

**Microsoft**

Foreword by David Cross  
*Microsoft Security Principal Program Manager*

# Windows Server® 2008 PKI and Certificate Security



Brian Komar



PUBLISHED BY

Microsoft Press  
A Division of Microsoft Corporation  
One Microsoft Way  
Redmond, Washington 98052-6399

Copyright © 2008 by Brian Komar

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2008920575

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWT 3 2 1 0 9 8

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at [www.microsoft.com/mspress](http://www.microsoft.com/mspress). Send comments to [mspinput@microsoft.com](mailto:mspinput@microsoft.com).

Microsoft, Microsoft Press, Access, Active Directory, ActiveX, Authenticode, BitLocker, Excel, IntelliMirror, Internet Explorer, MSDN, Outlook, SQL Server, Visual Basic, Visual C#, Visual C++, Visual Studio, Win32, Windows, Windows Server System and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

**Acquisitions Editor:** Martin DelRe

**Developmental Editor:** Karen Szall

**Project Editor:** Denise Bankaitis

**Editorial Production:** Interactive Composition Corporation

**Technical Reviewer:** Paul Adare; Technical Review services provided by Content Master, a member of CM Group, Ltd.

**Cover:** Tom Draper Design

Body Part No. X14-60364

# Contents at a Glance

<b>Part I</b>	<b>Foundations of PKI</b>	
1	Cryptography Basics .....	3
2	Primer to PKI.....	21
3	Policies and PKI .....	39
<b>Part II</b>	<b>Establishing a PKI</b>	
4	Preparing an Active Directory Environment .....	59
5	Designing a Certification Authority Hierarchy .....	73
6	Implementing a CA Hierarchy .....	99
7	Upgrading Your Existing Microsoft PKI .....	151
8	Verifying and Monitoring Your Microsoft PKI.....	165
9	Securing a CA Hierarchy .....	189
10	Certificate Revocation.....	207
11	Certificate Validation.....	235
12	Designing Certificate Templates .....	259
13	Role Separation .....	285
14	Planning and Implementing Disaster Recovery .....	307
15	Issuing Certificates.....	351
16	Creating Trust Between Organizations.....	383
<b>Part III</b>	<b>Deploying Application-Specific Solutions</b>	
17	Identity Lifecycle Manager 2007 Certificate Management.....	413
18	Archiving Encryption Keys .....	453
19	Implementing SSL Encryption for Web Servers .....	475
20	Encrypting File System .....	509
21	Deploying Smart Cards.....	535
22	Secure E-Mail .....	571
23	Virtual Private Networking.....	595
24	Wireless Networking .....	619
25	Document and Code Signing.....	647
26	Deploying Certificates to Domain Controllers .....	667
27	Network Device Enrollment Service .....	683
A	Case Study Questions and Answers.....	699



# Table of Contents

Acknowledgments.....	xxiii
Foreword.....	xxv
Introduction.....	xxvii
About This Book.....	xxvii
Windows Server 2008 PKI and Certificate Security Companion CD.....	xxviii
System Requirements.....	xxix

## Part I Foundations of PKI

<b>1</b>	<b>Cryptography Basics.....</b>	<b>3</b>
	Encryption Types.....	3
	Algorithms and Keys.....	4
	Data Encryption.....	4
	Symmetric Encryption.....	4
	Asymmetric Encryption.....	6
	Asymmetric Signing Process.....	8
	Combining Symmetric and Asymmetric Encryption.....	9
	Digital Signing of Data.....	11
	The Hash Process.....	11
	Hash Algorithms.....	11
	Combining Asymmetric Signing and Hash Algorithms.....	12
	Cryptography Next Generation (CNG).....	13
	Features of CNG.....	13
	Algorithms Supported.....	16
	Supported Clients and Applications.....	17

 **What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

[www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)

- Case Study: Microsoft Applications and Their Encryption Algorithms . . . . . 18
  - Opening the EFS White Paper . . . . . 18
  - Case Study Questions . . . . . 18
  - Additional Information . . . . . 19
- 2 Primer to PKI . . . . . 21**
  - Certificates . . . . . 21
    - X.509 Version 1 . . . . . 22
    - X.509 Version 2 . . . . . 23
    - X.509 Version 3 . . . . . 24
  - Certification Authorities . . . . . 29
    - Root CA . . . . . 31
    - Intermediate CA . . . . . 31
    - Policy CA . . . . . 31
    - Issuing CA . . . . . 33
  - Certificate Revocation Lists . . . . . 33
    - Types of CRLs . . . . . 33
    - Revocation Reasons . . . . . 34
    - Online Certificate Status Protocol (OCSP) . . . . . 35
    - OCSP Client . . . . . 36
    - Online Responder Service . . . . . 36
  - Case Study: Inspecting an X.509 Certificate . . . . . 37
    - Opening the Certificate File . . . . . 37
    - Case Study Questions . . . . . 37
    - Additional Information . . . . . 38
- 3 Policies and PKI . . . . . 39**
  - Security Policy . . . . . 40
    - Defining Effective Security Policies . . . . . 41
    - Resources for Developing Security Policies . . . . . 41
    - Effects of External Policies on Your PKI . . . . . 42
    - Defining PKI-Related Security Policies . . . . . 44
  - Certificate Policy . . . . . 45
    - Contents of a Certificate Policy . . . . . 45
    - Certificate Policy Example . . . . . 46
  - Certification Practice Statement (CPS) . . . . . 47
    - CPS Section: Introduction . . . . . 49
    - CPS Section: Publication and Repository Responsibilities . . . . . 49

CPS Section: Identification and Authentication . . . . .	50
CPS Section: Certificate Life-Cycle Operational Requirements . . . . .	50
CPS Section: Facility, Management, and Operational Controls . . . . .	52
CPS Section: Technical Security Controls . . . . .	53
CPS Section: Certificate, CRL, and OCSP Profiles . . . . .	53
CPS Section: Compliance Audit and Other Assessment . . . . .	53
CPS Section: Other Business and Legal Matters . . . . .	54
Case Study: Planning Policy Documents . . . . .	55
Design Requirements . . . . .	55
Case Study Questions . . . . .	55
Additional Information . . . . .	55

## Part II **Establishing a PKI**

<b>4</b>	<b>Preparing an Active Directory Environment . . . . .</b>	<b>59</b>
	Analyzing the Active Directory Environment . . . . .	59
	Upgrading the Schema . . . . .	60
	Identifying the Schema Operations Master . . . . .	61
	Performing the Schema Update . . . . .	61
	Modifying the Scope of the Cert Publishers Groups . . . . .	63
	Deploying Windows Server 2008 Enterprise CAs in Non-AD DS Environments . . . . .	68
	Case Study: Preparing Active Directory Domain Services . . . . .	68
	Network Details . . . . .	70
	Case Study Questions . . . . .	70
	Additional Information . . . . .	71
<b>5</b>	<b>Designing a Certification Authority Hierarchy . . . . .</b>	<b>73</b>
	Determining the Number of Tiers in a CA Hierarchy . . . . .	73
	Single-Tier CA Hierarchy . . . . .	73
	Two-Tier CA Hierarchy . . . . .	74
	Three-Tier CA Hierarchy . . . . .	75
	Four-Tier CA Hierarchy . . . . .	76
	Organizing Issuing CAs . . . . .	77
	Choosing an Architecture . . . . .	80
	Gathering Required Information . . . . .	80
	Identifying PKI-Enabled Applications . . . . .	81
	Determining Security Requirements . . . . .	83
	Determining Technical Requirements . . . . .	84



