Danksagungen 19

Vorwort 21

Einführung 23
Über das Buch 23
Die Begleit-CD 24
Systemvoraussetzungen 24

I PKI-Grundlagen 27

1 Grundlagen der Kryptografie 29
Verschlüsselungsarten 30
Algorithmen und Schlüssel 30
Datenverschlüsselung 31
Symmetrische Verschlüsselung 31
Asymmetrische Verschlüsselung 33
Asymmetrische Signatur 34
Kombination von symmetrischer und asymmetrischer Verschlüsselung 35
Digitale Signatur von Daten 37
Der Hashvorgang 37
Hashalgorithmen 37
Kombination von asymmetrischer Signatur und Hashalgorithmen 38
Cryptography Next Generation (CNG) 39
Eigenschaften von CNG 39
Unterstützte Algorithmen 42
Unterstützte Clients und Anwendungen 42
Fallstudie: Microsoft-Anwendungen und ihre Verschlüsselungsalgorithmen 43
Öffnen des EFS-Whitepapers 43
Fragen zur Fallstudie 44
Weitere Informationen 44

2 Einführung in PKI 47
Zertifikate 48
X.509 Version 1 49
X.509 Version 2 50
X.509 Version 3 52
Zertifizierungsstellen 55
Stammzertifizierungsstelle 57
Zwischenzertifizierungsstelle 58
Richtlinienzertifizierungsstelle 58
Ausstellende Zertifizierungsstelle 59
Zertifikatsperrlisten 59
Sperrlistenarten 60
Gründe für eine Zertifikatsperrung 60
OCSP (Online Certificate Status Protocol) 61
OCSP-Client 62
Online-Responder-Dienst 62
Fallstudie: Untersuchung eines X.509-Zertifikats 63
Öffnen der Zertifikatdatei 63

Fragen zur Fallstudie 63
Weitere Informationen 64

3 Richtlinien und PKI 65
Sicherheitsrichtlinie 67
Definition effektiver Sicherheitsrichtlinien 67
Unterlagen für die Entwicklung von Sicherheitsrichtlinien 68
Auswirkungen von externen Richtlinien auf Ihre PKI 68
Definition von PKI-bezogenen Sicherheitsrichtlinien 70
Zertifikatrichtlinie 71
Inhalt einer Zertifikatrichtlinie 71
Zertifikatrichtlinienbeispiel 72
Zertifikatverwendungserklärung (CPS) 74
CPS-Abschnitt: Einführung 75
CPS-Abschnitt: Verantwortlichkeit für Veröffentlichung und Speicherung 76
CPS-Abschnitt: Identifikation und Authentifizierung 76
CPS-Abschnitt: Anforderungen an die Vorgehensweisen 76
CPS-Abschnitt: Kontrolle der Räumlichkeiten, Verwaltung und Arbeitsabläufe 78
CPS-Abschnitt: Kontrolle der technischen Sicherheit 79
CPS-Abschnitt: Zertifikate, Zertifikatsperrlisten und OCSP-Profile 80
CPS-Abschnitt: Überwachung der Befolgung und andere Beurteilungen 80
CPS-Abschnitt: Andere geschäftliche und rechtliche Aspekte 80
Fallstudie: Entwurf der Richtliniendokumente 81
Anforderungen an den Entwurf 81
Fragen zur Fallstudie 82
Weitere Informationen 82

II Einrichtung einer PKI 83

4 Vorbereiten einer Active Directory-Umgebung 85
Analyse der Active Directory-Umgebung 86
Aktualisieren des Schemas 87
Identifizieren des Schemabetriebsmasters 87
Durchführen der Schema-Aktualisierung 88
Ändern der Bereiche der Zertifikatherausgeber-Gruppen 90
Bereitstellen von Windows Server 2008-Unternehmenszertifizierungsstellen in Umgebungen ohne AD DS 94
Fallstudie: Vorbereiten der Active Directory-Domänendienste 94
Netzwerkdetails 96
Fragen zur Fallstudie 96
Weitere Informationen 97

