

Úroveň I – Přehled

Kapitola 1

- 1. Základní pojmy a souvislosti — 27**
 - 1.1 Zpráva vs. dokument — 27
 - 1.2 Písemná, listinná a elektronická podoba dokumentu — 27
 - 1.3 Podpis, elektronický podpis, digitální podpis — 28
 - 1.4 Zaručený a uznávaný elektronický podpis — 30
 - 1.5 Integrita, identifikace a nepopíratelnost — 30
 - 1.6 Důvěrnost, autorizace, autenticita — 32
 - 1.7 Elektronické značky — 34
 - 1.8 Časová razítka — 35
 - 1.9 Klíče a asymetrická kryptografie — 36
 - 1.10 Certifikáty — 37
 - 1.10.1 Komerční a kvalifikované certifikáty — 40
 - 1.11 Certifikační autority — 42
 - 1.11.1 Kvalifikované a akreditované certifikační autority — 42
 - 1.11.2 Kořenové a podřízené certifikační autority — 44
 - 1.12 PKI, aneb infrastruktura veřejného klíče — 46
 - 1.12.1 Důvěra, nedůvěra a nedostatek informací o důvěryhodnosti — 50
 - 1.12.2 Vyjadřování důvěry v certifikát — 50
 - 1.12.3 Hierarchie certifikátů a certifikační cesty — 53
 - 1.13 Alternativní koncepce elektronického podpisu — 54
 - 1.13.1 Pavučina důvěry, místo stromu důvěry — 54
 - 1.13.2 Biometrické podpisy — 56

Úroveň II – Principy

Kapitola 2

- 2. Vytváření elektronických podpisů — 63**
 - 2.1 Elektronický podpis není jako známka — 63
 - 2.2 Elektronický podpis není jako otisk razítka — 65
 - 2.3 Prostředky a data pro vytváření elektronických podpisů — 66
 - 2.4 Zajištění integrity podepsaného dokumentu — 68
 - 2.5 Hašování a hašovací funkce — 70
 - 2.5.1 Máme se bát kolizí? — 71
 - 2.6 Faktor času u elektronického podpisu — 74
 - 2.6.1 Proč elektronické podpisy zastarávají? — 74
 - 2.6.2 Doba vzniku elektronického podpisu — 75
 - 2.7 Časová razítka — 76
 - 2.7.1 Jak vzniká časové razítko? — 78
 - 2.8 Interní a externí elektronické podpisy — 80

Kapitola 3

- 3. Ověřování elektronických podpisů — 85**
 - 3.1 Základní pravidla ověřování platnosti elektronických podpisů — 85
 - 3.2 Ověření integrity podepsaného dokumentu — 89
 - 3.3 Posuzovaný okamžik — 92
 - 3.4 Ověření platnosti certifikátu — 95
 - 3.4.1 Možnost revokace certifikátu — 96
 - 3.4.2 Protokol OCSP a seznamy CRL — 97
 - 3.4.3 Postup při ověřování revokace certifikátu — 99
 - 3.4.4 Kumulativní a intervalové CRL seznamy — 100
 - 3.4.5 Jak dlouho je možné revokovat? — 101
 - 3.5 Platnost nadřazených certifikátů — 102
 - 3.5.1 Certifikační cesta — 103
 - 3.5.2 Jak se hledá certifikační cesta? — 104

