

# Stručný obsah

|   |     |
|---|-----|
| 1. Symetrická a asymetrická kryptografie                                      | 21  |
| 2. Prostředky pro bezpečné ukládání aktiv                                     | 37  |
| 3. Certifikáty a certifikační autority  | 53  |
| 4. Žádost o certifikát  | 79  |
| 5. Odvolávání certifikátu   | 87  |
| 6. Certifikační cesta a důvěryhodné kotvy                                     | 95  |
| 7. Ověřování platnosti certifikátu a poznámka k ověřování digitálního podpisu | 107 |
| 8. Obnovování certifikátů   | 115 |
| 9. PKI nejsou jen certifikáty   | 121 |
| 10. Kvalifikované certifikáty a zaručené podpisy                              | 125 |
| 11. Má první certifikační autorita  | 139 |
| 12. Nástroje pro sledování sítě   | 161 |
| 13. ASN.1, BER, DER, UTF-8 a Base64   | 173 |
| 14. Žádost o vydání certifikátu pod lupou                                     | 199 |
| 15. Certifikát pod lupou  | 209 |
| 16. odvolání certifikátu pod lupou  | 257 |
| 17. CMP a CMC   | 275 |
| 18. Budujeme certifikační autoritu  | 297 |
| 19. Atributové certifikáty  | 323 |
| 20. Časová razítka  | 345 |
| 21. E-notary  | 369 |
| 22. Protokol TLS  | 381 |
| 23. PKCS#7 a CMS  | 415 |
| 24. Bezpečná pošta  | 441 |
| 25. Dlouhodobý digitální podpis   | 487 |
| 26. Dlouhodobá archivace nejenom digitálně podepsaných dokumentů              | 511 |
| 27. Budujeme PKI, TSA a důvěryhodné archivy                                   | 523 |
| Rejstřík  | 537 |



# Obsah

|                                  |           |
|----------------------------------|-----------|
| <b>Úvod</b>                      | <b>17</b> |
| <b>Jak tuto knihu číst</b> ..... | <b>18</b> |
| <b>Poděkování</b> .....          | <b>19</b> |

## Kapitola 1

|   |           |
|---|-----------|
| <b>Symetrická a asymetrická kryptografie</b>  | <b>21</b> |
| <b>Otisk (hash)</b> .....   | <b>21</b> |
| <b>Replay attack, nonce</b> .....   | <b>23</b> |
| <b>Symetrické šifry</b> .....   | <b>24</b> |
| <b>Asymetrické šifry</b> .....  | <b>25</b> |
| <b>Elektronická obálka</b> .....  | <b>26</b> |
| <b>Digitální podpis</b> .....   | <b>27</b> |
| <b>Prokazování totožnosti (autentizace) na základě asymetrické kryptografie</b> ..... | <b>28</b> |
| <b>Tři typy asymetrických klíčů</b> .....   | <b>29</b> |
| <b>Elektronický podpis, digitální podpis a kvalifikovaný podpis</b> .....             | <b>30</b> |
| <b>Autentizační metody založené na jiných principech</b> .....                        | <b>31</b> |
| Stálá hesla.....  | 31        |
| Jednorázová hesla.....  | 32        |
| Rekurentní algoritmus.....  | 33        |
| Sdílené tajemství.....  | 34        |
| Symetrická šifra.....   | 35        |
| Jednorázové heslo doručované přes nezávislý kanál.....                                | 35        |
| <b>Biometrika</b> .....   | <b>36</b> |
| <b>Shamirův algoritmus</b> .....  | <b>36</b> |

## Kapitola 2

|  |           |
|--|-----------|
| <b>Prostředky pro bezpečné ukládání aktiv</b>                                | <b>37</b> |
| <b>Uložení aktiv na disk</b> .....   | <b>37</b> |
| <b>Autentizační kalkulátory</b> .....  | <b>37</b> |
| <b>Hardwarové klíče</b> .....  | <b>38</b> |
| Čipové karty.....  | 39        |
| Mini klíč ( <i>USB token</i> ).....  | <b>48</b> |
| HSM ( <i>Host Security Modul</i> ).....                                      | <b>49</b> |
| <b>Prostředky pro bezpečné vytváření elektronického podpisu (SSCD)</b> ..... | <b>50</b> |
| <b>Porovnání jednotlivých prostředků</b> .....                               | <b>51</b> |