5 Entwerfen einer Zertifizierungsstellenhierarchie 99
Bestimmen der Anzahl der Schichten in einer Zertifizierungsstellenhierarchie 100
Einschichtige Zertifizierungsstellenhierarchie 100
Zweischichtige Zertifizierungsstellenhierarchie 101
Dreischichtige Zertifizierungsstellenhierarchie 102
Vierschichtige Zertifizierungsstellenhierarchie 103
Organisation ausstellender Zertifizierungsstellen 104
Auswahl einer Architektur 107
Sammlung der erforderlichen Informationen 107

Identifikation PKI-fähiger Anwendungen 107
Bestimmung der Anforderungen an die Sicherheit 109
Bestimmung der technischen Anforderungen 111
Ermittlung der betrieblichen Anforderungen 117
Ermitteln externer Anforderungen 118
Sammeln der AD DS-Anforderungen 120
Namenskonventionen 120
Auswählen der Domänen für Zertifizierungsstellencomputerkonten 121
Auswählen einer Organisationseinheitsstruktur 121
Fallstudie: Ermitteln der Anforderungen 122
Fragen zur Fallstudie 123
Weitere Informationen 124

6 Implementieren einer Zertifizierungsstellenhierarchie 125
Zertifizierungsstellen-Konfigurationsdateien 127
Die Datei CAPolicy.inf 127
Vorinstallationsskripts 136
Nachinstallationsskripts 140
Implementieren einer dreischichtigen Zertifizierungsstellenhierarchie 147
Einrichten einer Offline-Stammzertifizierungsstelle 147
Einrichten einer Offline-Richtlinienzertifizierungsstelle 151
Einrichten einer ausstellenden Onlinezertifizierungsstelle 157
Einrichten einer Organisations-Stammzertifizierungsstelle 165
Erstellen einer CAPolicy.inf-Datei 165
Installieren der Active Directory-Zertifikatdienste 166
Nachinstallationskonfiguration 168
Aktivieren der Überwachung 168
Überprüfen der Installation 170
Fallstudie: Einrichten einer PKI 171
Fragen zur Fallstudie 171
Weitere Informationen 173

7 Aktualisieren einer vorhandenen Microsoft-PKI 175
Unterstützte Szenarien 176
Welche Versionen lassen sich auf Windows Server 2008 aktualisieren? 176
Wechseln von 32-Bit- auf 64-Bit-Systeme 177
Durchführen der Aktualisierung 180
Aktualisieren des Schemas 180
Aktualisieren der Zertifikatvorlagen 181
Durchführen der Aktualisierung 181
Nacharbeiten nach der Aktualisierung 182
Fallstudie: Aktualisieren einer vorhandenen PKI 185
Fragen zur Fallstudie 186
Weitere Informationen 187

8 Überprüfen und Überwachen Ihrer Microsoft-PKI 189
Überprüfen der Installation 190
Unternehmens-PKI (PKI Health Tool) 190
Certutil 196
Laufende Überwachung 199
CAMonitor.vbs-Skript 199
Microsoft Operations Manager Certificate Services Management Pack 202
Fallstudie: Überprüfen einer PKI-Bereitstellung 208

Einzelheiten der Zertifizierungsstellenhierarchie 208
Fragen zur Überprüfung der Zertifizierungsstellenhierarchie 208
Anforderungen an die Überwachung 209
Fragen zur Überwachung 209
Weitere Informationen 210

9 Absichern einer Zertifizierungsstellenhierarchie 211
Sicherheitsmaßnahmen in der Konfiguration der Zertifizierungsstellen 212
Absichern der Hardware 215
Sichern des privaten Schlüssels der Zertifizierungsstelle 216
Speicherung privater Schlüssel im Speicher Lokaler Computer 216
Speichern privater Schlüssel auf Smartcards 217
Speicherung privater Schlüssel auf Hardwaresicherheitsmodulen 218
Hardwaresicherheitsmodule 219
Kategorien von Hardwaresicherheitsmodulen 219
Verschiedene Einsatzweisen der Hardwaresicherheitsmodule 220
Fallstudie: Planen einer HSM-Bereitstellung 225
Szenario 225
Fragen zur Fallstudie 226
Weitere Informationen 227

