

Obsah

Úvod	17
Jak tuto knihu číst	18
Poděkování	19

Kapitola 1

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

Kapitola 2

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

Kapitola 3

Certifikáty a certifikační autority	53
Jaká je obrana?	54
Vlastní Bohumila odpovídající soukromý klíč?	54
Důkaz o vlastnictví soukromého klíče	55
Generovala Bohumila svá párová data na bezpečném zařízení?	55
Závěr	56
Certifikace veřejného klíče	56
Achillova pata certifikátu	58
Certifikát	58
Verze certifikátu	60
Pořadové číslo certifikátu	60
Algoritmus podpisu	60
Platnost	60
Položky Vydavatel a Předmět	60
Veřejný klíč	63
Rozšíření certifikátu	64
Průvodce některými rozšířeními certifikátu	66
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	70
Omezení využívání certifikátu (Constraints)	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
Kvalifikované certifikáty	73
Životní cyklus certifikátu	74
Certifikát ve Windows	75
Certifikační a registrační autority	76

Kapitola 4

Žádost o certifikát	79
Údaje v žádosti o certifikát	79
Důkaz o vlastnictví soukromého klíče	80
Důkaz založený na digitálním podpisu	81
Verifikaci důkazu provedla RA jinou cestou	81

Důkaz pro šifrovací klíče81
Důkaz na základě výměny klíčů81
Kořenový certifikát82
Pozor! Není kořenový certifikát jako kořenový certifikát82
PEM83
PKCS#1083
CRMF84
SPK85
Žádosti generované webovou stránkou85
CMC86

Kapitola 5

Odvolávání certifikátu	87
Žádost o odvolání certifikátu89
CRL90
Rozšíření CRL91
Rozšíření položky CRL92
On Line zjišťování statusu certifikátu93
Platnost certifikátu k uvedenému datu94
Vzdálené ověřování platnosti certifikátu94

Kapitola 6

Certifikační cesta a důvěryhodné kotvy	95
Podvržení kořenového certifikátu96
Ověření certifikátu Bohumily97
Strom certifikačních autorit97
Řetězec certifikátů98
Vzájemná důvěra mezi certifikačními autoritami100
Křížová certifikace100
Most certifikačních autorit (Bridge)102
CTL (Certificate Trusted List)103
Distribuce veřejných důvěryhodných kotev104
WebTrust105

Kapitola 7

Ověřování platnosti certifikátu a poznámka k ověřování digitálního podpisu	107
Ověřování cesty začíná od důvěryhodné kotvy!107
Ověřujeme certifikační cestu108
Byl certifikát odvolán?109
Microsoft110

Sestavování certifikační cesty	110
Certifikační politiky nebo certifikační šablony?	112
Ověřování podpisu	112

Kapitola 8

Obnovování certifikátů	115
Renew nebo Rekey?	116
Vydání dalšího certifikátu koncového uživatele	117
Obnovení certifikátu CA	118
CRL	119
Doba platnosti certifikátu	119

Kapitola 9

PKI nejsou jen certifikáty	121
Certifikát veřejného klíče	121
Atributový certifikát	122
Časová razítka	123
DV-certifikát (DVC)	124

Kapitola 10

Kvalifikované certifikáty a zaručené podpisy	125
Směrnice Evropského parlamentu a Rady 1999/93/EC	127
Zákon č. 227/2000 Sb.	132
Vyhláška ÚOOÚ 366/2001 Sb.	135
RFC-3739	136
Alternativní jméno předmětu	137
Certifikační politiky	137
Použití klíče	137
Subject directory attributes	137
Biometrické informace (Biometric Information)	138
Prohlášení o kvalifikovaném certifikátu (Qualified Certificate Statements)	138

Kapitola 11

Má první certifikační autorita	139
CA na bázi OpenSSL	139
Budujeme certifikační autoritu	141
Microsoft CA	149
Kořenová stand-alone MSCA	150
CA vydávající uživatelské certifikáty	150

Kapitola 12

Ethereal	157
K čemu Ethereal slouží?	157
Packet driver, promiskuitní mód	157
WinPCapp	158
Začínáme s Etherealem	159
Filtry	161
Colorig rules	163
Follow TCP stream	164
Statistiky	164
Tisk a Export	166
Příkazová řádka	167
Sniffer	167
Závěr	167

Kapitola 13

ASN.1, BER, DER, UTF-8 a Base64	169
ASN.1	171
BER kódování	172
Pole typu dat	172
Pole délka dat	175
Pole data	176
Příklady	176
Jak je v BER-kódování kódován prázdný typ?	177
Jak je kódován typ BOOLEAN?	177
Jak je to s kódováním typu INTEGER?	177
Výčet	178
Typy SEQUENCE, SEQUENCE OF, SET a SET OF	178
Čas	178
Bit string	179
Identifikace objektů	179
Kódování identifikace objektů v BER	181
Odvozené typy	183
CHOICE	186
ANY	187
Kódování UTF-8	187
Base64	193