## Kapitola 3

|   |           |
|---|-----------|
| <b>Certifikáty a certifikační autority</b>                      | <b>53</b> |
| <b>Jaká je obrana?</b>  | <b>54</b> |
| Vlastní Bohumila odpovídající soukromý klíč?                    | 54        |
| Důkaz o vlastnictví soukromého klíče                            | 55        |
| Generovala Bohumila svá párová data na bezpečném zařízení?      | 55        |
| Závěr   | 56        |
| <b>Certifikace veřejného klíče</b>                              | <b>56</b> |
| Achillova pata certifikátu                                      | 58        |
| <b>Certifikát</b>   | <b>58</b> |
| Verze certifikátu   | 60        |
| Pořadové číslo certifikátu                                      | 60        |
| Algoritmus podpisu  | 60        |
| Platnost  | 60        |
| Položky Vydavatel a Předmět                                     | 60        |
| Veřejný klíč  | 63        |
| <b>Rozšíření certifikátu</b>                                    | <b>64</b> |
| <b>Průvodce některými rozšířeními certifikátu</b>               | <b>66</b> |
| Identifikátor klíče předmětu a Identifikátor klíče úřadu        | 66        |
| Platnost soukromého klíče                                       | 67        |
| Použití klíče   | 68        |
| Rozšířené použití klíče   | 69        |
| Alternativní jméno předmětu                                     | 69        |
| Certifikační politiky (certifikační zásady)                     | 70        |
| Mapování zásad  | 71        |
| Omezení využívání certifikátu (Constrains)                      | 71        |
| Distribuční místa seznamu odvolaných certifikátů                | 72        |
| Subject directory attributes                                    | 72        |
| Přístup k informacím úřadu (Authority Information Access – AIA) | 72        |
| Název šablony certifikátu                                       | 73        |
| Biometrické informace   | 73        |
| Qualified Certificate Statements                                | 73        |
| <b>Kvalifikované certifikáty</b>                                | <b>73</b> |
| <b>Životní cyklus certifikátu</b>                               | <b>74</b> |
| <b>Certifikát ve Windows</b>                                    | <b>75</b> |
| <b>Certifikační a registrační autority</b>                      | <b>76</b> |

## Kapitola 4

|   |           |
|---|-----------|
| <b>Žádost o certifikát</b>                  | <b>79</b> |
| <b>Údaje v žádosti o certifikát</b>         | <b>79</b> |
| <b>Důkaz o vlastnictví soukromého klíče</b> | <b>80</b> |
| Důkaz založený na digitálním podpisu        | 81        |
| Verifikaci důkazu provedla RA jinou cestou  | 81        |
| Důkaz pro šifrovací klíče                   | 81        |
| Důkaz na základě výměny klíčů               | 81        |
| <b>Kořenový certifikát</b>                  | <b>82</b> |

|  |           |
|--|-----------|
| <b>PEM</b> .....                                 | <b>83</b> |
| <b>PKCS#10</b> .....                             | <b>83</b> |
| <b>CRMF</b> .....                                | <b>84</b> |
| <b>SPK</b> .....                                 | <b>85</b> |
| <b>Žádosti generované webovou stránkou</b> ..... | <b>85</b> |
| <b>CMC</b> .....                                 | <b>86</b> |

## Kapitola 5

|   |           |
|---|-----------|
| <b>Odvolávání certifikátu</b> .....                   | <b>87</b> |
| <b>Žádost o odvolání certifikátu</b> .....            | <b>89</b> |
| <b>CRL</b> .....                                      | <b>90</b> |
| Rozšíření CRL .....                                   | 91        |
| Rozšíření položky CRL .....                           | 92        |
| <b>On Line zjišťování statusu certifikátu</b> .....   | <b>93</b> |
| <b>Platnost certifikátu k uvedenému datu</b> .....    | <b>94</b> |
| <b>Vzdálené ověřování platnosti certifikátu</b> ..... | <b>94</b> |

## Kapitola 6

|   |            |
|---|------------|
| <b>Certifikační cesta a důvěryhodné kotvy</b> .....         | <b>95</b>  |
| <b>Podvržení kořenového certifikátu</b> .....               | <b>96</b>  |
| Ověření certifikátu Bohumily .....                          | 97         |
| <b>Strom certifikačních autorit</b> .....                   | <b>97</b>  |
| Řetězec certifikátů .....                                   | 98         |
| <b>Vzájemná důvěra mezi certifikačními autoritami</b> ..... | <b>100</b> |
| Křížová certifikace .....                                   | 100        |
| Most certifikačních autorit ( <i>Bridge</i> ) .....         | <b>102</b> |
| CTL ( <i>Certificate Trusted List</i> ) .....               | <b>103</b> |
| <b>Distribuce veřejných důvěryhodných kotev</b> .....       | <b>104</b> |
| WebTrust .....  | 105        |

## Kapitola 7

|   |            |
|---|------------|
| <b>Ověřování platnosti certifikátu a poznámka k ověřování digitálního podpisu</b> ..... | <b>107</b> |
| <b>Ověřování cesty začíná od důvěryhodné kotvy!</b> .....                               | <b>107</b> |
| <b>Ověřujeme certifikační cestu</b> .....   | <b>108</b> |
| <b>Byl certifikát odvolán?</b> .....  | <b>109</b> |
| <b>Microsoft</b> .....  | <b>110</b> |
| Sestavování certifikační cesty .....  | 110        |
| Certifikační politiky, nebo certifikační šablony? .....                                 | 112        |
| <b>Ověřování podpisu</b> .....  | <b>112</b> |