	Determining Business Requirements .....	91
	Determining External Requirements.....	92
	Collecting AD DS Requirements .....	93
	Naming Conventions .....	94
	Choosing Domains for CA Computer Accounts.....	94
	Choosing an Organizational Unit Structure.....	95
	Case Study: Identifying Requirements .....	96
	Case Study Questions .....	97
	Additional Information .....	98
<b>6</b>	<b>Implementing a CA Hierarchy .....</b>	<b>99</b>
	CA Configuration Files .....	100
	CAPolicy.inf File .....	100
	Pre-Installation Scripts .....	110
	Post-Installation Scripts.....	113
	Implementing a Three-Tier CA Hierarchy .....	121
	Implementing an Offline Root CA .....	121
	Implementing an Offline Policy CA.....	125
	Implementing an Online Issuing CA.....	132
	Implementing an Enterprise Root CA.....	141
	Creating a CAPolicy.inf File.....	141
	Installing Active Directory Certificate Services.....	142
	Post-Installation Configuration .....	144
	Enabling Auditing .....	144
	Verifying Installation .....	146
	Case Study: Deploying a PKI .....	147
	Case Study Questions .....	147
	Additional Information .....	149
<b>7</b>	<b>Upgrading Your Existing Microsoft PKI .....</b>	<b>151</b>
	Supported Scenarios .....	151
	What Versions Can You Upgrade to Windows Server 2008?.....	151
	32-Bit to 64-Bit Considerations.....	152
	Performing the Upgrade.....	155
	Upgrading the Schema.....	155
	Upgrading Certificate Templates .....	156
	Performing the Upgrade .....	157
	Post-Upgrade Operations.....	158

Case Study: Upgrading an Existing PKI . . . . .	160
Case Study Questions . . . . .	161
Additional Information . . . . .	163
<b>8 Verifying and Monitoring Your Microsoft PKI. . . . .</b>	<b>165</b>
Verifying the Installation . . . . .	165
PKI Health Tool . . . . .	166
Certutil . . . . .	172
Ongoing Monitoring . . . . .	176
CAMonitor.vbs Script . . . . .	176
Microsoft Operations Manager Certificate Services Management Pack . . . . .	179
Case Study: Verifying a PKI Deployment. . . . .	185
CA Hierarchy Details . . . . .	185
CA Hierarchy Verification Questions . . . . .	186
Monitoring Requirements . . . . .	187
Monitoring Questions . . . . .	187
Additional Information . . . . .	187
<b>9 Securing a CA Hierarchy . . . . .</b>	<b>189</b>
CA Configuration Measures . . . . .	189
Designing Physical Security Measures. . . . .	192
Securing the CA's Private Key . . . . .	193
Private Key Stored in the Local Machine Store . . . . .	193
Private Keys Stored on Smart Cards . . . . .	194
Private Keys Stored on Hardware Security Modules . . . . .	195
Hardware Security Modules . . . . .	196
Categories of HSMs . . . . .	196
HSM Deployment Methods . . . . .	197
Case Study: Planning HSM Deployment . . . . .	202
Scenario . . . . .	202
Case Study Questions . . . . .	203
Additional Information . . . . .	204
<b>10 Certificate Revocation . . . . .</b>	<b>207</b>
When Do You Revoke Certificates? . . . . .	207
Revocation Reasons . . . . .	207
Revocation Policy . . . . .	208
Performing Revocation . . . . .	210

Methods of Identifying Revoked Certificates . . . . .	210
Problems with CRLs . . . . .	211
Latency . . . . .	211
Caching of CRLs . . . . .	211
Support for Delta CRLs . . . . .	212
Online Certificate Status Protocol (OCSP) . . . . .	212
Microsoft's Implementation of OCSP . . . . .	213
Implementing the Microsoft Online Responder . . . . .	217
Providing High Availability for the Online Responder . . . . .	230
Case Study: Planning Revocation . . . . .	232
Design Requirements . . . . .	232
Case Study Questions . . . . .	233
Additional Information . . . . .	234
<b>11 Certificate Validation . . . . .</b>	<b>235</b>
Certificate Validation Process . . . . .	235
Certificate Validity Checks . . . . .	236
Revocation Checking Methods . . . . .	237
Changing the Default Validation Behavior . . . . .	238
Building Certificate Chains . . . . .	240
Exact Match . . . . .	241
Key Match . . . . .	241
Name Match . . . . .	242
Designing PKI Object Publication . . . . .	243
Choosing Publication Protocols . . . . .	244
Choosing Publication Points . . . . .	245
Choosing Publication Intervals . . . . .	247
Troubleshooting Certificate Validation . . . . .	248
CAPI Diagnostics . . . . .	249
Case Study: Choosing Publication Points . . . . .	255
Design Requirements . . . . .	255
Case Study Questions . . . . .	256
Troubleshooting Exercise . . . . .	257
Additional Information . . . . .	257
<b>12 Designing Certificate Templates . . . . .</b>	<b>259</b>
Certificate Template Versions . . . . .	259
Version 1 Certificate Templates . . . . .	259

	Version 2 Certificate Templates . . . . .	261
	Version 3 Certificate Templates . . . . .	262
	Enrolling Certificates Based on Certificate Templates . . . . .	263
	Default Certificate Templates . . . . .	263
	Modifying Certificate Templates . . . . .	265
	Modifying Version 1 Certificate Template Permissions . . . . .	265
	Modifying Version 2 and Version 3 Certificate Templates . . . . .	266
	Case Study: Certificate Template Design . . . . .	280
	Requirements . . . . .	280
	Case Study Questions . . . . .	281
	Best Practices for Certificate Template Design . . . . .	282
	Additional Information . . . . .	283
<b>13</b>	<b>Role Separation . . . . .</b>	<b>285</b>
	Common Criteria Roles . . . . .	285
	Common Criteria Levels . . . . .	285
	Windows Implementation of Common Criteria . . . . .	288
	Assigning Common Criteria Roles . . . . .	291
	Implementing Certificate Manager Restrictions . . . . .	293
	Enforcing Common Criteria Role Separation . . . . .	295
	Other PKI Management Roles . . . . .	296
	Local Administrator . . . . .	296
	Enterprise Admins . . . . .	297
	Certificate Template Manager . . . . .	297
	Enrollment Agent . . . . .	300
	Key Recovery Agent . . . . .	301
	Case Study: Planning PKI Management Roles . . . . .	302
	Scenario . . . . .	302
	Case Study Questions . . . . .	303
	Additional Information . . . . .	304
<b>14</b>	<b>Planning and Implementing Disaster Recovery . . . . .</b>	<b>307</b>
	Developing Required Documentation . . . . .	308
	Choosing a Backup Method . . . . .	309
	Who Can Perform Backups of Certificate Services . . . . .	309
	System State Backups . . . . .	310
	Windows Server Backups . . . . .	310
	Manual Backups . . . . .	311

Performing a System State Backup . . . . .	311
Installing Windows Server Backup . . . . .	311
Performing a System State Backup . . . . .	312
Performing Windows Server Backups . . . . .	312
Creating a Scheduled Windows Server Backup . . . . .	312
Performing a One-Time-Only Windows Server Backup . . . . .	314
Performing Manual Backups . . . . .	315
Using the Certification Authority Console. . . . .	315
Certutil Commands. . . . .	316
Restoration Procedures. . . . .	318
Determining Backup Versions . . . . .	318
Restoring a System State Backup . . . . .	319
Restoring a Windows Server Backup . . . . .	319
Restoring a Manual Backup . . . . .	321
Evaluating Backup Methods. . . . .	323
Hardware Failure . . . . .	324
Certificate Services Failure . . . . .	324
Server Replacement . . . . .	324
Availability Options . . . . .	325
CRL Re-Signing . . . . .	326
HSM Fail Over. . . . .	327
Clustering Certificate Services. . . . .	327
Case Study: Replacing Server Hardware. . . . .	346
Scenario. . . . .	347
Case Study Questions . . . . .	348
Additional Information . . . . .	349
<b>15 Issuing Certificates. . . . .</b>	<b>351</b>
Certificate Enrollment Methods . . . . .	352
Choosing an Enrollment Method . . . . .	354
Choosing Among Manual Enrollment Methods. . . . .	354
Choosing Among Automatic Enrollment Methods . . . . .	355
Publishing Certificate Templates for Enrollment . . . . .	355
Performing Manual Enrollment. . . . .	357
Requesting Certificates by Running the Certificate Enrollment Wizard. . . . .	357
Using Web Enrollment to Request a Certificate. . . . .	360

