamu zneplatněných certifikátů CRL v2 .....	15-33
Obr. 15-6 Příklad použití atributového certifikátoru pro identifikátory úřadů.....	15-46
Obr. 16-1 Architektura použití kryptografických služeb a čipových karet v MS Windows .....	16-1
Obr. 17-1 Architektura specifikace PC/SC a rozdělení jejího popisu do dílů 1 až 8 .....	17-1
Obr. 17-2 PS/2 klávesnice kombinovaná s čtečkou a poskytující bezpečný izolovaný PIN.....	17-9
Obr. 17-3 Způsob identifikace ICC s ATR (v1.0) a s Card Info Structure (v2.0).....	17-12
Obr. 17-4 Moduly IFD SP a Logická zařízení .....	17-13
Obr. 18-1 Názvy a čísla norem ISO/IEC a CC pro hodnocení bezpečnosti informačních technologií .....	18-15