## Kapitola 8

|  |            |
|--|------------|
| <b>Obnovování certifikátů</b>                        | <b>115</b> |
| Renew, nebo Rekey? .....                             | 116        |
| Vydání dalšího certifikátu koncového uživatele ..... | 117        |
| Obnovení certifikátu CA .....                        | 118        |
| CRL .....  | 119        |
| Doba platnosti certifikátu .....                     | 119        |

## Kapitola 9

|                                   |            |
|-----------------------------------|------------|
| <b>PKI nejsou jen certifikáty</b> | <b>121</b> |
| Certifikát veřejného klíče .....  | 121        |
| Atributový certifikát .....       | 122        |
| Časová razítka .....              | 123        |
| DV-certifikát (DVC) .....         | 124        |

## Kapitola 10

|   |            |
|---|------------|
| <b>Kvalifikované certifikáty a zaručené podpisy</b>                                       | <b>125</b> |
| Směrnice Evropského parlamentu a Rady 1999/93/EC .....                                    | 127        |
| Zákon č. 227/2000 Sb. ....  | 132        |
| Vyhláška č. 378/2006 Sb. ....   | 135        |
| ETSI .....  | 135        |
| RFC-3739 .....  | 135        |
| Alternativní jméno předmětu .....   | 136        |
| Certifikační politiky .....   | 136        |
| Použití klíče .....   | 136        |
| Subject directory attributes .....  | 137        |
| Biometrické informace ( <i>Biometric Information</i> ) .....                              | 137        |
| Prohlášení o kvalifikovaném certifikátu ( <i>Qualified Certificate Statements</i> ) ..... | 137        |

## Kapitola 11

|  |            |
|--|------------|
| <b>Naše první certifikační autorita</b>                | <b>139</b> |
| <b>CA na bázi OpenSSL</b> .....                        | <b>139</b> |
| Budujeme certifikační autoritu .....                   | 141        |
| <b>Microsoft CA</b> .....                              | <b>149</b> |
| Kořenová stand-alone MSCA .....                        | 151        |
| CA vydávající uživatelské certifikáty .....            | 151        |
| CAPolicy.inf .....                                     | 155        |
| Automatické schvalování vs. registrační autorita ..... | 158        |
| Na co se hodí a na co nehodí Stand-alone CA .....      | 159        |

## Kapitola 12

|                                    |            |
|------------------------------------|------------|
| <b>Nástroje pro sledování sítě</b> | <b>161</b> |
| <b>Packet driver</b> .....         | <b>162</b> |
| <b>Promiskuitní mód</b> .....      | <b>162</b> |
| <b>Program Wireshark</b> .....     | <b>163</b> |
| Začínáme s Wiresharkem .....       | 163        |
| Filtry .....                       | 164        |
| Colorig rules .....                | 168        |
| Follow TCP stream .....            | 168        |
| Statistiky .....                   | 169        |
| Tisk a Export .....                | 169        |
| Další utility .....                | 170        |
| Domácí cvičení .....               | 171        |

## Kapitola 13

|  |            |
|--|------------|
| <b>ASN.1, BER, DER, UTF-8 a Base64</b>           | <b>173</b> |
| <b>ASN.1</b> .....                               | <b>175</b> |
| <b>BER kódování</b> .....                        | <b>176</b> |
| Pole typu dat .....                              | 176        |
| Pole délka dat .....                             | 179        |
| Pole data .....                                  | 180        |
| Příklady .....                                   | 180        |
| Jak je v BER-kódování kódován prázdný typ? ..... | 181        |
| Jak je kódován typ BOOLEAN? .....                | 181        |
| Jak je to s kódováním typu INTEGER? .....        | 181        |
| Výčet .....                                      | 182        |
| Typy SEQUENCE, SEQUENCE OF, SET a SET OF .....   | 182        |
| Čas .....  | 182        |
| Bit string .....                                 | 183        |
| Identifikace objektů .....                       | 183        |
| Kódování identifikace objektů v BER .....        | 185        |
| Odvozené typy .....                              | 187        |
| CHOICE .....                                     | 190        |
| ANY .....  | 191        |
| <b>Kódování UTF-8</b> .....                      | <b>191</b> |
| <b>Base64</b> .....                              | <b>197</b> |