Completing a Pending Certificate Request .....	362
Submitting a Certificate Request from Network Devices and Other Platforms .....	364
Performing Automatic Enrollment.....	367
Automatic Certificate Request Settings .....	368
Autoenrollment Settings.....	368
Performing Scripted Enrollment .....	371
Credential Roaming .....	374
What Is Included in the Roaming .....	375
How Does CRS Use Active Directory Domain Services?.....	376
Requirements .....	376
Group Policy Settings.....	376
Case Study: Selecting a Deployment Method .....	378
Scenario .....	379
Case Study Questions .....	379
Additional Information .....	380
<b>16   Creating Trust Between Organizations .....</b>	<b>383</b>
Methods of Creating Trust .....	383
Certificate Trust Lists .....	384
Common Root CAs.....	386
Cross Certification .....	387
Bridge CAs.....	389
Name Constraints.....	392
Basic Constraints .....	395
Application Policies .....	396
Certificate Policies .....	398
Best Practices .....	401
Implementing Cross Certification with Constraints .....	402
Implementing the Policy.inf File.....	404
Acquiring a Partner's CA Certificate .....	404
Generating the Cross Certification Authority Certificate.....	405
Publishing to Active Directory Domain Services.....	406
Verifying Cross Certification Constraints .....	406
Case Study: Trusting Certificates from Another Forest.....	407
Case Study Questions .....	408
Additional Information .....	409

## Part III Deploying Application-Specific Solutions

<b>17</b>	<b>Identity Lifecycle Manager 2007 Certificate Management . . . . .</b>	<b>413</b>
	Key Concepts . . . . .	414
	Profile Templates . . . . .	414
	CLM Roles . . . . .	415
	Permissions . . . . .	415
	Permission Assignment Locations . . . . .	416
	CLM Components . . . . .	417
	Planning an ILM 2007 Certificate Management Deployment . . . . .	419
	Management Policies . . . . .	419
	Registration Models . . . . .	421
	Deploying ILM 2007 Certificate Management . . . . .	425
	Installation of Server . . . . .	426
	Configuration of Server . . . . .	429
	CA Component Installation . . . . .	436
	Deploying a Code Signing Certificate . . . . .	439
	Defining Certificate Template Permissions . . . . .	440
	Creating a Profile Template . . . . .	440
	Executing the Management Policies . . . . .	447
	Case Study: Contoso, Ltd. . . . .	449
	Proposed Solution . . . . .	450
	Case Study Questions . . . . .	451
	Best Practices . . . . .	451
	Additional Information . . . . .	452
<b>18</b>	<b>Archiving Encryption Keys . . . . .</b>	<b>453</b>
	Roles in Key Archival . . . . .	454
	The Key Archival Process . . . . .	454
	The Key Recovery Process . . . . .	457
	Requirements for Key Archival . . . . .	458
	Defining Key Recovery Agents . . . . .	459
	Enabling a CA for Key Archival . . . . .	465
	Enabling Key Archival in a Certificate Template . . . . .	466
	Performing Key Recovery . . . . .	468
	Using Certutil to Perform Key Recovery . . . . .	468
	Performing Key Recovery with ILM 2007 Certificate Management . . . . .	470

Case Study: Lucerne Publishing . . . . .	471
Scenario . . . . .	472
Case Study Questions . . . . .	472
Best Practices. . . . .	473
Additional Information . . . . .	474
<b>19 Implementing SSL Encryption for Web Servers . . . . .</b>	<b>475</b>
How SSL Works . . . . .	475
Certificate Requirements for SSL . . . . .	478
Choosing a Web Server Certificate Provider . . . . .	478
Placement of Web Server Certificates. . . . .	479
Single Web Server . . . . .	480
Clustered Web Servers. . . . .	480
Web Server Protected by ISA Server with Server Publishing . . . . .	481
Web Server Protected by ISA Server with Web Publishing . . . . .	481
Choosing a Certificate Template . . . . .	483
Issuing Web Server Certificates . . . . .	483
Issuing Web Server Certificates to Domain Members . . . . .	484
Issuing Web Server Certificates to Non-Forest Members . . . . .	489
Issuing Web Server Certificates to Third-Party Web Servers and Web Acceleration Devices. . . . .	495
Certificate-Based Authentication. . . . .	495
Defining Certificate Mapping . . . . .	496
Performing Certificate-Based Authentication . . . . .	497
Creating a Certificate Template . . . . .	497
Defining the Mapping in Active Directory Domain Services . . . . .	498
Enabling Windows Server 2003 to Use Certificate Mapping . . . . .	500
Enabling Windows Server 2008 to Use Certificate Mapping . . . . .	501
Connecting to the Web Site . . . . .	503
Case Study: The Phone Company . . . . .	505
Scenario . . . . .	505
Case Study Questions . . . . .	506
Best Practices. . . . .	507
Additional Information . . . . .	507
<b>20 Encrypting File System . . . . .</b>	<b>509</b>
EFS Processes. . . . .	509
How Windows Chooses an EFS Encryption Certificate . . . . .	510
Local EFS Encryption . . . . .	510



	Remote Encryption . . . . .	512
	EFS Decryption. . . . .	513
	EFS Data Recovery. . . . .	514
	One Application, Two Recovery Methods . . . . .	515
	Data Recovery . . . . .	516
	Key Recovery . . . . .	519
	Implementing EFS . . . . .	519
	Enabling and Disabling EFS . . . . .	519
	Certificate Templates for EFS Encryption. . . . .	520
	Certificate Enrollment. . . . .	523
	What's New in Windows Vista for EFS Management. . . . .	524
	Case Study: Lucerne Publishing. . . . .	527
	Scenario. . . . .	528
	Design Requirements . . . . .	528
	Proposed Solution. . . . .	529
	Case Study Questions . . . . .	530
	Best Practices . . . . .	531
	Additional Information . . . . .	532
<b>21</b>	<b>Deploying Smart Cards . . . . .</b>	<b>535</b>
	Using Smart Cards in an Active Directory Environment . . . . .	535
	Smart Cards and Kerberos . . . . .	536
	Requirements for Smart Card Certificates. . . . .	536
	Planning Smart Card Deployment . . . . .	538
	Deploying Smart Cards with Windows Vista. . . . .	539
	Deploying Smart Cards by Using ILM 2007 Certificate Management . . . . .	547
	Managing Issued Smart Cards. . . . .	562
	Requiring Smart Cards for Interactive Logon . . . . .	562
	Requiring Smart Cards at Specific Computers . . . . .	563
	Requiring Smart Cards for Remote Access . . . . .	563
	Configuring Smart Card Removal Behavior . . . . .	563
	Configuring Smart Card Settings . . . . .	564
	Case Study: City Power and Light . . . . .	566
	Case Study Questions . . . . .	567
	Best Practices . . . . .	568
	Additional Information . . . . .	569

<b>22</b>	<b>Secure E-Mail</b> .....	<b>571</b>
	Securing E-Mail .....	571
	Secure/Multipurpose Internet Mail Extensions (S/MIME) .....	571
	SSL for Internet Protocols .....	574
	Choosing Certification Authorities .....	578
	Choosing Commercial CAs .....	578
	Choosing Private CAs .....	578
	Choosing Certificate Templates .....	579
	A Combined Signing and Encryption Template .....	579
	Dual Certificates for E-Mail .....	581
	Choosing Deployment Methods .....	583
	Software-Based Certificate Deployment .....	583
	Smart Card-Based Certificate Deployment .....	585
	Enabling Secure E-Mail .....	585
	Enabling Outlook .....	585
	Enabling S/MIME in OWA .....	588
	Sending Secure E-Mail .....	588
	Case Study: Adventure Works .....	589
	Scenario .....	590
	Case Study Questions .....	591
	Best Practices .....	592
	Additional Information .....	593
<b>23</b>	<b>Virtual Private Networking</b> .....	<b>595</b>
	Certificate Deployment for VPN .....	595
	Point-to-Point Tunneling Protocol (PPTP) .....	595
	Layer Two Tunneling Protocol (L2TP) with Internet Protocol Security .....	598
	Secure Sockets Tunneling Protocol (SSTP) .....	599
	Certificate Template Design .....	600
	User Authentication .....	600
	Server Authentication .....	601
	IPsec Endpoint Authentication .....	602
	SSTP Endpoint Authentication .....	602
	Deploying a VPN Solution .....	603
	Network Policy Server Configuration .....	603
	VPN Server Configuration .....	608
	Create a VPN Client Connection .....	610

