

Spis treści

1.	Wstęp	13
1.1.	Suma kontrolna (Hash)	18
1.2.	Szyfry symetryczne	21
1.3.	Szyfry asymetryczne	22
1.4.	Opakowanie elektroniczne	24
1.5.	Podpis elektroniczny	24
1.6.	Podrobienie klucza publicznego	26
1.7.	Certyfikacja klucza publicznego	28
1.8.	Podpis elektroniczny po raz drugi	29
1.9.	Certyfikat atrybutowy	29
1.10.	Znacznik czasu	30
1.11.	Poświadczenie notarialne	32
1.12.	Architektura systemu wystawiania „elektronicznych formularzy wniosku”	34
2.	Rodzina protokołów TCP/IP	37
2.1.	Protokoły warstwy fizycznej	39
2.1.1.	Zakłócenia komunikacyjne	39
2.1.2.	Przerwanie komunikacji	40
2.1.3.	Podsłuch	41
2.1.4.	Modyfikacje przesyłanych danych	41
2.1.5.	Szyfratory	42
2.2.	Protokoły warstwy łącza danych (liniowe)	42
2.2.1.	Ethernet	43
2.2.2.	FrameRelay	44
2.2.3.	PPP	44
2.2.4.	WLAN (IEEE 802.11)	54
2.3.	Ipv4	55
2.3.1.	Protokół ICMP	57
2.3.2.	Aspekty bezpieczeństwa IP	60
2.4.	IPv6	61
2.5.	NAT i NAT-PT	61
2.6.	IPsec	63
2.7.	Wirtualna sieć prywatna (VPN)	64
2.7.1.	Adresacja prywatna	65
2.7.2.	Tunel	65
2.8.	TCP	66
2.9.	UDP	70

2.10.	Zabezpieczenie danych aplikacyjnych.....	71
2.11.	Prezentacja danych	71
2.12.	Protokoły aplikacyjne	72
2.12.1.	DNS	73
2.12.2.	Protokół HTTP	82
2.12.3.	Poczta elektroniczna	85
2.12.4.	Protokół NTP.....	93
2.13.	Proxy, bramy i tunele aplikacyjne	99
2.13.1.	Proxy.....	99
2.13.2.	Brama.....	103
2.13.3.	Tunel.....	104
2.13.4.	Więcej pośrednich węzłów	106
2.14.	Aplikacje.....	107
2.15.	PKIX i PKI	108
2.16.	IDS (Intrusion Detection System)	109
2.17.	Dokumentacja	111
3.	MIME.....	113
3.1.	Nagłówki MIME.....	114
3.1.1.	Nagłówek Mime-Version	115
3.1.2.	Nagłówek Content-Type.....	115
3.1.3.	Nagłówek Content-Transfer-Encoding.....	116
3.1.4.	Nagłówek Content-ID.....	118
3.1.5.	Nagłówek Content-Description	118
3.1.6.	Nagłówek Content-Disposition	118
3.2.	Standardowe mechanizmy kodujące.....	119
3.2.1.	Quoted-printable.....	119
3.2.2.	Base64	120
3.2.3.	Radix-64	122
3.3.	Znaki w nagłówku, które nie są kodowane w ASCII	123
3.4.	Proste typy danych w nagłówku Content-Type.....	123
3.4.1.	Text.....	124
3.4.2.	Application	125
3.4.3.	Image	125
3.4.4.	Audio	126
3.4.5.	Video	126
3.4.6.	Model.....	126
3.5.	Typy złożone w Content-Type	126
3.5.1.	Multipart	127
3.5.2.	Message	132
4.	Uwierzytelnianie użytkownika i autoryzacja danych.....	137
4.1.	Hasła	138
4.2.	Hasło jednorazowe.....	139
4.2.1.	Lista haseł jednorazowych.....	139
4.2.2.	Algorytm rekurencyjny.....	141
4.2.3.	S/KEY.....	142