## Kapitola 14

|   |            |
|---|------------|
| <b>Žádost o vydání certifikátu pod lupou</b>        | <b>199</b> |
| <b>Žádost ve tvaru kořenového certifikátu</b> ..... | <b>199</b> |
| <b>PKCS#10</b> .....                                | <b>200</b> |
| Atributy v PKCS#10 .....                            | 201        |
| Žádost o certifikát v prostředí Microsoft .....     | 202        |

|  |            |
|--|------------|
| <b>CRMF .....</b>                        | <b>204</b> |
| Žádost .....                             | 205        |
| Důkaz vlastnictví soukromého klíče ..... | 207        |
| Dodatečné registrační informace .....    | 208        |

## Kapitola 15

### **Certifikát pod lupou 209**

|   |            |
|---|------------|
| <b>Struktura certifikátu .....</b>                      | <b>209</b> |
| Algoritmus podpisu ( <i>signatureAlgorithm</i> ) .....  | 210        |
| Podpis certifikátu ( <i>signatureValue</i> ) .....      | 211        |
| <b>TBSCertificate .....</b>                             | <b>212</b> |
| Základní položky certifikátu .....                      | 212        |
| Jedinečná jména (Name) .....                            | 214        |
| Položky issuer a subject .....                          | 217        |
| Certifikovaný veřejný klíč (SubjectPublicKeyInfo) ..... | 219        |
| Rozšíření certifikátu (extensions) .....                | 220        |
| Microsoft .....   | 249        |

## Kapitola 16

### **Odvolání certifikátu pod lupou 257**

|  |            |
|--|------------|
| <b>CRL .....</b>                             | <b>257</b> |
| Rozšíření CRL („rozšíření celého CRL“) ..... | 260        |
| Rozšíření položek CRL .....                  | 263        |
| <b>OCSP .....</b>                            | <b>265</b> |
| OCSP dotaz .....                             | 266        |
| OCSP odpověď .....                           | 269        |
| Transportní protokol .....                   | 274        |

## Kapitola 17

### **CMP a CMC 275**

|                                       |            |
|---------------------------------------|------------|
| <b>Protokol CMP .....</b>             | <b>275</b> |
| Formát CMP zprávy .....               | 276        |
| Žádost o certifikát .....             | 279        |
| Odpověď na žádosti o certifikát ..... | 280        |
| Obnovení klíčů .....                  | 281        |
| Odvolání certifikátu .....            | 281        |
| Vydání nového certifikátu CA .....    | 282        |
| Potvrzení .....                       | 282        |
| Další zprávy .....                    | 282        |
| Přenos CMP zpráv .....                | 283        |
| <b>Protokol CMC .....</b>             | <b>283</b> |
| Formát CMC zpráv .....                | 284        |
| Atributy .....                        | 288        |
| Příklad (Windows 2003) .....          | 294        |



## Kapitola 18

|   |            |
|---|------------|
| <b>Budujeme certifikační autoritu</b>         | <b>297</b> |
| <b>Bezpečnostní dokumentace</b>               | <b>298</b> |
| Analýza rizik                                 | 299        |
| Od TCSEC a ITSEC k ISO/IEC 15408              | 301        |
| FIPS  | 306        |
| Řízení bezpečnosti firmy/organizace           | 306        |
| <b>Dokumentace certifikační autority</b>      | <b>308</b> |
| <b>Testovací CA</b>                           | <b>310</b> |
| <b>Veřejné CA</b>                             | <b>310</b> |
| Důvěryhodné kotvy                             | 311        |
| <b>Enterprise CA – Windows Server 2008 R2</b> | <b>312</b> |
| Navrhujeme strukturu CA                       | 312        |
| Administrace MSCA                             | 313        |
| Certifikační politika Enterprise CA           | 314        |
| Separace rolí a oprávnění                     | 316        |
| Způsoby vydávání certifikátů                  | 317        |
| Záloha a obnova MSCA                          | 320        |
| Volitelné komponenty ADCS                     | 321        |
| Závěr   | 322        |

## Kapitola 19

|  |            |
|--|------------|
| <b>Atributové certifikáty</b>  | <b>323</b> |
| <b>Atributy v certifikátu veřejného klíče</b>                          | <b>323</b> |
| <b>Atributové certifikáty</b>  | <b>325</b> |
| <b>Specifikace držitele atributového certifikátu</b>                   | <b>326</b> |
| Mohou fungovat atributové certifikáty bez certifikátu veřejného klíče? | 327        |
| <b>Struktura atributového certifikátu</b>                              | <b>328</b> |
| Vnitřek atributového certifikátu                                       | 329        |
| <b>Rozšíření atributového certifikátu</b>                              | <b>332</b> |
| Audit Identity   | 332        |
| AC Targeting   | 332        |
| Authority Key Identifier   | 332        |
| Authority Information Access   | 333        |
| CRL Distribution Points  | 333        |
| No Revocation Available  | 333        |
| <b>Atributy</b>  | <b>333</b> |
| Service Authentication Information                                     | 333        |
| Access Identity  | 333        |
| Charging Identity  | 334        |
| Group  | 334        |
| Role   | 334        |
| Clearance  | 334        |
| <b>Šifrované atributy</b>  | <b>334</b> |
| <b>Certifikát AA</b>   | <b>334</b> |