	Case Study: Lucerne Publishing . . . . .	613
	Scenario . . . . .	613
	Case Study Questions . . . . .	615
	Best Practices . . . . .	616
	Additional Information . . . . .	617
<b>24</b>	<b>Wireless Networking . . . . .</b>	<b>619</b>
	Threats Introduced by Wireless Networking . . . . .	619
	Protecting Wireless Communications . . . . .	620
	MAC Filtering . . . . .	620
	Wired Equivalent Privacy . . . . .	620
	Wi-Fi Protected Access (WPA) and WPA2 . . . . .	621
	802.1x Authentication Types . . . . .	622
	EAP-TLS Authentication . . . . .	622
	PEAP Authentication . . . . .	623
	How 802.1x Authentication Works . . . . .	623
	Planning Certificates for 802.1x Authentication . . . . .	624
	Computer Certificates for RADIUS Servers . . . . .	624
	User Certificates for Clients . . . . .	626
	Computer Certificates for Clients . . . . .	626
	Deploying Certificates to Users and Computers . . . . .	627
	RADIUS Server . . . . .	627
	Client Computers . . . . .	627
	Users . . . . .	628
	Implementing 802.1x Authentication . . . . .	629
	Configuring the RADIUS Server . . . . .	629
	Configuring the Wireless Access Point . . . . .	635
	Connecting to the Wireless Network . . . . .	636
	Using Group Policy to Enforce Correct Wireless Client Configuration . . . . .	640
	Case Study: Margie's Travel . . . . .	641
	Scenario . . . . .	641
	Case Study Questions . . . . .	643
	Best Practices . . . . .	643
	Additional Information . . . . .	644
<b>25</b>	<b>Document and Code Signing . . . . .</b>	<b>647</b>
	How Code Signing Works . . . . .	647
	How Document Signing Works . . . . .	648

Certification of Signing Certificates . . . . .	649
Commercial Certification of Code Signing Certificates . . . . .	649
Corporate Certification of Code Signing and Document Signing Certificates . . . . .	650
Planning Deployment of Signing Certificates . . . . .	651
Certificate Template Design . . . . .	651
Planning Enrollment Methods . . . . .	652
Time Stamping Considerations . . . . .	653
Performing Code Signing . . . . .	654
Gathering the Required Tools . . . . .	654
Using SignTool.exe . . . . .	655
Visual Basic for Applications Projects . . . . .	656
Performing Document Signing . . . . .	657
Microsoft Office 2007 Documents . . . . .	658
Adobe PDF Documents . . . . .	659
Verifying the Signature . . . . .	660
Internet Explorer . . . . .	660
Validating Signed Code . . . . .	662
Microsoft Office Documents . . . . .	662
PDF Documents . . . . .	663
Case Study: Lucerne Publishing . . . . .	663
Scenario . . . . .	663
Case Study Questions . . . . .	664
Best Practices . . . . .	665
Additional Information . . . . .	666
<b>26 Deploying Certificates to Domain Controllers . . . . .</b>	<b>667</b>
Changes in Domain Controller Certificates . . . . .	667
Enforcing Strong KDC Validation . . . . .	669
Windows Server 2008 Domain Controller Certificate Selection . . . . .	670
Deploying Domain Controller Certificates . . . . .	671
Automatic Certificate Request Settings . . . . .	671
Autoenrollment . . . . .	671
Third-Party CAs or CAs in Other Forests . . . . .	672
Add the Internal Root CA as a Trusted Root CA . . . . .	674
Add the Subordinate CA Certificates . . . . .	674
Define NTAAuth Certificates . . . . .	674

	Enable the SAN Extension for Certificate Requests . . . . .	675
	Creating the Certificate Requests . . . . .	675
	Managing Domain Controller Certificates . . . . .	677
	Verifying Existing Certificates . . . . .	677
	Replacing Existing Certificates . . . . .	678
	Removing all Existing Certificates . . . . .	678
	Case Study: Consolidated Messenger . . . . .	678
	Deployment Progress . . . . .	679
	Case Study Questions . . . . .	679
	Best Practices . . . . .	680
	Additional Information . . . . .	680
<b>27</b>	<b>Network Device Enrollment Service . . . . .</b>	<b>683</b>
	History of NDES and Microsoft PKI . . . . .	683
	Simple Certificate Enrollment Protocol Enroll Process . . . . .	684
	Implementing an NDES Server . . . . .	687
	Permission Requirements . . . . .	688
	CA Requirements . . . . .	689
	Create the Service Account . . . . .	690
	Installing the NDES Server . . . . .	690
	Configuring NDES . . . . .	692
	Modifying the Registry . . . . .	692
	Enabling Logging . . . . .	694
	Backup and Restoration . . . . .	694
	Case Study: Lucerne Publishing . . . . .	695
	Requirements . . . . .	695
	Case Study Questions . . . . .	696
	Best Practices . . . . .	696
	Additional Information . . . . .	697
<b>A</b>	<b>Case Study Questions and Answers . . . . .</b>	<b>699</b>
	Chapter 1: Cryptography Basics . . . . .	699
	Chapter 2: Primer to PKI . . . . .	700
	Chapter 3: Policies and PKI . . . . .	701
	Chapter 4: Preparing an Active Directory Environment . . . . .	702
	Chapter 5: Designing a Certification Authority Hierarchy . . . . .	704
	Chapter 6: Implementing a CA Hierarchy . . . . .	706

Chapter 7: Upgrading Your Existing Microsoft PKI . . . . .	710
Chapter 8: Verifying and Monitoring Your Microsoft PKI . . . . .	712
CA Hierarchy Verification Questions . . . . .	712
Monitoring Questions . . . . .	713
Chapter 9: Securing a CA Hierarchy . . . . .	714
Chapter 10: Certificate Revocation . . . . .	715
Chapter 11: Certificate Validation . . . . .	716
Troubleshooting Exercise. . . . .	716
Chapter 12: Designing Certificate Templates . . . . .	717
Chapter 13: Role Separation. . . . .	719
Chapter 14: Planning and Implementing Disaster Recovery. . . . .	721
Chapter 15: Issuing Certificates . . . . .	722
Chapter 16: Creating Trust Between Organizations . . . . .	724
Chapter 17: Identity Lifecycle Manager 2007 Certificate Management . . . . .	725
Chapter 18: Archiving Encryption Keys. . . . .	727
Chapter 19: Implementing SSL Encryption for Web Servers. . . . .	729
Chapter 20: Encrypting File System. . . . .	730
Chapter 21: Deploying Smart Cards . . . . .	731
Chapter 22: Secure E-Mail. . . . .	733
Chapter 23: Virtual Private Networking . . . . .	735
Chapter 24: Wireless Networking . . . . .	736
Chapter 25: Document and Code Signing . . . . .	738
Chapter 26: Deploying Certificates to Domain Controllers. . . . .	738
Chapter 27: Network Device Enrollment Service . . . . .	739
 Index . . . . .	 741



**What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

[www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)



# Acknowledgments

When you work on a book project, several people are involved in the writing process one way or another, and I am going to try my best to thank everyone who helped me through the research, envisioning, and writing of this book. If I did miss anyone, it is only because there were so many people who played a part in making this book a reality!

The first group of people that I want to thank is the PKI product and testing team, current members and past members, from Microsoft: David Cross, Vic Heller, Phil Hallin, Avi Ben-Menahem, Oded Ye Shekel, Jen Field, Kelvin Yiu, and Yogesh Mehta. All of you helped me get my head around several of the specifics of the Microsoft PKI and the new features of Windows Server 2008.

I especially want to thank Avi, Oded, Jen, and Carsten Kinder, who wrote many of the draft white papers that I used to research the topics for the second edition. Your white papers helped me learn the technologies and get my head around the the new nuances.