10 Sperrung von Zertifikaten 229
Wann sperrt man Zertifikate? 230
Gründe für eine Zertifikatsperrung 230
Sperrrichtlinie 231
Sperren eines Zertifikats 232
Methoden zur Identifizierung von gesperrten Zertifikaten 233
Probleme mit Zertifikatsperrlisten 234
Verzögerter Informationsfluss 234
Zwischenspeichern von Zertifikatsperrlisten 234
Unterstützung für Deltasperrlisten 234
Online Certificate Status Protocol (OCSP) 235
Microsofts OCSP-Implementierung 235
Bereitstellen des Microsoft Online-Responders 239
Sichern einer hohen Verfügbarkeit des Online-Responders 250
Fallstudie: Planung der Zertifikatsperrung 252
Anforderungen an den Entwurf 252
Fragen zur Fallstudie 253
Weitere Informationen 254

11 Überprüfen von Zertifikaten 255
Der Ablauf der Überprüfung 256
Gültigkeitsprüfungen 257
Sperrungsüberprüfungsmethoden 258
Ändern der Standardüberprüfung 258
Aufstellen von Zertifikatketten 260
Genaue Übereinstimmung 261
Übereinstimmende Schlüssel 262
Übereinstimmende Namen 263
Veröffentlichen der PKI-Objekte 264
Wählen der Veröffentlichungsprotokolle 264
Wählen der Veröffentlichungspunkte 265
Festlegen der Veröffentlichungsintervalle 266

Beheben von Problemen bei der Überprüfung von Zertifikaten 268
CAPI-Diagnose 268
Fallstudie: Wählen der Veröffentlichungspunkte 274
Anforderungen an den Entwurf 274
Fragen zur Fallstudie 275
Übung zur Problembehebung 275
Weitere Informationen 276

12 Entwerfen von Zertifikatvorlagen 277

Zertifikatvorlagenversionen 278
Version 1-Zertifikatvorlagen 278
Version 2-Zertifikatvorlagen 280
Version 3-Zertifikatvorlagen 281
Registrieren von Zertifikaten, die mit Zertifikatvorlagen ausgestellt werden 281
Standardzertifikatvorlagen 282
Ändern von Zertifikatvorlagen 283
Ändern der Berechtigungen für Version 1-Zertifikatvorlagen 284
Bearbeiten von Version 2- und Version 3-Zertifikatvorlagen 284
Fallstudie: Entwerfen von Zertifikatvorlagen 297
Anforderungen 297
Fragen zur Fallstudie 298
Empfehlungen für den Entwurf von Zertifikatvorlagen 299
Weitere Informationen 300

13 Rollentrennung 301

Common Criteria-Rollen 302
Common Criteria-Rollen und Sicherheitsstufen 302
Die Windows-Implementierung der Common Criteria 304
Zuweisen von Common Criteria-Rollen 307
Beschränken der Aufgaben eines Zertifikatmanagers 309
Durchsetzen der Common Criteria-Rollentrennung 311
Andere PKI-Verwaltungsrollen 312
Lokaler Administrator 312
Organisations-Admins 313
Zertifikatvorlagenmanager 313
Registrierungs-Agent 316
Schlüsselwiederherstellungs-Agent 316
Fallstudie: Planen der PKI-Managementrollen 317
Szenario 317
Fragen zur Fallstudie 318
Weitere Informationen 319