4.2.4.	OTP (One Time Password).....	143
4.2.5.	Uwierzytelnianie użytkownika i autoryzacja danych z wykorzystaniem wspólnego sekretu	144
4.2.6.	Kalkulatory uwierzytelniające	148
4.2.7.	Jednorazowe hasła przez GSM.....	151
4.3.	Kryptografia asymetryczna.....	152
4.3.1.	Zapisywanie prywatnego klucza na dysku	153
4.3.2.	Klucz sprzętowy	153
4.4.	Biometryka	155
4.5.	Charakterystyka środowiska	156
4.6.	Wrapper	157
4.6.1.	tcpd	160
4.6.2.	Protokół identyfikacyjny	161
4.7.	Protokoły RADIUS i TACACS+.....	161
4.7.1.	Niektóre atrybuty protokołu RADIUS	166
4.7.2.	Protokół RADIUS Accounting.....	167
4.7.3.	Przetwarzanie logu RADIUS Accounting	169
5.	Filtracja, proxy, ściana ogniowa oraz internetowy FrontEnd	173
5.1.	Filtracja	173
5.1.1.	Filtracja na poziomie protokołu IP	176
5.1.2.	Filtracja na poziomie TCP	182
5.1.3.	Filtry refleksyjne.....	188
5.1.4.	Filtracja protokołu UDP, ICMP i ewentualnie innych protokołów	192
5.1.5.	Zakazane adresy	193
5.1.6.	Protokoły aplikacyjne a filtracja.....	193
5.1.7.	Podsumowanie	198
5.2.	Proxy	199
5.2.1.	Klasyczne proxy	202
5.2.2.	Generyczne proxy	203
5.2.3.	Transparentne proxy	205
5.2.4.	Zakończenie.....	207
5.3.	SOCKS	208
5.3.1.	Protokół SOCKS.....	211
5.4.	WIN SOCKS	216
5.5.	Ukryte sieci	218
5.5.1.	Routowanie	220
5.6.	NAT	221
5.6.1.	Prosty NAT.....	222
5.6.2.	Rozszerzony NAT	223
5.6.3.	Podwójny NAT.....	225
5.6.4.	Rozkładanie obciążenia	226
5.6.5.	ALG.....	226
5.7.	Ściana ogniowa	227
5.7.1.	Jak wybrać ścianę ogniową?.....	234
5.7.2.	Strefy zdemilitaryzowane	235

5.7.3.	Firewall on Firewall.....	236
5.7.4.	Extranet.....	238
5.7.5.	Dostęp z Internetu do sieci wewnętrznej.....	239
5.7.6.	Protokoły aplikacyjne.....	240
5.8.	Internetowy FrontEnd.....	245
5.9.	Osobista ściana ogniowa.....	250
5.10.	Podsumowanie.....	252
6.	ASN.1, BER & DER.....	255
6.1.	Typy i identyfikatory.....	256
6.2.	Kodowanie BER.....	258
6.2.1.	Pole typu danych.....	259
6.2.2.	Pole długości danych.....	262
6.2.3.	Pole z danymi.....	263
6.2.4.	Przykłady.....	263
6.2.5.	Jak jest w kodowaniu BER zakodowany pusty typ?.....	265
6.2.6.	W jaki sposób koduje się typ BOOLEAN?.....	265
6.2.7.	Co z kodowaniem typu INTEGER?.....	265
6.2.8.	Wyliczenie.....	266
6.2.9.	Typy SEQUENCE, SEQUENCE OF, SET i SET OF.....	266
6.2.10.	Czas.....	267
6.2.11.	Bit string.....	268
6.3.	Identyfikator obiektu.....	268
6.3.1.	Kodowanie identyfikatorów obiektów w BER.....	271
6.4.	Typy wyprowadzone.....	273
6.5.	CHOICE.....	276
6.6.	ANY.....	277
6.7.	Kodowanie UTF-8.....	277
7.	Kryptografia.....	285
7.1.	Podstawowe systemy historyczne.....	288
7.2.	Szyfry symetryczne.....	289
7.3.	Tryby szyfrów blokowych.....	290
7.4.	Funkcja jednokierunkowa – Hash.....	293
7.5.	Systemy kryptograficzne z kluczem publicznym.....	294
7.6.	Podpis cyfrowy.....	297
7.7.	Kryptoanaliza.....	298
8.	PKI.....	299
8.1.	Certyfikat.....	300
8.1.1.	Wersja certyfikatu.....	306
8.1.2.	Numer seryjny certyfikatu.....	307
8.1.3.	Algorytm.....	308
8.1.4.	Ważność certyfikatu.....	308
8.1.5.	Nazwy wyróżnione.....	310
8.1.6.	Dane identyfikacyjne CA (wystawcy certyfikatu) – Issuer.....	316
8.1.7.	Dane identyfikacyjne użytkownika (podmiot certyfikatu) – subject.....	317