The second group of people that I have to thank are the clients that IdentIT Inc. has had the pleasure of working with over the last five years. Paul Adare and I have learned more than you can imagine by interacting with you and your networks.

A book is only as good as the project team that helps the author translate thoughts to words on a page. I want to specifically thank the following individuals:

- Martin DelRe, the product planner, for bringing the book proposal to Microsoft Press.
- Seth Scruggs, Chris Gregory, and Shawn Rouborn, for pushing me to proceed with a second edition.
- Denise Bankaitis, for keeping the project flowing (especially with my attempting to write parts of this book on every continent—again...).
- Paul Adare, for your outstanding technical review of the content. Although the reviews took me hours to incorporate, the book is much stronger because of your efforts and knowledge.
- The Trustworthy Computing Security Content Review Board (TwC SCRB), a Microsoft team that reviewed each and every chapter to provide the final check for technical accuracy and consistency with Microsoft product and technology messaging and strategies. The SCRB team members for this book were David Kennedy, Shawn Rouborn, Jonathan Stephens, Michiko Short, Elton Tucker, Ken Carr, Sanjay Pandit, Jose Luis Auricchio, Matthijs ten Seldam, Akshat Kesarwani, Edward Gomes, Lupe Brieno, Anders Brabæk, Mark Eden, and Monica Ene-Pietrosanu. A special thank-you to Ken, Shawn, and Jonathon for finding the time to review each and every chapter of this book.



**xxiv Acknowledgments**

- Sue McClung, for managing the vendor editorial team and keeping this book moving during the development process.
- Kenneth Jackson, for updating the enrollment script and creating a new version based on Certenroll.dll for Windows Vista clients.
- Ryan Hurst, for providing me information on the Online Certificate Status Protocol (OCSP) and agreeing to be quoted in the OCSP chapter.

Finally, I would like to thank you, the reader. If you bought the first edition of this book, your purchase helped convince Microsoft that this is a technology that needs to be documented and discussed for successful deployments. I have talked with many of you on public news groups and look forward to working with you in the future.

# Foreword

The world of PKI, the deployments and the applications, have evolved significantly since Microsoft introduced user certificate enrollment in Windows XP and Windows Server 2003. Although we anticipated that we would change the world in how public key infrastructures were deployed and leveraged, little did we know how fast the market would change and the deployments flourish. When we set out with the Microsoft Windows 2000 release of the Microsoft PKI, we wanted to make PKI as easy and ubiquitous as TCP/IP, Web browsing, and Kerberos. To achieve that goal, we needed to accomplish two critical criteria:

- Simplify the configuration and management of certification authorities
- Eliminate the need for end users to see or understand PKI

Of course, every deployment and every application requirement is different—but the reality was the world needed an easy, cost-effective, and secure infrastructure to support the growing need for encryption, data integrity, and authentication capabilities in an increasingly hostile world. Five years later, when we look at our goals and the success to date, I am more than pleasantly surprised when I see the number of deployments and maturity of public key infrastructures in use. Not a week goes by that I don't hear about another customer that has issued millions of certificates for IPsec from a single Windows Server 2003 certificate server or an enterprise that has deployed a global smart card logon solution for all remote access and VPN users. What took months to set up and years to deploy in large numbers is now taking days and the deployments completed in the matter of a few months.

Yet, despite the maturity of PKI and the mass deployments, the technology continues to evolve and change with the security risks, attacks, and requirements of the time. Customer, consumers, and enterprises are becoming increasingly aware and demanding encryption and protection of data be applied and used whenever sensitive information is stored or transferred. This leads to increasing performance, reliability, and usability requirements in both the platform and applications. Windows Server 2008 includes the latest advancements in cryptographic algorithm strength, performance, and optimizations.

Windows Server 2008 provides the latest technology and updates to meet those ever-evolving needs and security requirements of the future. It not only provides support for the latest hash algorithms and asymmetric public key technologies and a modern revocation technology infrastructure, it also provides this capability on top of a modern agile cryptographic platform. What is unique in Windows Server 2008 is the introduction of Cryptography Next Generation (CNG), which enables independent hardware vendors, independent software vendors, and customers to use and plug in their own algorithms without waiting for a complete update or revision to the Windows platform. This is a significant step forward for the infrastructure to evolve dynamically as the security landscape changes unpredictably.

In addition to development and use of new algorithms, hashing techniques, and protocols, Windows Server 2008 introduces additional management and deployment enhancements such as native integration of the Simple Certificate Enrollment Protocol (SCEP), Microsoft Operations Manager (MOM) monitor and management pack, and inline revocation services that support Online Certificate Status Protocol (OCSP) clients. When you look at the number of enhancements and overall functionality in Windows Server 2008, you would agree the technology area is continuing to mature and innovate.

What's next for the future of PKI? If I were to be an oracle and predict the future, I would say that the industry will continue to see integration with card management systems, additional integration with identity management systems, and next generation deployment capabilities that are natively integrated into the latest Web service and wireless protocols. I think that you will see Windows Server 2008 as a preview of many of these integrations along with the release of other Microsoft products such as Identity Lifecycle Manager, System Center, and Forefront.

Why a second book on Microsoft PKI? Well, very frankly, the market demand for PKI and Active Directory Certificate Services demands it. As a whole, the market has not produced many PKI books, but I think Microsoft Press has found and hit a "sweet spot" in the industry—it focuses on real world deployments and IT professional needs, and of course, it is based on the most popular and widely deployed PKI globally: Active Directory Certificate Services.

Brian Komar has become a beacon and unique champion for the Microsoft PKI vision and solution around the world. He has a unique style and balance in his approach, which provides IT professionals and enterprises a pragmatic view of deployments while at the same time providing all the tricks, traps, and best practices to be aware of...before the deployment starts. Brian has built this database of knowledge, and subsequently represented in this book, through his long-term working relationship with the PKI product development team here in Redmond combined with numerous hands-on customer engagement and deployments using the Microsoft PKI solution.

This book is a "must have" for the Microsoft PKI administrator. It takes the best of the product team development knowledge, the best practices from our field consultants around the world (Microsoft Consulting Services), and our customer deployments to date and distills into a one-stop resource kit of knowledge that cannot be found in any other single source to my knowledge. The goal of the book helps to achieve the goal that we set out many years ago: Enable customers to deploy PKI to achieve their security and application protection requirements as easily as any other critical network infrastructure technology. I look forward to the day when PKI becomes a household word on the Internet just like "IP addresses." I think we are well on our way with people like Brian carrying the message.

*December 2007*

*David B. Cross*

*Director of Program Management*

*Windows Security*

*Microsoft Corporation*

# Introduction

Welcome to *Windows Server 2008 PKI and Certificate Security*. This book provides detailed information about designing and implementing public key infrastructure (PKI) solutions with the Windows Server 2008 certification authority (CA). This book is based on the white papers and guidelines produced by the Microsoft PKI product team and on my experience working with Microsoft Consulting Services and my company's consulting engagements at customer sites over the past five years.

## About This Book

Although you are welcome to read the book from cover to cover, it is divided into three self-contained parts. Each part contains chapters that build on the lessons and practices described within that part. Each chapter ends with a case study that enforces the critical concepts discussed in the chapter, allowing you to validate how well you understand the concepts of the chapter.



**Note** The answers for the case study questions are available in the appendix, "Case Study Questions and Answers" in both the print copy of the book and the eBook, which can be found on the *Windows Server 2008 PKI and Certificate Security* companion CD.

The three parts of this book are the following:

- **Part I, "Foundations of PKI"** Part I provides an overview of cryptography and PKI concepts and culminates with one of the most important chapters in the book, Chapter 3, "Policies and PKI." Part I ensures that you understand the relationship between a PKI and your organization's security policies. Without strong policies and procedures, a PKI is simply a collection of application servers, rather than a mechanism for securing your network and its applications.
- **Part II, "Establishing a PKI"** Part II provides a framework for designing and implementing a PKI within your organization, including detailed information on preparing your Active Directory Domain Services (AD DS) environment and designing and implementing your organization's CA hierarchy. Part II includes information on designing and implementing a CA hierarchy, designing certificate templates, planning deployment of certificates to users and computers, and disaster recovery recommendations. When you complete Part II, you will have a CA hierarchy that is ready to deploy certificates for any PKI-enabled application used by your organization. In addition, this section covers clustering a CA and implementing Online Certificate Status Protocols (OCSPs).