14 Planen und Implementieren der Notfallwiederherstellung 321

Entwickeln der erforderlichen Dokumentation 322
Auswählen einer Sicherungsmethode 324
Wer darf die Zertifikatdienste sichern? 324
Systemstatussicherungen 325
Windows Server-Sicherungen 325
Manuelle Sicherungen 325
Durchführen einer Systemstatussicherung 326
Installieren der Windows Server-Sicherung 326

Durchführen einer Systemstatussicherung 327
Durchführen von Windows Server-Sicherungen 327
Erstellen einer Windows Server-Sicherung nach Zeitplan 327
Erstellen einer Windows Server-Einmalsicherung 328
Durchführen manueller Sicherungen 329
Manuelle Sicherung mit der Konsole Zertifizierungsstelle 330
Certutil-Befehle 330
Wiederherstellungsmethoden 332
Ermitteln der Sicherungsversionen 332
Wiederherstellen einer Systemstatussicherung 333
Wiederherstellen einer Windows Server-Sicherung 334
Wiederherstellen einer manuellen Sicherung 335
Bewerten der Sicherungsmethoden 337
Hardwareausfall 338
Ausfall der Zertifikatdienste 338
Ersetzen des Servers 339
Optionen zur Verbesserung der Verfügbarkeit 339
CRL-Verlängerung 340
HSM-Failover 341
Zertifikatdienstecluster 341
Fallstudie: Ersetzen der Serverhardware 359
Szenario 359
Fragen zur Fallstudie 360
Weitere Informationen 361

15 Ausstellen von Zertifikaten 363
Zertifikatregistrierungsmethoden 365
Auswählen einer Registrierungsmethode 367
Auswählen unter den manuellen Registrierungsmethoden 367
Auswählen unter den automatischen Registrierungsmethoden 367
Veröffentlichen von Zertifikatvorlagen für die Registrierung 368
Manuelle Registrierung 370
Anfordern von Zertifikaten mit dem Zertifikatregistrierungs-Assistenten 370
Anfordern von Zertifikaten mit der Webregistrierung 373
Abfragen einer ausstehenden Zertifikatanforderung 375
Übermittlung einer Zertifikatanforderung von Netzwerkgeräten und anderen Plattformen 376
Automatische Registrierung 379
Einstellungen der automatischen Zertifikatanforderung 379
Einstellung für die automatische Registrierung 380
Registrieren mit Skripts 382
Serverspeicherung von Anmeldeinformationen 386
Was wird auf dem Server gespeichert? 387
Wie ist die Serverspeicherung von Anmeldeinformationen in die Active Directory Domänendienste integriert? 387
Voraussetzungen 387
Gruppenrichtlinieneinstellungen 388
Fallstudie: Auswählen einer Zertifikatanforderungsmethode 389
Szenario 389
Fragen zur Fallstudie 391
Weitere Informationen 391

16 Vertrauen zwischen Organisationen 393

Vertrauenschaffende Maßnahmen 394
Zertifikatvertrauenslisten 395
Gemeinsame Stammzertifizierungsstellen 396
Kreuzzertifizierung 398
Brückenzertifizierungsstellen 399
Namenseinschränkungen 403
Basiseinschränkungen 405
Anwendungsrichtlinien 406
Zertifikatrichtlinien 408
Empfehlungen 410
Implementieren der Kreuzzertifizierung mit Beschränkungen 411
Erstellen der Datei Policy.inf 413
Beschaffen eines Zertifizierungsstellenzertifikats von einem Partner 413
Anfordern eines Kreuzzertifizierungsstellenzertifikats 413
Veröffentlichen in den Active Directory-Domänendiensten 414
Überprüfen der Kreuzzertifizierung 415
Fallstudie: Zertifikaten aus anderen Gesamtstrukturen vertrauen 415
Fragen zur Fallstudie 417
Weitere Informationen 417