|   |            |
|---|------------|
| <b>Vydávání atributového certifikátu</b> .....            | <b>334</b> |
| Uživatel sám žádá o vydání atributového certifikátu ..... | 335        |
| Smluvní odběratel (Subscriber) .....                      | 335        |
| Na požadavek .....  | 336        |
| <b>Odvolávání atributových certifikátů</b> .....          | <b>336</b> |
| ACRL .....  | 337        |
| On line zjišťování revokační informace .....              | 337        |
| <b>Verifikace atributového certifikátu</b> .....          | <b>337</b> |
| <b>Atributová autorita</b> .....                          | <b>339</b> |
| Akviziční služba .....                                    | 340        |
| Služba pro generování AC .....                            | 341        |
| Služba registrace atributů .....                          | 341        |
| Služba pro šíření AC .....                                | 341        |
| Služba odvolání atributových certifikátů .....            | 341        |
| Služba pro poskytování revokačního statusu .....          | 341        |
| <b>Dokumentace</b> .....                                  | <b>342</b> |
| Prováděcí (organizační) dokumentace .....                 | 342        |
| Bezpečnostní dokumentace .....                            | 342        |
| <b>Další technologie přiřazování atributů</b> .....       | <b>342</b> |

## Kapitola 20

|   |            |
|---|------------|
| <b>Časová razítka</b> .....                               | <b>345</b> |
| <b>Co to je čas?</b> .....                                | <b>346</b> |
| Kalendář .....  | 347        |
| Délka dne a sekunda .....                                 | 347        |
| Přestupné vteřiny, UTC .....                              | 348        |
| Časové zóny, letní čas .....                              | 348        |
| Počítačový čas .....                                      | 349        |
| Zdroje času .....   | 349        |
| Poskytovatelé času .....                                  | 349        |
| Synchronizace času přes síť .....                         | 350        |
| Zaručený čas .....  | 352        |
| <b>TSA</b> .....  | <b>352</b> |
| <b>Protokol pro vydávání časových razítek (TSP)</b> ..... | <b>354</b> |
| Transportní protokoly .....                               | 355        |
| <b>Žádost o časové razítko</b> .....                      | <b>356</b> |
| <b>Odpoověď TSA</b> .....                                 | <b>357</b> |
| <b>Časové razítko</b> .....                               | <b>357</b> |
| CMS zpráva SignedData .....                               | 357        |
| Obsah položek zprávy CMS Signed-data .....                | 358        |
| TSTInfo .....   | 360        |
| <b>Ověřování časového razítka</b> .....                   | <b>361</b> |
| <b>Platnost časového razítka</b> .....                    | <b>362</b> |
| <b>Co časové razítko není</b> .....                       | <b>363</b> |
| <b>Provázané otisky</b> .....                             | <b>364</b> |
| Lineární schéma .....                                     | 364        |

|   |     |
|---|-----|
| Stromové schéma .....                         | 366 |
| Zkratka .....                                 | 367 |
| Kombinace redukovaného stromu a zkratek ..... | 368 |

## Kapitola 21

|  |            |
|--|------------|
| <b>E-notary</b> .....                                    | <b>369</b> |
| <b>Důvěryhodný archiv Rakouské notářské komory</b> ..... | <b>370</b> |
| <b>Komerční organizace</b> .....                         | <b>370</b> |
| <b>Protokol DVCSP</b> .....                              | <b>371</b> |
| <b>SCVP</b> .....  | <b>372</b> |

## Kapitola 22

|  |            |
|--|------------|
| <b>Protokol TLS</b> .....                                | <b>381</b> |
| <b>TLS relace a TLS spojení</b> .....                    | <b>384</b> |
| <b>Autentizace</b> .....                                 | <b>386</b> |
| Autentizace serveru .....                                | 386        |
| Autentizace klienta .....                                | 387        |
| <b>Předběžné a hlavní sdílené tajemství</b> .....        | <b>387</b> |
| <b>Record Layer Protocol (RLP)</b> .....                 | <b>388</b> |
| <b>Alert protocol</b> .....                              | <b>390</b> |
| <b>Change Cipher Specification Protocol (CCSP)</b> ..... | <b>390</b> |
| <b>Handshake Protocol (HP)</b> .....                     | <b>391</b> |
| Zřízení nové relace .....                                | 392        |
| Obnovení relace .....                                    | 393        |
| Zpráva ClientHello .....                                 | 394        |
| Zpráva ServerHello .....                                 | 396        |
| Zpráva Certificate .....                                 | 397        |
| Zpráva CertificateRequest .....                          | 397        |
| Zpráva ServerHelloDone .....                             | 398        |
| Zpráva ClientKeyExchange .....                           | 399        |
| Zpráva CertificateVerify .....                           | 400        |
| Zpráva Finished .....                                    | 400        |
| Zpráva ServerKeyExchange .....                           | 400        |
| Zpráva HelloRequest .....                                | 400        |
| <b>Zpětná kompatibilita</b> .....                        | <b>401</b> |
| <b>HTTP</b> .....  | <b>401</b> |
| HTTP dotaz .....   | 402        |
| HTTP odpověď .....                                       | 404        |
| Některé další hlavičky .....                             | 405        |
| Proxy .....  | 407        |
| Brána .....  | 408        |
| Tunel .....  | 409        |
| <b>Bouncer (BNC)</b> .....                               | <b>410</b> |
| <b>HTTPS</b> .....                                       | <b>411</b> |
| Protocol upgrade .....                                   | 413        |