- **Part III, “Deploying Application-Specific Solutions”** Part III provides detailed information on deploying certificates for specific PKI-enabled applications. Each chapter in this section offers details on the types of certificates required for the specific application, recommendations on how to deploy the certificates to the required users and computers, and provides best practices for deploying each PKI-enabled application. New applications have been added in this second edition of the PKI book. The new applications include Microsoft Identity Lifecycle Manager (ILM) 2007, Document Signing, deploying certificates to domain controllers, and Network Device Enrollment Services (NDES). Also, major updates were performed on the chapters covering smart cards and implementing Secure Sockets Layer (SSL) for Web servers.



**Note** Unfortunately, when you write a book, you must consider page count limits. Due to page count, I was unable to include chapters on deploying certificates for Network Access Protection (NAP) and Remote Desktop Protocol (RDP). I have included documentation on these two technologies on the *Windows Server 2008 PKI and Certificate Security* companion CD to provide you with at least some information on these technologies.

## Windows Server 2008 PKI and Certificate Security Companion CD

The companion CD included with this book contains a variety of tools and scripts to help you deploy a Windows Server 2008 PKI and issue certificates to computers running Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.



**Note** The scripts are provided “as is” and serve as examples of how you can use scripts to configure your Windows Server 2008 PKI deployment.

To connect directly to the Microsoft Knowledge Base and enter a query regarding a question or issue you might have, go to <http://www.microsoft.com/learning/support/search.asp>. For issues related to the Windows operating system, please refer to the support information included with your product.

## System Requirements

To use the scripts included on the companion CD-ROM, the following system requirements exist:

1. You can run the scripts included on the companion CD-ROM on a computer running Windows 2000, Windows XP, Windows Vista, Windows Server 2003, or Windows Server 2008. The specific operating system requirements are included in the chapter referencing the script.
2. You can deploy Certificate Services only on a computer running Windows Server 2003 or Windows Server 2008 Standard, Enterprise, and DataCenter editions.
3. A standalone certification authority (CA) in the CA hierarchy should be deployed on a computer running Windows Server 2003 or Windows Server 2008 Standard.
4. An issuing CA should be deployed on a computer running Windows Server 2003 or Windows Server 2008 Enterprise and DataCenter editions.



## Chapter 3

# Policies and PKI

A public key infrastructure (PKI) is only as secure as the policies and procedures that are implemented by an organization in conjunction with its PKI. Three policy documents directly affect the design of an organization's PKI:

- **Security policy** A *security policy* is a document that defines an organization's standards in regard to security. The policy usually includes the assets an organization considers valuable, potential threats to those assets, and, in general terms, measures that must be taken to protect these resources.
- **Certification policy** A *certification policy* (CP) is a document that describes the measures an organization will use to validate the identity of a certificate's subject and for what purposes a certificate following the certificate policy can be used. Validation might require a requestor-provided account and password submitted to the organization's directory, or photo identification and submission to a background check through a registration authority (RA) process.
- **Certification practice statement** A *certification practice statement* (CPS) is a public document that describes how a certification authority (CA) is managed by an organization to uphold its security and certificate policies. A CPS is published at a CA and describes the operation of the CA.

Security policies, certificate policies, and CPSs are typically created by members of an organization's legal, human resources, and information technology (IT) departments. The PKI design must enforce these policies.



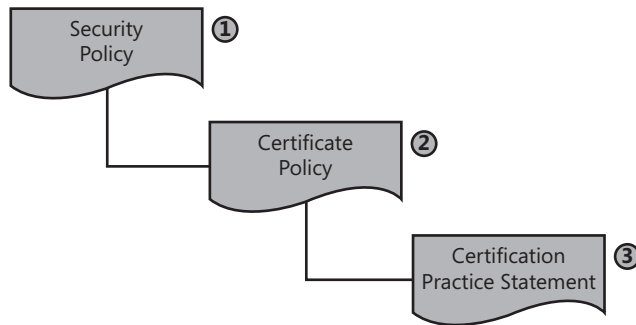
**Warning** Certificate policies and CPSs are used by other organizations to determine how well they trust certificates issued by an organization's CA hierarchy. You trust a certificate from another organization when you allow that certificate to be used on your network for signing or encryption purposes. Deploying a PKI without implementing certificate policies and CPSs can result in a PKI that causes your organization to be deemed untrustworthy by other organizations.

A dependency exists between the security policy, certificate policy, and CPS in a PKI, as shown in Figure 3-1. It operates as follows:

1. An organization first develops a security policy, defining the organization's security standards.



2. Next, a certificate policy is drafted to enforce and reflect the organization's security policy.
3. Finally, the CPS defines the CA's management procedures that enforce the certificate policy.



**Figure 3-1** The dependency between the security policy, certificate policy, and certification practice statement (CPS)



**Note** Security policies, certificate policies, and CPSs are typically legal documents that must be reviewed by an organization's legal department or legal representatives before publication to ensure that the documents are enforceable and do not misrepresent the organization's intent.

## Security Policy

The design of a PKI starts with an inspection of the organization's security policy. A PKI designer uses a security policy to answer the following questions:

- **What data should be secured with certificates?** Not all applications support certificate-based security. Typically, a security policy defines classes of data within the organization and measures that must be taken to protect that data when stored and when transmitted across a network. With a PKI in place, these measures can include the use of protocols such as Secure Sockets Layer (SSL) or Internet Protocol security (IPsec) to protect transmitted data and Encrypting File System (EFS) to protect stored data.
- **What measures must be taken to protect the private keys associated with a certificate?** Measures can include storing the certificate on a smart card, protecting a CA's private key by implementing hardware security modules (HSMs), or preventing the export of a certificate's private key.

## Defining Effective Security Policies

A security policy defines an organization's security standards. An organization typically has several security policy documents that provide comprehensive definitions of security issues, the risks and threats faced by the organization, and the measures that must be taken to protect the organization's data and assets.



**Note** An organization must do more than just define security policies. It must ensure that it deploys security solutions to enforce the security policies, and it must ensure that employees are aware of those security policies and their roles and responsibilities in maintaining security.

Once an organization defines its security policies, an initial assessment must be performed to identify measures that enforce those policies. Once these measures are identified, a *gap analysis* determines whether additional measures should be implemented to meet the defined security policies. After proper planning, the security policy implementation process can begin.

An organization should periodically review its security policies and the measures taken to enforce them to determine if modifications are necessary. Modifications might involve updating security policies or revising the processes and procedures that enforce them.

## Resources for Developing Security Policies

Two of the most commonly used resources for defining a security policy are ISO 27002, "Code of Practice for Information Security Management," and RFC 2196, "The Site Security Handbook."



**Note** The International Standards Organization (ISO) recently renamed ISO 17799 and its predecessor British Standards (BS) 7799. The newly assigned numbers are ISO 27002 (formerly known as ISO 17799) and ISO 27001 (formerly known as BS 7799-2). The rename was initiated by ISO to align the standard under a common naming structure, the ISO 27000 series.

ISO 27002, available for purchase at <http://www.27000-toolkit.com>, provides detailed information and recommendations for developing enforceable security policies. Several Web sites provide security policy samples based on the intent and recommendations of ISO 27002.

RFC 2196, "Site Security Handbook," available at <http://www.ietf.org/rfc/rfc2196.txt>, is another guide for developing security policies. Although directed more toward computer security policies, the RFC describes several types of resources that should be covered in an overall security policy, as well as recommendations for securing those resources.

## Effects of External Policies on Your PKI

As more and more organizations consider using certificates to authenticate, sign, or encrypt communications between their organization and other organizations, external policies are starting to influence your PKI design. To allow exchange and trust of certificates between your organization and a partner organization, you may need to meet the security policies defined in these common standards:

- **Qualified Certificates** A *qualified certificate* (see RFC 3739, “Internet X.509 Public Key Infrastructure Qualified Certificates Profile”) refers to a certificate issued in Europe that is defined to meet the requirements for the European Directive on Electronic Signatures. The primary purpose of a qualified certificate is to identify a person with a high level of assurance.