III Bereitstellen anwendungsspezifischer Lösungen 419

17 Zertifikatverwaltung mit Identity Lifecycle Manager 2007 421

Schlüsselkonzepte 422
Profilvorlagen 422
CLM-Rollen 423
Berechtigungen 423
Orte für die Zuweisung von Berechtigungen 424
CLM-Komponenten 426
Planen einer ILM 2007 Certificate Management-Bereitstellung 427
Verwaltungsrichtlinien 427
Registrierungsmodelle 429
Bereitstellen von ILM 2007 Certificate Management 432
Installation des Servers 432
Konfigurieren des Servers 435
Installieren der Zertifizierungsstellenkomponenten 442
Bereitstellen eines Codesignaturzertifikats 445
Festlegen der Zertifikatvorlagenberechtigungen 445
Erstellen einer Profilvorlage 445
Ausführen der Verwaltungsrichtlinien 451
Fallstudie: Contoso 453
Vorgeschlagene Lösung 454
Fragen zur Fallstudie 455
Empfohlene Vorgehensweisen 455
Weitere Informationen 456

18 Archivieren von Verschlüsselungsschlüsseln 457

Rollen bei der Schlüsselarchivierung 459
Die Schlüsselarchivierung 460
Die Schlüsselwiederherstellung 462

Voraussetzungen für die Schlüsselarchivierung 462
Definieren der Schlüsselwiederherstellungs-Agenten 464
Aktivieren einer Zertifizierungsstelle für die Schlüsselarchivierung 469
Aktivieren der Schlüsselarchivierung in einer Zertifikatvorlage 471
Durchführen der Schlüsselwiederherstellung 472
Durchführen der Schlüsselwiederherstellung mit Certutil 472
Durchführen der Schlüsselwiederherstellung mit ILM 2007 Certificate Management 474
Fallstudie: Lucerne Publishing 475
Szenario 476
Fragen zur Fallstudie 476
Empfohlene Vorgehensweisen 477
Weitere Informationen 478

19 Implementieren der SSL-Verschlüsselung für Webserver 479

So funktioniert SSL 480
Zertifikaterfordernisse für SSL 482
Auswählen eines Webserverzertifikatanbieters 483
Speicherorte für Webserverzertifikate 484
Einzelne Webserver 484
Webservercluster 484
Durch ISA Server mit Server Publishing geschützte Webserver 485
Durch ISA Server mit Web Publishing geschützte Webserver 486
Wählen einer Zertifikatvorlage 487
Ausstellen von Webserver-Zertifikaten 487
Ausstellen von Webserver-Zertifikaten an Domänenmitglieder 488
Ausstellen von Webserver-Zertifikaten an Websites, die nicht zur Gesamtstruktur gehören 493
Ausstellen von Webserver-Zertifikaten an Webserver von anderen Herstellern und an Webbeschleuniger 498
Authentifizierung mit Zertifikaten 498
Definieren der Zertifikatzuordnungen 499
Authentifizierung auf Zertifikatbasis in der Praxis 500
Erstellen einer Zertifikatvorlage 500
Definieren der Zuordnung in den Active Directory-Domänendiensten 500
Aktivieren von Zertifikatzuordnungen unter Windows Server 2003 502
Aktivieren von Zertifikatzuordnungen unter Windows Server 2008 503
Aufnehmen einer Verbindung mit der Website 505
Fallstudie: The Phone Company 506
Szenario 506
Fragen zur Fallstudie 508
Empfohlene Vorgehensweisen 508
Weitere Informationen 509

20 Das verschlüsselnde Dateisystem 511

EFS-Prozesse 512
So wählt Windows ein EFS-Verschlüsselungszertifikat aus 512
Lokale EFS-Verschlüsselung 513
Remoteverschlüsselung 514
EFS-Entschlüsselung 516
EFS-Datenwiederherstellung 517
Eine Anwendung, zwei Wiederherstellungsmethoden 518
Datenwiederherstellung 518