## Kapitola 23

|  |            |
|--|------------|
| <b>PKCS#7 a CMS</b>                        | <b>415</b> |
| <b>Položka contentType</b> .....           | <b>417</b> |
| <b>Typ zprávy Data</b> .....               | <b>418</b> |
| <b>Typ zprávy SignedData</b> .....         | <b>418</b> |
| Podpis (SignerInfos) .....                 | 420        |
| Útoky na zprávu SignedData .....           | 422        |
| Podepsované a nepodepsované atributy ..... | 423        |
| Paralelní a sériový podpis .....           | 426        |
| Ověřování digitálního podpisu .....        | 427        |
| Příklad podepsané zprávy .....             | 429        |
| Export certifikátu .....                   | 433        |
| <b>Typ zprávy EnvelopedData</b> .....      | <b>434</b> |
| Položka RecipientInfos .....               | 435        |
| <b>Typ zprávy DigestData</b> .....         | <b>438</b> |
| <b>Typ zprávy EncryptedData</b> .....      | <b>438</b> |
| <b>Typ zprávy AuthenticatedData</b> .....  | <b>438</b> |

## Kapitola 24

|  |            |
|--|------------|
| <b>Bezpečná pošta</b>                      | <b>441</b> |
| <b>Poštovní transport</b> .....            | <b>444</b> |
| SMTP a ESMTP .....                         | 444        |
| POP3 .....                                 | 450        |
| IMAP4 .....                                | 454        |
| <b>Formát poštovní zprávy</b> .....        | <b>454</b> |
| E-mailová adresa .....                     | 455        |
| <b>MIME</b> .....                          | <b>457</b> |
| Hlavičky MIME .....                        | 458        |
| Hlavička Mime-Version .....                | 458        |
| Hlavička Content-Transfer-Encoding .....   | 458        |
| Hlavička Content-Type .....                | 459        |
| <b>S/MIME</b> .....                        | <b>462</b> |
| CMS a S/MIME .....                         | 465        |
| Certifikáty a CRL využívané v S/MIME ..... | 470        |
| MIME obálka .....                          | 470        |
| Příklad digitálně podepsané zprávy .....   | 473        |
| Příklad šifrované zprávy .....             | 476        |
| Jaká nebezpečí číhají na adresáta .....    | 480        |
| <b>Rozšířeně S/MIME (ESS)</b> .....        | <b>481</b> |

## Kapitola 25

|                                    |            |
|------------------------------------|------------|
| <b>Dlouhodobý digitální podpis</b> | <b>487</b> |
| <b>CMS</b> .....                   | <b>488</b> |

|   |            |
|---|------------|
| <b>LTES</b> .....   | <b>488</b> |
| Basic Electronic Signature (BES).....                         | 489        |
| Explicit Policy Electronic Signatures (EPES).....             | 489        |
| Electronic Signature with Time (ES-T).....                    | 490        |
| ES with Complete validation data reference (ES-C).....        | 491        |
| Extended electronic signature (ES-X).....                     | 492        |
| Archival electronic signature (ES-A).....                     | 493        |
| <b>Obnovování digitálního podpisu (signature renew)</b> ..... | <b>494</b> |
| <b>Nové atributy digitálního podpisu</b> .....                | <b>494</b> |
| Other Signing Certificate .....                               | 496        |
| Commitment Type Indication .....                              | 497        |
| Signer Location .....   | 498        |
| Signer Attributes .....                                       | 498        |
| Content Time Stamp .....                                      | 499        |
| Signature Policy Identifier .....                             | 499        |
| Signature Time Stamp.....                                     | 501        |
| Complete Certificate References.....                          | 501        |
| Complete Revocation References.....                           | 501        |
| Attribute Certificate References.....                         | 502        |
| Attribute Revocation References.....                          | 502        |
| Certificate Values.....                                       | 503        |
| Revocation Values.....  | 503        |
| ES-C Time Stamp.....  | 503        |
| ES-C Time Stamped Certs and CRLs References .....             | 504        |
| Archive Time Stamp.....                                       | 504        |
| <b>Politika digitálního podpisu</b> .....                     | <b>504</b> |
| Pravidla pro vytváření a ověřování podpisu .....              | 506        |