A qualified certificate can optionally include biometric information, such as the digital image of the subject’s written signature or a digital picture of the subject, to further validate the identity of the certificate subject.

- **Sarbanes-Oxley Act** The Sarbanes-Oxley Act of 2002 (SOX) is a United States federal law that establishes reporting and operations standards for all U.S. public companies or public companies that do business in the United States. The act also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure. The act affects PKI deployments and policies regarding change control and auditing requirements and log maintenance. Likewise, PKI can assist an organization with SOX compliance by supporting initiatives for strong authentication, data encryption, and digital signing.
- **FIPS 201—Personal Identity Verification (PIV) of Federal Employees and Contractors** FIPS 201 is a standard developed by the National Institute of Standards and Technology (NIST) to meet the deadlines set by President George W. Bush in Homeland Security Presidential Directive 12 (HSPD-12). FIPS 201 defines a standard for electronic identification for federal employees and contractors for both physical and logical access control. The standard is made up of two major sections.
  - Part one describes the minimum requirements for a Federal personal identity verification system. The requirements include recommendations for personnel identity proofing, registration, and issuance.
  - Part two provides detailed specifications on storing, processing, and retrieving identity credentials from a two-factor device to allow interoperability between different devices.
- **Federal Bridge Certification Authority (FBCA)** The U.S. government has established a bridge CA to allow organizations participating in the FBCA to accept certificates issued to

other participating organizations in the FBCA. The bridge CA acts as a hub between the relying parties allowing them to trust certificates issued to all participants in the bridge.

To participate in the bridge, an organization must meet the FBCA's certificate policy. To allow flexibility, the original FBCA has evolved into the Federal Public Key Infrastructure Architecture (FBKIA), which supports multiple policies and functions. The policies supported by the FPKIA include the FBCA, the Federal PKI Common Policy Framework (FCPF) CA, and the Citizen and Commerce Class Common (C4) CA.



**Note** Details on the FBCA can be found at <http://www.cio.gov/fbca/>.

- **Certipath** Certipath is another implementation of a bridge CA in the United States. The difference between Certipath and the FBCA is the scope of the bridge. Participants in the Certipath bridge are aerospace and defense industry companies such as Lockheed Martin, Northrop Grumman, and Boeing. In addition to providing trust between other Certipath bridge members, Certipath is also cross-certified with the FBCA. This cross-certification allows all Certipath members to interoperate with all FBCA participants in certificate-based applications.

### Bridge CAs for Business-to-Business (B2B) Trust

As the co-author of the “Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003” white paper for Microsoft (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.msp>), it is exciting to see theory come to life.

When David Cross and I drafted the white paper, we were putting on our visionary hats, discussing a future method of providing certificate trust between organizations. In the ensuing years, Certipath and the FBCA are now in operation and allowing bridge trust between organizations.

The biggest impact I see on customers is the certificate policy requirements for bridge CAs. In some cases, organizations have been forced to establish dedicated CA hierarchies to cross-certify with a bridge CA. Unfortunately, the main reason is that their current CA hierarchy would not pass compliance requirements for the bridge they wish to participate in.

The best advice I can give is that if you see the possibility of participating in the FBCA or another industry bridge, be sure to review the FBCA certificate policy (available at [http://www.cio.gov/fpkipa/documents/FBCA\\_CP\\_RFC3647.pdf](http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf)), and ensure that your PKI design meets these certificate policy requirements.

## Defining PKI-Related Security Policies

Using ISO 27002 as a guide for developing security policies, you should consider updating or creating security policies for the following areas:

- **Organizational security** Establish enforceable security policies for an organization. ISO 27002 is especially helpful when an organization does not have security policies in place prior to starting a PKI design.
- **Organizational security infrastructure** Ensure the existence of security policies that recommend the implementation of a single organization-wide PKI. An organizational PKI is easier to manage than several project-based CAs. For example, an organization should not deploy separate CA implementations for a virtual private network (VPN), Secure/Multipurpose Internet Mail Extensions (S/MIME), and wireless projects. An enterprise PKI that provides certificates for all applications and services is preferred.
- **Asset classification and control** Identify classes of assets that require public key encryption, digital signing, or other PKI-related technologies to ensure security. PKI-related security can be applied to both data storage and transmission.
- **Personnel security** Include job descriptions and requirements for members of the PKI administration team in security policies. Requirements can include mandatory background checks for all administrators, tasks and procedures that must be followed, and any agreements or policies that administrators must sign when accepting their positions.
- **Physical and environmental security** Ensure that the security policy includes requirements for physical security measures to protect CAs and their deployment in a PKI. Different security measures can be required for offline versus online CAs.
- **Communications and operations management** Define managerial and operational roles for your PKI. These can include CA administrators, certificate managers, backup operators, auditors, certificate template designers, and key recovery agents.
- **Access control** Define what measures will be taken to secure access to a CA. These measures might include manually approving Web-based enrollment requests or placing the physical CA in a server room with keycard access. Access control can dictate what forms of authentication are required to access data. For example, some asset classifications can require two-factor authentication (something you have and something you know) before access is permitted.
- **Change control process** Establish what measures will be taken to maintain and modify a PKI after deployment.
- **Business continuity management** Define measures that will ensure recovery of the PKI in the event of a disaster. These measures should include actions to be taken in advance of a catastrophe so that a CA can be recovered, what information must be documented about the CA configuration, and who will perform the recovery.

- **Compliance** Provide recommendations to ensure that the implemented PKI enforces security policies that affect it. Nonconformance with security policies can devalue a PKI-issued certificate to the point that all certificates must be revoked and reissued to ensure compliance and trust of other organizations.

## Certificate Policy

A certificate policy describes the measures taken to validate a certificate's subject prior to certificate issuance and the intended purposes of the certificate. For many organizations, it is the certificate-issuance policy that determines whether the presented certificate will be trusted.

For example, an organization is more likely to trust a certificate issued after a requestor presents photo identification than a certificate issued based on a user knowing an account and password combination.

## Contents of a Certificate Policy

A certificate policy should include the following information:

- **How the user's identity is validated during certificate enrollment** Is identity provided by an account and password combination or must requestors present themselves for face-to-face interviews? If interviews are required, what forms of identification must requestors present for validation?
- **The certificate's intended purpose** Is the certificate used for authentication on the network or for signing purchase orders? If the certificate is used for signing purchase orders, is there a maximum value allowed? These questions should be addressed in the certificate policy.
- **The type of device in which the certificate's private key is stored** Is the private key stored on the computer's local disk in the user's profile, or is the private key stored on a hardware device such as a smart card? Other measures, such as implementing strong private key protection or requiring a password to access the private key, can be included in this information.
- **The subject's responsibility for the private key associated with the certificate in the event that the private key is compromised or lost** Is the user responsible for any actions performed using the acquired private key if the private key is compromised or a backup of the private key is lost? This decision can lead to preventing the archival or export of the private key associated with the certificate.
- **Revocation policies, procedures, and responsibilities** Under what circumstances will your organization revoke an issued certificate before its validity period expires? This decision will determine what actions or events will lead to the revocation of a certificate, how the revocation process is initiated, and who performs the actual revocation procedure.

## Certificate Policy Example

An excellent example of certificate policy is the X.509 Certificate Policy for the U.S. Department of Defense (DoD), available at <http://iase.disa.mil/pki/dod-cp-v90-final-9-feb-05-signed.pdf>.

