

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 (<i>USB token</i>)	48
HSM (<i>Host Security Modul</i>)	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	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
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 klíče	81
Důkaz na základě výměny klíčů	81
Kořenový certifikát	82

PEM	83
PKCS#10	83
CRMF	84
SPK	85
Žádosti generované webovou stránkou	85
CMC	86

Kapitola 5

Odvolávání certifikátu	87
Žádost o odvolání certifikátu	89
CRL	90
Rozšíření CRL	91
Rozšíření položky CRL	92
On Line zjišťování statusu certifikátu	93
Platnost certifikátu k uvedenému datu	94
Vzdálené ověřování platnosti certifikátu	94

Kapitola 6

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

Kapitola 7

Ověřování platnosti certifikátu a poznámka k ověřování digitálního podpisu	107
Ověřování cesty začíná od důvěryhodné kotvy!	107
Ověřujeme certifikační cestu	108
Byl certifikát odvolán?	109
Microsoft	110
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 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

Naše první certifikační autorita	139
CA na bázi OpenSSL	139
Budujeme certifikační autoritu	141
Microsoft CA	149
Kofenová 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

Nástroje pro sledování sítě	161
Packet driver	162
Promiskuitní mód	162
Program Wireshark	163
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

ASN.1, BER, DER, UTF-8 a Base64	173
ASN.1	175
BER kódování	176
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
Kódování UTF-8	191
Base64	197

Kapitola 14

Žádost o vydání certifikátu pod lupou	199
Žádost ve tvaru kořenového certifikátu	199
PKCS#10	200
Atributy v PKCS#10	201
Žádost o certifikát v prostředí Microsoft	202

CRMF	204
Žádost	205
Důkaz vlastnictví soukromého klíče	207
Dodatečné registrační informace	208

Kapitola 15

Certifikát pod lupou 209

Struktura certifikátu	209
Algoritmus podpisu (<i>signatureAlgorithm</i>)	210
Podpis certifikátu (<i>signatureValue</i>)	211
TBSCertificate	212
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

CRL	257
Rozšíření CRL („rozšíření celého CRL“)	260
Rozšíření položek CRL	263
OCSP	265
OCSP dotaz	266
OCSP odpověď	269
Transportní protokol	274

Kapitola 17

CMP a CMC 275

Protokol CMP	275
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
Protokol CMC	283
Formát CMC zpráv	284
Atributy	288
Příklad (Windows 2003)	294

Kapitola 18

Budujeme certifikační autoritu	297
Bezpečnostní dokumentace	298
Analýza rizik	299
Od TCSEC a ITSEC k ISO/IEC 15408	301
FIPS	306
Řízení bezpečnosti firmy/organizace	306
Dokumentace certifikační autority	308
Testovací CA	310
Veřejné CA	310
Důvěryhodné kotvy	311
Enterprise CA – Windows Server 2008 R2	312
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

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

Vydávání atributového certifikátu	334
Uživatel sám žádá o vydání atributového certifikátu	335
Smluvní odběratel (Subscriber)	335
Na požadavek	336
Odvolávání atributových certifikátů	336
ACRL	337
On line zjišťování revokační informace	337
Verifikace atributového certifikátu	337
Atributová autorita	339
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
Dokumentace	342
Prováděcí (organizační) dokumentace	342
Bezpečnostní dokumentace	342
Další technologie přiřazování atributů	342

Kapitola 20

Časová razítka	345
Co to je čas?	346
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
TSA	352
Protokol pro vydávání časových razítek (TSP)	354
Transportní protokoly	355
Žádost o časové razítko	356
Odpověď TSA	357
Časové razítko	357
CMS zpráva SignedData	357
Obsah položek zprávy CMS Signed-data	358
TSTInfo	360
Ověřování časového razítka	361
Platnost časového razítka	362
Co časové razítko není	363
Provázané otisky	364
Lineární schéma	364

Stromové schéma	366
Zkratka	367
Kombinace redukováného stromu a zkratek	368

Kapitola 21

E-notary	369
Důvěryhodný archiv Rakouské notářské komory	370
Komerční organizace	370
Protokol DVCSP	371
SCVP	372

Kapitola 22

Protokol TLS	381
TLS relace a TLS spojení	384
Autentizace	386
Autentizace serveru	386
Autentizace klienta	387
Předběžné a hlavní sdílené tajemství	387
Record Layer Protocol (RLP)	388
Alert protocol	390
Change Cipher Specification Protocol (CCSP)	390
Handshake Protocol (HP)	391
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
Zpětná kompatibilita	401
HTTP	401
HTTP dotaz	402
HTTP odpověď	404
Některé další hlavičky	405
Proxy	407
Brána	408
Tunel	409
Bouncer (BNC)	410
HTTPS	411
Protocol upgrade	413

Kapitola 23

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

Kapitola 24

Bezpečná pošta	441
Poštovní transport	444
SMTP a ESMTP	444
POP3	450
IMAP4	454
Formát poštovní zprávy	454
E-mailová adresa	455
MIME	457
Hlavičky MIME	458
Hlavička Mime-Version	458
Hlavička Content-Transfer-Encoding	458
Hlavička Content-Type	459
S/MIME	462
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
Rozšířené S/MIME (ESS)	481

Kapitola 25

Dlouhodobý digitální podpis	487
CMS	488

LTES	488
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
Obnovování digitálního podpisu (signature renew)	494
Nové atributy digitálního podpisu	494
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
Politika digitálního podpisu	504
Pravidla pro vytváření a ověřování podpisu.....	506

Kapitola 26

Dlouhodobá archivace nejenom digitálně podepsaných dokumentů	511
Doba archivace dokumentů	512
Krátkodobá archivace.....	513
Střednědobá archivace.....	514
Dlouhodobá a trvalá archivace.....	514
Problém formátu dat	514
Archivy	515
OAIS	517
Důvěryhodná archivační autorita (TAA)	519
Přístup k archivovaným informacím.....	519
LTANS.....	520
ERS.....	520
Závěr	522

Kapitola 27

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