## Kapitola 26

### Dlouhodobá archivace nejenom digitálně podepsaných dokumentů

|  |            |
|--|------------|
| <b>Doba archivace dokumentů</b> .....              | <b>512</b> |
| Krátkodobá archivace .....                         | 513        |
| Střednědobá archivace.....                         | 514        |
| Dlouhodobá a trvalá archivace .....                | 514        |
| <b>Problém formátu dat</b> .....                   | <b>514</b> |
| <b>Archivy</b> .....                               | <b>515</b> |
| <b>OAIS</b> .....                                  | <b>517</b> |
| <b>Důvěryhodná archivační autorita (TAA)</b> ..... | <b>519</b> |
| Přístup k archivovaným informacím.....             | 519        |
| LTANS.....   | 520        |
| ERS .....  | 520        |
| <b>Závěr</b> .....                                 | <b>522</b> |

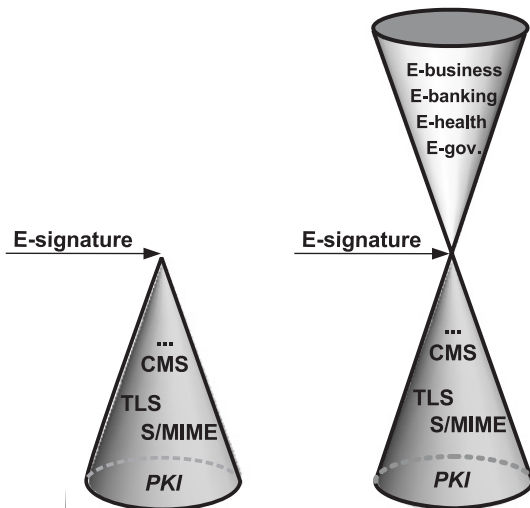
## Kapitola 27

|  |            |
|--|------------|
| <b>Budujeme PKI, TSA a důvěryhodné archivy</b>   | <b>523</b> |
| <b>Identita koncového uživatele PKI</b>          | <b>524</b> |
| Identifikace zákazníků                           | 524        |
| Identifikace zaměstnanců a partnerů v aplikacích | 526        |
| Identifikace systémů a aplikací                  | 527        |
| <b>Mapujeme využití PKI ve firmě/organizaci</b>  | <b>527</b> |
| Klienti/občané                                   | 527        |
| Zaměstnanci/partneři                             | 528        |
| Interní systémy a aplikace                       | 528        |
| Veřejné aplikace                                 | 529        |
| Vyhodnocení                                      | 529        |
| <b>Navrhujeme certifikační autority</b>          | <b>531</b> |
| Náklady na implementaci PKI v aplikacích         | 532        |
| Náklady na čipové karty                          | 533        |
| Náklady na projekt a dokumentaci                 | 534        |
| <b>Budujeme TSA</b>                              | <b>535</b> |
| Veřejná TSA                                      | 535        |
| Vlastní TSA                                      | 535        |
| <b>Volíme odpovídající důvěryhodný archiv</b>    | <b>535</b> |
| <b>Rejstřík</b>                                  | <b>537</b> |

# Úvod

Je to již několik let, kdy jsme byli naposledy v Paříži. I tenkrát jsme si vzpomněli na Petera Sylvestera. A hned nás napadlo, že se u něj opět zastavíme. P. Sylvester je spoluautor legendárního standardu-nestandardu RFC-3029 „*Internet X.509 Public Key Infrastructure: Data Validation and Certification Server Protocols*“, který už tehdy mnozí kritizovali, ale přitom nikdo nedokázal vymyslet nic lepšího. Což bohužel víceméně platí dodnes.

I přes stávku pařížských dopraváků jsme dorazili včas a začali naši diskusi. Uprostřed diskuse Peter namaloval kužel (obr. ú.1 vlevo), který komentoval slovy, že PKI si můžeme představit jako podstavu kužele, nad níž je vybudována řada protokolů (S/MIME, TLS, CMS, IPsec, EAP-TLS...). Na vrcholu kužele je pak elektronický podpis.