Kapitola 4**4. Elektronický podpis z pohledu práva — 111**

- 4.1 Co není (zaručeným) elektronickým podpisem — 112
- 4.2 Zaručený elektronický podpis — 116
 - 4.2.1 Co schází zaručenému elektronickému podpisu? — 119
- 4.3 Certifikáty, certifikační autority a certifikační politiky — 119
 - 4.3.1 Účely certifikátů — 120
 - 4.3.1.1 Kritické a nekritické účely — 121
 - 4.3.2 Certifikační politiky — 122
 - 4.3.3 Osobní vs. systémové certifikáty — 123
 - 4.3.4 Kvalifikované vs. komerční certifikáty — 124
 - 4.3.5 Proč je nutné používat komerční certifikáty? — 126
 - 4.3.6 Jak se pozná kvalifikovaný certifikát? — 127
- 4.4 Zaručený elektronický podpis, založený na kvalifikovaném certifikátu — 128
 - 4.4.1 Prostředky pro bezpečné vytváření a ověřování elektronických podpisů — 130
- 4.5 Uznávaný elektronický podpis — 131
 - 4.5.1 Jak se pozná uznávaný elektronický podpis? — 131
 - 4.5.2 Platnost elektronického podpisu z pohledu programů — 133
 - 4.5.3 TSL, Trusted Services List — 135
 - 4.5.4 Aplikace CertIQ — 137
- 4.6 Elektronická značka — 139
 - 4.6.1 Uznávaná elektronická značka — 141
 - 4.6.2 Elektronické značky a systémové certifikáty — 141
- 4.7 Časové razítko — 142
 - 4.7.1 Kvalifikované časové razítko — 145
- 4.8 Hierarchie podpisů, značek a razítek — 145
- 4.9 Komu patří elektronický podpis? — 147
 - 4.9.1 Subjekt certifikátu — 148
 - 4.9.2 Požadavek zákona na jednoznačnou identifikaci držitele certifikátu — 151
 - 4.9.3 Certifikáty s pseudonymem — 152

- 4.9.4 Zaměstnanecké certifikáty — 153
- 4.10 Platnost elektronického podpisu — 155
 - 4.10.1 Platnost podpisu vs. možnost ověřit platnost podpisu — 156
 - 4.10.2 Digitální kontinuita — 156
 - 4.10.2.1 Řešení s přerázkováním — 159
 - 4.10.2.2 Řešení s důvěryhodnou úschovou — 160
 - 4.10.2.3 Řešení na bázi vyvratitelné domněnky pravosti — 161
 - 4.10.2.4 Proč to s elektronickými podpisy není stejné, jako s vlastnoručními? — 162
 - 4.10.3 Elektronické podpisy s možností ověření i po dlouhé době — 164
 - 4.10.3.1 Koncept LTV (Long Term Validation) — 164
 - 4.10.3.2 „Pokročilé“ elektronické podpisy – CadES, XAdES a PAdES — 165

Úroveň III – Praxe**Kapitola 5****5. Elektronický podpis v počítači — 173**

- 5.1 Úložiště certifikátů — 173
 - 5.1.1 Vlastní certifikáty vs. certifikáty třetích stran — 174
 - 5.1.2 Logická a fyzická úložiště — 177
 - 5.1.3 Úložiště na čipových kartách a USB tokenech — 178
 - 5.1.3.1 Rozhraní CryptoAPI a moduly CSP — 180
 - 5.1.3.2 Softwarová instalace externích úložišť — 181
 - 5.1.3.3 Programy vyžadující uživatelskou instalaci externího úložiště — 185
- 5.2 Příprava webového prohlížeče pro práci s elektronickými podpisy — 187
 - 5.2.1 XML Filler jako plug-in — 188
 - 5.2.2 Softwarové knihovny pro podepisování — 189
- 5.3 Formáty certifikátů — 191
 - 5.3.1 Standard X.509 a položky certifikátu — 192