Kapitola 14

Žádost o vydání certifikátu pod lupou	195
Žádost ve tvaru kořenového certifikátu	195

PKCS#10	196
Atributy v PKCS#10	197
Žádost o certifikát v prostředí Microsoft	198
CRMF	200
Žádost	201
Důkaz vlastnictví soukromého klíče	203
Dodatečné registrační informace	204

Kapitola 15

Certifikát pod lupou	205
Struktura certifikátu	205
Algoritmus podpisu (signatureAlgorithm)	206
Podpis certifikátu (signatureValue)	207
TBSCertificate	207
Základní položky certifikátu	208
Jedinečná jména (Name)	210
Položky issuer a subject	213
Certifikovaný veřejný klíč (SubjectPublicKeyInfo)	215
Rozšíření certifikátu (extensions)	216
Microsoft	245

Kapitola 16

Odvolání certifikátu pod lupou	253
CRL	253
Rozšíření CRL („rozšíření celého CRL“)	256
Rozšíření položek CRL	259
OCSP	262
OCSP dotaz	262
OCSP odpověď	265
Transportní protokol	270

Kapitola 17

CMP a CMC	271
Protokol CMP	271
Formát CMP zprávy	272
Žádost o certifikát	275
Odpověď na žádosti o certifikát	276
Obnovení klíčů	277
Odvolání certifikátu	277
Vydání nového certifikátu CA	278
Potvrzení	278
Další zprávy	278
Přenos CMP zpráv	279

Protokol CMC	279
Formát CMC zpráv	280
Atributy	284
Příklad (Windows 2003)	289

Kapitola 18

Budujeme certifikační autoritu	293
Bezpečnostní dokumentace	294
Analýza rizik	295
Od TCSEC a ITSEC k ISO/IEC 15408	297
FIPS	302
Řízení bezpečnosti firmy/organizace	302
Dokumentace certifikační autority	304
Testovací CA	306
Veřejné CA	306
WebTrust	308
Enterprise MSCA 2003	308
Navrhujeme strukturu CA	308
Administrace MSCA	309
Certifikační politika MSCA	311
Separace rolí a oprávnění	311
Vydáváme certifikáty	313
Záloha a obnova MSCA	316
Závěr	316

Kapitola 19

Atributové certifikáty	317
Atributy v certifikátu veřejného klíče	317
Atributové certifikáty	319
Specifikace držitele atributového certifikátu	320
Mohou fungovat atributové certifikáty bez certifikátu veřejného klíče?	321
Struktura atributového certifikátu	322
Vnitřek atributového certifikátu	323
Rozšíření atributového certifikátu	326
Audit Identity	326
AC Targeting	326
Authority Key Identifier	326
Authority Information Access	327
CRL Distribution Points	327
No Revocation Available	327
Atributy	327
Service Authentication Information	327
Access Identity	327

Charging Identity	328
Group	328
Role	328
Clearance	328
Šifrované atributy	328
Certifikát AA	328
Vydávání atributového certifikátu	328
Uživatel sám žádá o vydání atributového certifikátu	329
Smluvní odběratel (Subscriber)	329
Na požadavek	330
Odvolávání atributových certifikátů	330
ACRL	331
On line zjišťování revokační informace	331
Verifikace atributového certifikátu	331
Atributová autorita	333
Akviziční služba	334
Služba pro generování AC	335
Služba registrace atributů	335
Služba pro šíření AC	335
Služba odvolání atributových certifikátů	335
Služba pro poskytování revokačního statusu	335
Dokumentace	336
Prováděcí (organizační) dokumentace	336
Bezpečnostní dokumentace	336
Další technologie přiřazování atributů	336

Kapitola 20

Časová razítka	339
Co to je čas?	340
Kalendář	341
Délka dne a sekunda	341
Přestupné vteřiny, UTC	342
Časové zóny, letní čas	342
Počítačový čas	343
Zdroje času	343
Poskytovatelé času	343
Synchronizace času přes síť	344
Zaručený čas	346
TSA	346
Protokol pro vydávání časových razítek (TSP)	348
Transportní protokoly	349
Žádost o časové razítko	350
Odpověď TSA	351

Časové razítko	351
CMS zpráva SignedData	351
Obsah položek zprávy CMS Signed-data	352
TSTInfo	354
Ověřování časového razítka	355
Platnost časového razítka	356
Co časové razítko není	357
Provázané otisky	358
Lineární schéma	358
Stromové schéma	360
Zkratka	361
Kombinace redukováného stromu a zkratek	362