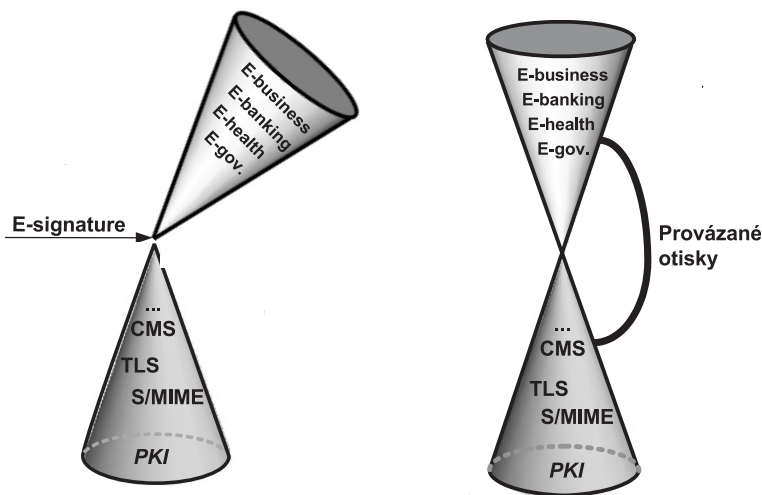
**Obrázek ú.1:** Sylvesterovy kužely

Vedle namaloval též kužel, ale na jeho vrchol přidal ještě další kužel otočený vrcholem dolů (obr. ú.1 vpravo). A pokračoval tvrzením, že na tom jediném elektronickém podpisu stojí všechny nejrůznější aplikace jako E-government, E-health, E-banking, E-business, E-procurement a kdoví jaké další „E-“.

„No a nyní si stačí představit“, zaníceně pokračoval, „že někdo jen zpochybní ten elektronický podpis.“ A už maloval další kužely (obr. ú.2). Hned bylo vidět, jak se celý ten humbuk „E-“ kácí jako krabička sirek. Zdůrazňoval, že je třeba hledat i jiné algoritmy a postupy, které ty užitečné aplikace podepřou, a jako rozumný mu připadal systém provázaných otisků (viz kapitola 20).

Nás tyto Sylvesterovy kužely přímo nadchly. Avšak u mnohých kolegů jsme s nimi nepochodili. Připadalo jim to totiž nadnesené.

Cílem této publikace je začít zkoumat Sylvesterovy kužely od spodní podstavy, kterou je PKI. Dále si objasníme zejména protokoly popsané ve spodním kuželu a elektronický podpis. Pochopitelně že kužely rovněž pořádně zatřepeme, když si položíme otázku o platnosti elektronického podpisu po vypršení platnosti certifikátu určeného k ověření tohoto podpisu. A nebojte se, i na provázané otisky dojde.



**Obrázek ú.2:** Provázané otisky možná pomohou udržet Sylvesterovy kužely ve správné poloze nad sebou

## Jak tuto knihu číst

Kniha je určena jak pro začátečníky v oblasti PKI, tak i pro odborníky, kteří se potřebují dozvědět řadu detailů. Aby začátečníci nebyli zahlceni, je prvních deset kapitol napsáno populární formou tak, aby byly dobře srozumitelné i pro ně. Těchto prvních 10 kapitol objasňuje princip certifikátu veřejného klíče a jeho životní cyklus.

Kapitoly 11, „Má první certifikační autorita“, a 12, „Wireshark“, jsou určeny štouralům, kteří si chtějí pohrát s jednoduchou certifikační autoritou a připravit se na pitvání nejenom certifikátu po jednotlivých bitech.

Přelomovou kapitolou je kapitola 13, „ASN.1, BER, DER, UTF-8 a Base64“, zabývající se jazykem ASN.1 sloužícím k definování jednotlivých datových struktur. Dále se zabývá kódováním BER a DER těchto struktur pro počítačovou komunikaci. Pokud se laskavý čtenář seznámí s jazykem ASN.1 a kódováním BER a DER (tj. s obsahem této kapitoly), pak bez jakýchkoliv problémů může rozebírat dále popisované datové struktury po jednotlivých bitech. Stane se tak pokročilým čtenářem této publikace.

Kapitoly 14, „Žádost o vydání certifikátu pod lupou“, 15, „Certifikát pod lupou“, 16, „Žádost a odvolání certifikátu pod lupou“, a 17, „CMP a CMC“, jsou určeny pro pokročilé čtenáře. Mají obdobný obsah jako kapitoly 1–10, ale zaměřují se na detailní popis jednotlivých datových struktur.



Zbývající část publikace pak obsahuje tematicky zaměřené kapitoly (Atributové certifikáty, Časová razítka, Bezpečný web, Bezpečná pošta, Dlouhodobý digitální podpis a Dlouhodobá archivace). Tyto kapitoly jsou určeny jak začátečníkům, tak i pokročilým čtenářům. Začátečníci jen přeskochí popisy jednotlivých datových struktur.

Kapitola 27, „Budujeme PKI, TSA a důvěryhodné archivy“, je pak závěrem celé publikace.

## Poděkování

Chtěli bychom poděkovat všem, kteří nám zapůjčili nejrůznější zařízení, abychom mohli připravit jednotlivé příklady. Dále bychom chtěli poděkovat Ludku Raškovi za podnětnou odbornou korekturu a Michalu Hojsíkovi, který rukopis pozorně přečetl a opravil mnohé chyby.