8.1.8.	Klucz publiczny	319
8.1.9.	Jednoznaczne identyfikatory	321
8.1.10.	Standardowe rozszerzenia certyfikatów	321
8.1.11.	Prywatne rozszerzenie certyfikatu	341
8.1.12.	Rozszerzenia wykorzystywane przez Microsoft	343
8.1.13.	Przykład certyfikatu	344
8.2.	Certyfikaty kwalifikowane	349
8.2.1.	Dane identyfikacyjne CA – issuer	350
8.2.2.	Dane identyfikacyjne użytkownika (podmiot certyfikatu)	351
8.2.3.	Wymagania przy standardowym rozszerzeniu certyfikatu	351
8.2.4.	Nowo wprowadzone rozszerzenia	353
8.3.	Wniosek o unieważnienie certyfikatu	355
8.4.	Lista certyfikatów unieważnionych – CRL	355
8.4.1.	Rozszerzenia CRL	360
8.4.2.	Rozszerzenie pozycji CRL	361
8.4.3.	Przykład CRL	363
8.5.	Weryfikacja online ważności certyfikatu – OCSP	364
8.5.1.	Wezwanie OCSP	365
8.5.2.	Odpowiedź OCSP	366
8.5.3.	Protokół transportowy	369
8.6.	Wniosek o certyfikat formatu PKCS#10	369
8.6.1.	Format wniosku o certyfikat	370
8.6.2.	Przykład wniosku	372
8.7.	Wniosek o certyfikat w formacie CRMF	374
8.7.1.	Dowód posiadania klucza prywatnego	375
8.7.2.	Właściwy wniosek o certyfikat	376
8.8.	Protokół CMP	378
8.8.1.	Nagłówek wiadomości CMP	379
8.8.2.	Ciało wiadomości CMP	380
8.8.3.	Pole ochrona	382
8.8.4.	Wniosek o certyfikat	384
8.8.5.	Odpowiedź na wniosek o certyfikat	384
8.8.6.	Odnawianie kluczy	386
8.8.7.	Unieważnienie certyfikatu	386
8.8.8.	Wydanie nowego certyfikatu głównego CA	387
8.8.9.	Potwierdzenie	387
8.8.10.	Inne wiadomości	388
8.8.11.	Transfer protokołem TCP/IP i rozszerzenia plików	388
8.9.	PKCS#7 i CMS	389
8.9.1.	Typy danych	391
8.9.2.	Typ wiadomości „Data”	392
8.9.3.	Typ wiadomości „SignedData”	392
8.9.4.	Przykład podpisanej wiadomości	397
8.9.5.	Eksport certyfikatu	406
8.9.6.	Typ wiadomości „Enveloped Data”	407
8.9.7.	Typ wiadomości „Digest Data”	411

8.9.8.	Typ wiadomości „Encrypted Data”	412
8.9.9.	Typ wiadomości „Authenticated Data”	412
8.10.	Protokół CMC.....	414
8.10.1.	Format wiadomości CMC	415
8.10.2.	Atrybuty.....	420
8.10.3.	MIME a rozszerzenie pliku	427
8.11.	Protokoły transportowe dla certyfikatów i CRL.....	428
8.12.	Time Stamp Protocol (TSP).....	428
8.12.1.	Wniosek o znacznik czasu	430
8.12.2.	Znacznik czasu	431
8.12.3.	Protokoły transportowe.....	433
8.13.	Protokół DVCSP.....	433
8.13.1.	Serwer DVC	436
8.13.2.	Wniosek o certyfikat DV	438
8.13.3.	Odpowiedź serwera DVC.....	440
8.13.4.	Certyfikat DV	441
8.13.5.	Sekwencja TargetEtcChain.....	442
8.13.6.	Komunikat serwera DVC o błędzie.....	443
8.13.7.	Przykład	444
8.14.	Certyfikaty atrybutowe	444
8.14.1.	Atrybuty.....	447
8.14.2.	Rozszerzenia certyfikatu atrybutowego.....	447
9.	Centrum certyfikacji (CA).....	449
9.1.	Ciąg certyfikatów.....	452
9.2.	Certyfikacja krzyżowa	454
9.3.	Odnowienie certyfikatu CA	457
9.4.	Polityki certyfikacji (zasady certyfikacji).....	458
9.4.1.	Testowe centrum certyfikacji	459
9.5.	Utworzenie wniosku o certyfikat	460
9.5.1.	Utworzenie wniosku za pomocą komponentów	460
9.5.2.	Wniosek formatu SPK	462
9.6.	PKI w środowisku Windows 2000	462
9.6.1.	Główne części PKI w Windows 2000	464
9.6.2.	Usługi i aplikacje używające certyfikatów	466
9.6.3.	Szablony certyfikatów	466
9.6.4.	Konsola Microsoft centrum certyfikacji MMC	468
9.6.5.	Mapowanie certyfikatów na konta użytkowników	469
9.6.6.	Hierarchia MSCA	470
10.	Bezpieczna poczta: S/MIME	475
10.1.	Wiadomość CMS wykorzystywana w S/MIME.....	475
10.2.	Certyfikaty i CRL	478
10.3.	MIME: Multipart/Signed a Multipart/Encrypted.....	479
10.4.	S/MIME	483
10.5.	Przykład elektronicznie podpisanej i zaszyfrowanej wiadomości.....	486
10.5.1.	Przykład zaszyfrowanej wiadomości.....	501