- 5.3.1.1 DN: Distinguished Name — 194
- 5.3.1.2 Formáty DER a PEM (pro certifikáty) — 196
- 5.3.2 Standardy PKCS — 198
 - 5.3.2.1 Formát PKCS#7 (pro podpisy i certifikáty) — 199
 - 5.3.2.2 Kódování PKCS#12 (pro certifikáty a soukromé klíče) — 199
- 5.3.3 Přípony souborů s certifikáty (a klíči) — 200
- 5.4 Správa certifikátů třetích stran — 201
 - 5.4.1 Není úložiště jako úložiště — 201
 - 5.4.2 Struktura úložišť certifikátů — 202
 - 5.4.2.1 Úložiště certifikátů programu Adobe Reader — 203
 - 5.4.2.2 Úložiště certifikátů prohlížeče Mozilla Firefox — 205
 - 5.4.2.3 Systémové úložiště certifikátů v MS Windows — 206
 - 5.4.3 Počáteční obsah úložišť certifikátů — 209
 - 5.4.3.1 Program MRCP společnosti Microsoft — 210
 - 5.4.3.2 Statut autorit, jejichž certifikáty nejsou zařazeny do úložišť — 211
 - 5.4.3.3 Program AATL společnosti Adobe — 214
 - 5.4.4 Přidávání dalších certifikátů do úložišť důvěryhodných certifikátů — 214
 - 5.4.4.1 Automatické přidávání kořenových certifikátů — 215
 - 5.4.4.2 Automatické přidávání podřízených certifikátů — 217
 - 5.4.4.3 Ruční přidávání certifikátů — 219
- 5.5 Správa vlastních certifikátů — 227
 - 5.5.1 Co je třeba vědět, než budete žádat o vydání certifikátu? — 228
 - 5.5.1.1 Kde generovat párová data? — 229
 - 5.5.1.2 Možnost exportu soukromého klíče — 230
 - 5.5.1.3 Generování soukromého klíče přímo v čipové kartě či tokenu — 232
 - 5.5.1.4 Ověření identity žadatele — 233
 - 5.5.1.5 Obnova certifikátů — 233
 - 5.5.2 Žádost o vydání nového certifikátu — 234
 - 5.5.2.1 Možnosti generování žádostí o vydání certifikátu — 235
 - 5.5.2.2 Generování žádosti on-line způsobem — 235
 - 5.5.2.3 Generování žádosti off-line způsobem — 242
 - 5.5.3 Generování žádosti o následný certifikát (obnova certifikátu) — 243
 - 5.5.3.1 Kdy je vhodné žádat o následný certifikát? — 245
 - 5.5.4 Zálohování a obnova certifikátů a soukromých klíčů — 246
 - 5.5.5 Revokace certifikátu — 251

Kapitola 6

6. PDF dokumenty a elektronický podpis — 257

- 6.1 Interní podpisy PDF dokumentů — 257
- 6.2 Certifikace PDF dokumentů — 260
- 6.3 Časová razítka na PDF dokumentech — 262
- 6.4 Důvod a místo podpisu — 265
- 6.5 Ověřování interních elektronických podpisů v programu Adobe Reader — 267
 - 6.5.1 Identita podepsané osoby — 270
 - 6.5.2 Kontrola integrity podepsaného dokumentu — 272
 - 6.5.3 Volba posuzovaného okamžiku — 272
 - 6.5.4 Kontrola revokace certifikátu — 277
 - 6.5.5 Kontrola revokace již expirovaného certifikátu — 282
 - 6.5.6 Kontrola revokace podle vložených revokačních informací — 283
 - 6.5.7 Kontrola řádné doby platnosti certifikátu — 286
 - 6.5.8 Platnost nadřazených certifikátů — 286
 - 6.5.9 Úložiště certifikátů — 287
 - 6.5.10 Jaké certifikáty zařadit mezi důvěryhodné? — 289
 - 6.5.11 Jak poznat uznávaný podpis? — 289
 - 6.5.12 Jak poznat kvalifikované časové razítko — 292