Kapitola 21

E-notary	363
Důvěryhodný archiv Rakouské notářské komory	364
Komerční organizace	365
Protokol DVCSP	365
DVC-server	367
Žádost o DV-certifikát	368
Odpověď DVC-serveru	370
DV-certifikát	370
Sekvence TargetEtcChain	371
Chybová hláška DVC-serveru	372
Příklady	372

Kapitola 22

Protokol TLS	373
TLS relace a TLS spojení	376
Autentizace	378
Autentizace serveru	378
Autentizace klienta	379
Předběžné a hlavní sdílené tajemství	379
Record Layer Protocol (RLP)	380
Alert protocol	382
Change Cipher Specification Protocol (CCSP)	382
Handshake Protocol (HP)	383
Zřízení nové relace	384
Obnovení relace	385
Zpráva ClientHello	386
Zpráva ServerHello	388
Zpráva Certificate	389

Zpráva CertificateRequest	389
Zpráva ServerHelloDone	390
Zpráva ClientKeyExchange	390
Zpráva CertificateVerify	391
Zpráva Finished	392
Zpráva ServerKeyExchange	392
Zpráva HelloRequest	392
Zpětná kompatibilita	393
HTTP	393
HTTP dotaz	394
HTTP odpověď	396
Některé další hlavičky	397
Proxy	399
Brána	400
Tunel	401
Bouncer	402
HTTPS	403
Protocol upgrade	405

Kapitola 23

PKCS#7 a CMS	407
Položka contentType	409
Typ zprávy Data	410
Typ zprávy SignedData	410
Podpis (SignerInfos)	412
Útoky na zprávu SignedData	414
Podepisované a nepodepisované atributy	415
Paralelní a sériový podpis	418
Ověřování digitálního podpisu	419
Příklad podepsané zprávy	421
Export certifikátu	425
Typ zprávy EnvelopedData	426
Položka RecipientInfos	427
Typ zprávy DigestData	430
Typ zprávy EncryptedData	430
Typ zprávy AuthenticatedData	430

Kapitola 24

Bezpečná pošta	433
Poštovní transport	436
SMTP a ESMTP	436
POP3	442

IMAP4	446
Formát poštovní zprávy	446
E-mailová adresa	447
MIME	449
Hlavičky MIME	450
Hlavička Mime-Version	450
Hlavička Content-Transfer-Encoding	450
Hlavička Content-Type	451
S/MIME	454
CMS a S/MIME	457
Certifikáty a CRL využívané v S/MIME	462
MIME obálka	462
Příklad digitálně podepsané zprávy	465
Příklad šifrované zprávy	468
Jaká nebezpečí číhají na adresáta	472
Rozšířené S/MIME (ESS)	473

Kapitola 25

Dlouhodobý digitální podpis	479
CMS	480
LTES	480
Basic Electronic Signature (BES)	481
Explicit Policy Electronic Signatures (EPES)	481
Electronic Signature with Time (ES-T)	482
ES with Complete validation data reference (ES-C)	483
Extended electronic signature (ES-X)	484
Archival electronic signature (ES-A)	485
Obnovování digitálního podpisu (signature renew)	486
Nové atributy digitálního podpisu	486
Other Signing Certificate	488
Commitment Type Indication	489
Signer Location	490
Signer Attributes	490
Content Time Stamp	491
Signature Policy Identifier	491
Signature Time Stamp	493
Complete Certificate References	493
Complete Revocation References	493
Attribute Certificate References	494
Attribute Revocation References	494
Certificate Values	495
Revocation Values	495
ES-C Time Stamp	495
ES-C Time Stamped Certs and CRLs References	496

Archive Time Stamp	496
Politika digitálního podpisu	496
Pravidla pro vytváření a ověřování podpisu	498

Kapitola 26

Dlouhodobá archivace nejenom digitálně podepsaných dokumentů	503
Doba archivace dokumentů	504
Krátkodobá archivace	505
Střednědobá archivace	506
Dlouhodobá a trvalá archivace	506
Problém formátu dat	506
Archivy	507
OAIS	509
Důvěryhodná archivační autorita (TAA)	511
Přístup k archivovaným informacím	511
LTANS	512
ERS	512
Závěr	514

Kapitola 27

Budujeme PKI, TSA a důvěryhodné archivy	515
Identita koncového uživatele PKI	516
Identifikace zákazníků	516
Identifikace zaměstnanců a partnerů v aplikacích	518
Identifikace systémů a aplikací	519
Mapujeme využití PKI ve firmě/organizaci	519
Klienti/občané	519
Zaměstnanci/partneři	520
Interní systémy a aplikace	520
Veřejné aplikace	521
Vyhodnocení	521
Navrhujeme certifikační autority	523
Náklady na implementaci PKI v aplikacích	524
Náklady na čipové karty	525
Náklady na projekt a dokumentaci	526
Budujeme TSA	527
Veřejná TSA	527
Vlastní TSA	527
Volíme odpovídající důvěryhodný archiv	527
Rejstřík	529