Schlüsselwiederherstellung 521
Implementieren von EFS 521
Aktivieren und Deaktivieren von EFS 522
Zertifikatvorlagen für die EFS-Verschlüsselung 523
Zertifikatregistrierung 525
Was gibt es Neues für die EFS-Verwaltung in Windows Vista? 526
Fallstudie: Lucerne Publishing 529
Szenario 529
Planungsvorgaben 530
Lösungsvorschlag 531
Fragen zur Fallstudie 532
Empfohlene Vorgehensweisen 532
Weitere Informationen 533

21 Bereitstellen von Smartcards 535
Verwenden von Smartcards in einer AD DS-Umgebung 536
Smartcards und Kerberos 536
Voraussetzungen für Smartcard-Zertifikate 536
Planen der Smartcard-Bereitstellung 538
Bereitstellen von Smartcards mit Windows Vista 540
Bereitstellen von Smartcards mit ILM 2007 Certificate Management 547
Verwalten ausgestellter Smartcards 560
Smartcard-Pflicht bei der interaktiven Anmeldung 560
Smartcard-Pflicht bei der Anmeldung an bestimmten Computern 561
Smartcard-Pflicht für Remote-Anmeldungen 561
Konfigurieren des Systemverhaltens bei der Entfernung einer Smartcard 561
Konfigurieren der Standardeinstellungen für Smartcards 561
Fallstudie: City Power and Light 563
Fragen zur Fallstudie 565
Empfohlene Vorgehensweisen 565
Weitere Informationen 566

22 Sichere E-Mail 569
Sicherung von E-Mail 570
Secure/Multipurpose Internet Mail Extensions (S/MIME) 570
SSL für Internetprotokolle 573
Auswählen der Zertifizierungsstellen 576
Kommerzielle Zertifizierungsstellen 576
Eigene Zertifizierungsstellen 576
Auswählen der Zertifikatvorlagen 577
Eine Zertifikatvorlage für Signatur und Verschlüsselung 577
Separate Zertifikatvorlagen für Signatur und Verschlüsselung 579
Wählen der Bereitstellungsmethoden 581
Bereitstellen von Softwarezertifikaten 581
Bereitstellen von Smartcard-Zertifikaten 582
Aktivieren sicherer E-Mail 582
Aktivieren von Outlook 583
Aktivieren von S/MIME in Outlook Web Access 585
Versenden sicherer E-Mails 585
Fallstudie: Adventure Works 586
Szenario 586
Fragen zur Fallstudie 588
Empfohlene Vorgehensweisen 589

Weitere Informationen 590

23 Virtuelle private Netzwerke 591
Bereitstellen von Zertifikaten für VPN 592
Point-to-Point Tunneling Protocol (PPTP) 592
Layer Two Tunneling Protocol (L2TP) mit Internetprotokollsicherheit 594
Secure Sockets Tunneling Protocol (SSTP) 596
Entwerfen der Zertifikatvorlagen 597
Benutzerauthentifizierung 597
Serverauthentifizierung 598
IPsec-Endpunktauthentifizierung 598
SSTP-Endpunktauthentifizierung 599
Einrichten einer VPN-Lösung 599
Netzwerkrichtlinienserverkonfiguration 600
VPN-Server-Konfiguration 604
Erstellen einer VPN-Clientverbindung 605
Fallstudie: Lucerne Publishing 608
Szenario 608
Fragen zur Fallstudie 610
Empfohlene Vorgehensweisen 611
Weitere Informationen 612

24 Drahtlose Netzwerke 615
Neue Gefahren durch drahtlose Netzwerke 616
Schutz der drahtlosen Kommunikation 617
MAC-Filterung 617
Wired Equivalent Privacy (WEP) 617
Wi-Fi Protected Access (WPA) und WPA2 618
802. lx-Authentifizierungsarten 619
EAP-TLS-Authentifizierung 619
PEAP-Authentifizierung 619
So funktioniert die 802.1x-Authentifizierung 620
Planung der Zertifikate zur 802.1x-Authentifizierung 621
Computerzertifikate für RADIUS-Server 621
Benutzerzertifikate für Clients 622
Computerzertifikate für Clients 622
Ausstellen von Zertifikaten an Benutzer und Computer 623
RADIUS-Server 623
Clientcomputer 624
Benutzer 624
Implementieren der 802.1x-Authentifizierung 625
Konfigurieren des RADIUS-Servers 625
Konfigurieren des drahtlosen Zugriffspunkts 631
Verbinden mit dem drahtlosen Netzwerk 631
Durchsetzung der Clientkonfiguration mit Gruppenrichtlinien 635
Fallstudie: Margie's Travel 636
Szenario 636
Fragen zur Fallstudie 637
Empfohlene Vorgehensweisen 638
Weitere Informationen 638