10.6.	Jakie niebezpieczeństwa czyhają na adresata	507
10.7.	Rozszerzone S/MIME (Enhanced Security Services for S/MIME – ESS).....	508
10.7.1.	Potwierdzenie doręczenia (Receipt)	510
10.7.2.	Wskazówki do zawartości (Podpisany temat wiadomości).....	512
10.7.3.	Etykiety bezpieczeństwa (Security Labels).....	513
10.7.4.	Bezpieczna lista dyskusyjna	513
10.7.5.	Certyfikat przeznaczony do weryfikacji podpisu	516
10.8.	MS Outlook XP	517
10.8.1.	Wysyłamy wiadomość.....	517
10.8.2.	Odbieramy wiadomość	519
10.9.	Podpis elektroniczny.....	521
10.9.1.	Podpis równoległy i seryjny	524
10.9.2.	Niektóre z wymienionych atrybutów podpisu.....	524
11.	Bezpieczny web: SSL i TLS.....	527
11.1.	Record Layer Protocol.....	534
11.2.	Alert Protocol.....	537
11.3.	Change Cipher Specification Protocol.....	538
11.4.	Handshake Protocol (HP)	539
11.4.1.	Utworzenie nowej sesji.....	540
11.4.2.	Odnawianie sesji.....	542
11.4.3.	Komunikaty ServerHello, Certificate, CertificateRequest i ServerHelloDone	550
11.4.4.	Komunikaty Certificate, ClientKeyExchange i CertificateVerify.....	557
11.4.5.	ServerKeyExchange	559
11.4.6.	HelloRequest	560
11.5.	Jak doszło do uwierzytelnienia	560
11.6.	SGC.....	560
11.7.	HTTPS (bezpieczny web).....	561
11.7.1.	Protocol upgrade.....	562
11.8.	Protokoły POP3 i IMAP4	563
11.9.	Filtrowanie SSL/TLS ścianą ogniową.....	564
12.	LDAP.....	565
12.1.	Nawiązanie i zakończenie sesji.....	570
12.2.	Search Request.....	573
12.3.	Search Response	579
13.	Podpis elektroniczny komponentów	583
13.1.	Komponenty ActiveX w przeglądarkach.....	583
13.1.1.	Inicjacja obiektu ActiveX.....	583
13.1.2.	Ustawienia bezpieczeństwa Microsoft Internet Explorera	586
13.1.3.	Program do podpisywania pliku SignCode.exe.....	587
13.2.	Wiarygodne aplety Java.....	588
13.2.1.	Ważne właściwości języka Java	588
13.2.2.	Platforma Javy	589
13.2.3.	Bezpieczny model Javy	590