- 6.6 Ověřování interních podpisů jinými programy — 296
- 6.7 Ověřování externích elektronických podpisů na PDF dokumentech — 298
- 6.8 Podepisování PDF dokumentů nástroji třetích stran — 301
 - 6.8.1 Virtuální PDF tiskárny — 301
 - 6.8.2 Samostatné konverzní programy — 304
 - 6.8.3 Samostatné programy pro podepisování — 305
 - 6.8.4 Vytváření viditelných podpisů — 306
 - 6.8.5 Vytváření externích podpisů — 308
 - 6.8.6 Přidávání (podpisových) časových razítek — 311
- 6.9 Podepisování PDF dokumentů programem Adobe Acrobat — 314
 - 6.9.1 Nastavení programu Adobe Acrobat — 314
 - 6.9.2 Náhled podpisu — 316
 - 6.9.3 Druhy podpisů — 319
 - 6.9.4 Správa viditelných podpisů — 321
 - 6.9.5 Certifikační podpisy — 323
 - 6.9.6 Prázdné podpisy — 325
 - 6.9.7 „Schvalující“ podpisy — 327
- 6.10 Podepisování PDF dokumentů programem Adobe Reader — 328
 - 6.11 PDF dokumenty „na delší dobu“ — 331
 - 6.11.1 „Nálepka“ PDF/A-1 — 331
 - 6.11.2 Dokumenty PAdES — 333
 - 6.11.3 Nastavení Acrobatu a Readeru verze 9 pro vytváření podpisů PAdES Basic — 335
 - 6.11.4 Nastavení Acrobatu a Readeru verze X pro vytváření podpisů PAdES — 337
 - 6.11.5 Přidávání „archivních“ časových razítek k PDF dokumentům — 338

Kapitola 7

- 7. Elektronický podpis v MS Office — 343**
 - 7.1 Elektronické podpisy v programu MS Word XP a 2003 — 344
 - 7.1.1 Ověřování podpisů — 345
 - 7.2 Elektronické podpisy v programu MS Word 2007 — 348

- 7.2.1 Ověřování podpisů — 349
- 7.2.2 Vytváření podpisů — 353
- 7.3 Elektronické podpisy v programu MS Word 2010 — 354
 - 7.3.1 Podpora XAdES — 355
 - 7.3.1.1 Nastavení XAdES — 356
 - 7.3.1.2 Vytváření neviditelných XAdES podpisů — 358
 - 7.3.2 Ověřování podpisů — 362
 - 7.3.3 Částečné podpisy — 365
 - 7.3.4 Zpětná kompatibilita XAdES podpisů — 365
 - 7.3.5 Viditelné elektronické podpisy — 367
- 7.4 Elektronické podepisování e-mailových zpráv — 370
 - 7.4.1 Profily (nastavení zabezpečení) — 371
 - 7.4.2 Podepisování odesílaných zpráv — 374
 - 7.4.2.1 Význam podpisu na odesílané poštovní zprávě — 376
 - 7.4.2.2 E-mailová adresa v certifikátu — 376
 - 7.4.3 Příjem podepsaných zpráv — 377
 - 7.4.4 Ověřování podpisů v MS Outlook — 379
- 7.5 MS Office a SHA-2 — 381
 - 7.5.1 Operační systém — 382
 - 7.5.2 Aplikace — 383
 - 7.5.3 Moduly CSP — 384
 - 7.5.4 Příklady, kdy SHA-2 není podporována — 385

Kapitola 8

- 8. Šifrování, přihlašování a zabezpečená komunikace — 391**
 - 8.1 Šifrování — 391
 - 8.1.1 Symetrické šifrování — 391
 - 8.1.2 Asymetrické šifrování — 393
 - 8.1.3 Šifrování v programu MS Outlook — 395
 - 8.2 Přihlašování — 399
 - 8.2.1 Registrace uživatelského certifikátu — 401
 - 8.2.2 Přihlašování ke službě MojeID prostřednictvím certifikátu — 402
 - 8.2.3 Přihlašování k datovým schránkám pomocí certifikátu — 405

- 8.3 Zabezpečená komunikace — **409**
- 8.3.1 Sítě VPN — **409**
- 8.3.2 SSL komunikace — **410**
- 8.3.2.1 SSL certifikáty s rozšířenou validací
(EV certifikáty) — **414**
- 8.3.3 DNSSEC — **416**

Literatura a další zdroje — 425

On-line podpora knihy — 429