25 Dokument- und Codesignatur 641
So funktioniert die Codesignatur 642

So funktioniert die Dokumentsignatur 643
Zertifizierung von Signaturzertifikaten 643
Kommerzielle Zertifizierung von Codesignaturzertifikaten 644
Eigenzertifizierung von Code- und Dokumentsignaturzertifikaten 645
Planen der Bereitstellung von Codesignaturzertifikaten 645
Entwerfen von Zertifikatvorlagen 645
Planen der Methoden zur Zertifikatanforderung 647
Zeitstempel 648
Durchführen der Codesignatur 648
Beschaffen der erforderlichen Programme 648
Verwenden von SignTooLexe 649
VBA-Projekte 650
Durchführen der Dokumentsignatur 651
Microsoft Office 2007-Documente 651
Adobe-PDF-Documente 652
Überprüfen der Signatur 654
Internet Explorer 654
Überprüfen von signiertem Code 655
Microsoft Office-Dokumente 655
PDF-Dokumente 656
Fallstudie: Lucerne Publishing 656
Szenario 656
Fragen zur Fallstudie 657
Empfohlene Vorgehensweisen 657
Weitere Informationen 658

26 Bereitstellen von Zertifikaten für Domänencontroller 661
Änderungen in Domänencontrollerzertifikaten 662
Durchsetzen der strengen KDC-Überprüfung 664
Zertifikatauswahl auf einem Windows Server 2008-Domänencontroller 664
Bereitstellen von Domänencontrollerzertifikaten 665
Einstellungen der automatischen Zertifikatanforderung 665
Automatische Registrierung 666
Zertifizierungsstellen anderer Hersteller und Zertifizierungsstellen in anderen Gesamtstrukturen 666
Hinzufügen der internen Stammzertifizierungsstelle als vertrauenswürdige Stammzertifizierungsstelle 668
Hinzufügen der untergeordneten Zertifizierungsstellenzertifikate 668
Definieren der NTAuth-Zertifikate 668
Aktivieren der Erweiterung Alternativer Antragstellername für Zertifikatanforderungen 669
Erstellen der Zertifikatanforderungen 669
Verwalten der Domänencontrollerzertifikate 670
Überprüfen von Zertifikaten 671
Ersetzen vorhandener Domänencontrollerzertifikate 672
Entfernen aller Domänencontrollerzertifikate 672
Fallstudie: Consolidated Messenger 672
Stand der Umstellungsarbeiten 673
Fragen zur Fallstudie 673
Empfohlene Vorgehensweisen 673
Weitere Informationen 674

27 Registrierungsdienst für Netzwerkgeräte 675
Geschichte von NDES und der Microsoft PKI 676

SCEP-Registrierung 677
Implementieren eines NDES-Servers 680
Berechtigungen 681
Vorbereiten der Zertifizierungsstelle 682
Erstellen eines Dienstkontos 682
Installieren des NDES-Servers 683
Konfigurieren von NDES 685
Anpassen der Registrierung 686
Aktivieren der Protokollierung 686
Sicherung und Wiederherstellung 686
Fallstudie: Lucerne Publishing 687
Anforderungen 687
Fragen zur Fallstudie 688
Empfohlene Vorgehensweisen 688
Weitere Informationen 689

A Antworten zu den Fallbeispielen 691

Stichwortverzeichnis 727

Der Autor 759