13.2.4.	Aplikacja a aplet	591
13.2.5.	Co jest konieczne do prawidłowego działania podpisanego apletu?	592
13.2.6.	Przykład – w jaki sposób podpisać aplet	595
13.2.7.	Java plugin 1.3	596
14.	Przechowywanie certyfikatów	599
14.1.	Architektura kryptograficznych komponentów	599
14.2.	CSP i CryptoSPI	600
14.3.	CryptoAPI	604
14.4.	Logiczna i fizyczna przechowalnia certyfikatów	609
14.5.	Powiązanie certyfikatów i kluczy	610
14.6.	Typowy sposób wykorzystania	612
14.7.	Jak powstaje powiązanie pomiędzy certyfikatem i parą kluczy?	613
14.8.	Protected Storage System	615
14.9.	Źródła	616
15.	IPsec	619
15.1.	Protokoły AH i ESP	621
15.1.1.	Protokół AH	623
15.1.2.	Protokół ESP	624
15.1.3.	SPI	626
15.2.	Protokół ISAKMP	629
15.2.1.	Pakiet protokołu ISAKMP	630
15.3.	Protokół IKE	644
15.3.1.	Pierwsza faza	645
15.3.2.	Druga faza (Quick Mode)	646
15.3.3.	PFS	647
16.	SSH	649
16.1.	Protokół SSH wersja 2	650
16.1.1.	Transport Layer Protocol	650
16.1.2.	Authentication Protocol	657
16.1.3.	Connection Protocol	660
16.1.4.	SecureFTP	664
16.2.	Część praktyczna	665
16.2.1.	Uwierzytelnianie	665
16.2.2.	Serwer SSH (dla platformy Unix)	666
16.2.3.	Klient SSH (dla platformy Unix)	667
16.2.4.	Inne pomocne programy do pracy z SSH	669
16.2.5.	Pliki związane z SSH	670
16.2.6.	Kanał szyfrujący dla protokołu Telnet	671
16.2.7.	SCP	671
16.2.8.	Różnice między wersjami SSH1 a wersjami SSH2	672
16.2.9.	Pobieranie SSH	672

17. Bankowość elektroniczna i Internet.....	673
17.1. Home Banking, Internet Banking itd.....	673
17.2. Karty i SET (Secure Electronic Transactions).....	677
17.2.1. Wydanie certyfikatu	682
17.2.2. Podwójny podpis elektroniczny.....	686
17.2.3. Płatność.....	688
17.2.4. Autoryzacja płatności	691
17.2.5. Rozliczenie sprzedawcy z bankiem	693
17.3. 3D-SET	694
18. XML i podpis elektroniczny	697
18.1. Walidacja dokumentu	698
18.2. Wykorzystywanie URI	700
18.3. XML Namespace	700
18.4. XML i podpis elektroniczny	702
18.4.1. Encryption XML.....	702
18.4.2. Signature XML	703
18.4.3. Kanonizacja XML	703
18.4.4. Struktura XML podpisu cyfrowego.....	704
18.4.5. Przykład podpisu cyfrowego w XML	705
18.4.6. Reguły przetwarzania	707
18.4.7. Typy kluczy i algorytmów podpisujących.....	708
19. Protokół Kerberos	709
19.1. Poświadczenia.....	710
19.2. Key Distribution Center KDC – trzecia głowa Cerbera	711
19.3. Bilety.....	712
19.4. Bilety do wydawania biletów	713
19.5. Uwierzytelnianie pomiędzy domenami	714
19.5.1. Uwierzytelnianie pomiędzy dwiema domenami	714
19.5.2. Uwierzytelnianie pomiędzy większą liczbą domen.....	715
19.6. Podprotokoły protokołu Kerberos	717
19.6.1. Usługa uwierzytelniania AS	717
19.6.2. Usługa wydawania biletów TGS	718
19.6.3. CS Exchange.....	718
19.7. Cały proces	719
19.8. Struktura biletów	719
19.8.1. Czas ważności biletu	721
19.8.2. Odnawialne TGT	722
19.8.3. Delegowanie uwierzytelniania	722
19.9. Struktura KDC	723
19.10. Programy.....	724
19.11. Implementacja Kerberosa w wersji 5 w Windows 2000	727
19.11.1. Konto domeny	728
19.11.2. Baza danych kont.....	728

19.11.3. Polityka Kerberos	729
19.11.4. Usługi wykorzystujące protokół Kerberos	729
19.11.5. DNS i Kerberos	730
19.11.6. Dane autoryzacji	730
19.11.7. Zgłaszanie za pomocą karty chipowej	732
20. OpenSSL	735
20.1. Opis systemu	735
20.1.1. Instalacja	735
20.1.2. Wykorzystanie	736
20.2. Proste testowe centrum certyfikacji	739
20.2.1. req	742
20.2.2. ca	745
20.3. asn1parse	746
20.4. SSL/TLS	746
21. Bezpieczeństwo danych	749
Skorowidz	755