The DoD defines five classes of certificates in its certificate policy document. The distinction between the various classes is based on the following variables:

- The measures taken to validate the subject's identity
- The value of transactions allowed for a certificate class
- The type of storage required for the private key material

A combination of these three variables leads to the following certificate classes:

- **DoD Class 1** Users must provide a valid e-mail address for communications during the enrollment process. No other validation of the user's identity is performed.
- **DoD Class 2** Users prove identity by providing a user name and password for an account in the organization's authoritative directory. Once a valid user name and password are provided, a certificate is issued. The certificate is typically stored on the hard drive of the computer where the certificate request is generated. A DoD Class 2 certificate can be used for:
  - Digital signatures for administrative data or day-to-day work on any network.
  - Key exchange for high-value data on an encrypted network or confidentiality of low-value information on nonencrypted networks.
- **DoD Class 3** Users prove identity by providing at least one piece of official federal government photo identification or two credentials issued by other entities, with one of the documents being a photo ID (such as a driver's license). The private key associated with the certificate is still stored on the user's hard disk, but the increased subject validation allows the private key to be used for medium-value transactions on a public network.
- **DoD Class 3 Hardware** A DoD Class 3 Hardware certificate uses the same subject validation process as a DoD Class 3 certificate. The difference is that the private key material and certificate are exported from the user's hard disk to a hardware token, such as a USB token. The movement of the private key to a hardware device increases the security of the private key.



**Note** Once the private key is successfully transferred to a hardware device, the private key should be deleted from the computer's hard drive to prevent unauthorized access.

- **DoD Class 4** A DoD Class 4 certificate requires presentation of the same photo identification as the DoD Class 3 and DoD Class 3 Hardware certificates. The difference is that the private key pair is not generated on the local hard disk but on a hardware two-factor device such as a smart card. The increased security of the key pair associated with the certificate results in the certificate being valid for high-value transactions on public networks.
- **DoD Class 5** Currently, there is no PKI that meets the subject-identification requirements for a DoD Class 5 certificate. In the future, a DoD Class 5 certificate will require biometric validation of the certificate's subject. This can include retinal scans, fingerprint matches, or even DNA matching. A DoD Class 5 certificate can be used to secure classified materials on public networks.

The DoD classifications do not assign actual values to low-value, medium-value, or high-value transactions. Rather than providing predetermined values that can become dated, general terms are used to allow value modification without requiring certificate policy modification.

### Comparing Certificate Policies

Sometimes it is valuable to compare different available certificate policies when you are developing the certificate policies for your organization. As mentioned in the section “Federal Bridge Certification Authority (FBCA)” earlier in this chapter, the U.S. FBCA also defines a certificate policy.

When you compare the policies to the DoD certificate policies, you can see a definite similarity between the assurance levels.

The FBCA defines a Rudimentary assurance level that relies on the subscriber providing an e-mail address to receive a certificate. This is very close to the DoD Class 1 definition.

Likewise, the FBCA Low, Medium, and High assurance levels map pretty much one-to-one with the DoD Class 2, DoD Class 3, and DoD Class 4 definitions. This really should not come as a surprise, though. The DoD is one of the organizations participating in the Federal Bridge!

## Certification Practice Statement (CPS)

A certification practice statement (CPS) defines the measures taken to secure CA operations and the management of CA-issued certificates. You can consider a CPS to be an agreement between the organization managing the CA and the people relying on the certificates issued by the CA.



By reviewing a CA's CPS—a public document that should be readily available to all participants—a relying party can determine whether the certificates issued by that CA meet its security requirements. The CPS can contain the following information:

- How the CA will enforce the measures necessary to validate the certificate's subject, as required by the certificate policy
- The liability of the organization in the event that an act of fraud is performed against the service protected by the certificate and the fault is found to be associated with the certificate
- The circumstances under which a certificate can be revoked before its expiration

When a certificate is issued by a CA that follows a CPS, the CA's certificate (or that of its parent CA) can include a URL pointer to the CPS. If included in the CA's certificate, the CPS is viewed by clicking the Issuer Statement button on the General tab of the certificate, as shown in Figure 3-2.



Figure 3-2 A CA certificate that references a CPS



**Note** When a CPS is included in a CA certificate, it is applicable to that CA and all subordinate CAs in the CA hierarchy. This means that the practices defined in the CPS must be implemented by that CA and all subordinate CAs.

RFC 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,” available at <http://www.ietf.org/rfc/rfc3647.txt>, recommends a

standard CPS format to ensure compatibility between organizations and promote a stronger degree of trust of an organization's CPS by other companies. The RFC recommends the following nine sections:

- Introduction
- Publication and Repository Responsibilities
- Identification and Authentication (I&A)
- Certificate Life-Cycle Operational Requirements
- Facility, Management, and Operational Controls
- Technical Security Controls
- Certificate, CRL, and OCSP Profiles
- Compliance Audit and Other Assessment
- Other Business and Legal Matters



**Note** RFC 3647 recommends that the same format be used for both certificate policies and CPSs. The X.509 certificate policies for both the United States Department of Defense and the United States FBCA implement the nine sections discussed here. Differences between the certificate policy and the CPS are mainly related to the documents' focus. A certificate policy focuses on subject validation and is often compared between organizations to find similar policies, whereas a CPS describes the operations of the CA to enforce the implemented certificate policies.

## CPS Section: Introduction

The introduction of a CPS provides an overview of the CA, as well as the types of users, computers, network devices, or services that will receive certificates. The introduction also includes information on certificate usage. This includes what types of applications can consume certificates issued under the CP or CPS and what types of applications are explicitly prohibited from consuming the CA's certificates. If a representative of another organization has any questions regarding the information published in the CPS, the introduction also provides contact information.

## CPS Section: Publication and Repository Responsibilities

The Publication and Repository Responsibilities section contains details regarding who operates the components of the public key infrastructure. This section also describes the responsibilities for publishing the CP or CPS, whether the CP or CPS will be publicly available, whether portions of the CP or CPS will remain private, and descriptions of access controls on published information. The published information includes CPs, CPSs, certificates, certificate status information, and certificate revocation lists (CRLs).

## CPS Section: Identification and Authentication

This section describes the name formats assigned and used in certificates issued by the CA. The section will also specify whether the names must be unique, meaningful, allow nicknames, and so on. The section's main focus is on the measures taken to validate a requestor's identity prior to certificate issuance. The section describes the certificate policy and assurance levels implemented at the CA and details identification procedures for:

- **Initial registration for a certificate** The measures taken to validate the identity of the certificate requestor.
- **Renewal of a certificate** Are the measures used for initial registration repeated when a certificate is renewed? In some cases, possession of an existing certificate and private key is sufficient proof of identity to receive a new certificate at renewal time.
- **Requests for revocation** When a certificate must be revoked, what measures will be taken to ensure that the requestor is authorized to request revocation of a certificate?



**Note** A CA can implement more than one assurance level, so long as the CA's procedures and operations allow enforcement of each assurance level. To implement multiple assurance levels within a certificate policy, separate subsections can be defined, one for each assurance level.

## CPS Section: Certificate Life-Cycle Operational Requirements

This section defines the operating procedures for CA management, issuance of certificates, and management of issued certificates. It is detailed in the description of the management tasks. Operating procedures described in this section can include the following:

- **Certificate application** The application process for each certificate policy supported by a CA should be described. Applications can range from the use of autoenrollment to distribute certificates automatically to users or computers, to a detailed procedure that pends certificate requests until the requestor's identity is proved through ID inspection and background checks.
- **Certificate application processing** Once the application is received by the registration authorities, the application must be processed. This section describes what must be done to ensure that the subscriber is who he says he is. The section can include what forms of identification are required, whether background checks are required, and whether there are time limits set on processing the application. The section may include recommendations on when to approve or deny a request.
- **Certificate issuance** Once the identity of a certificate requestor is validated, what is the procedure to issue the certificate? The process can range from simply issuing the certificate in the CA console to recording the certificate requestor's submitted identification in a separate database maintained by an RA.

- **Certificate acceptance** When a certificate is issued to a computer or user, what procedures must be performed to install the certificate on the user's computer or a certificate-bearing device such as a smart card?
- **Key pair and certificate usage** Once a certificate is issued, the parties involved in the usage of the certificate must understand when and how the certificate may be used. The section describes responsibilities for the certificate subscriber and relying parties when the certificate is used.
- **Certificate renewal** When a certificate reaches its end of lifetime, the certificate can be renewed with the same key pair. The section provides details on when you can renew with the same key pair, who can initiate the request, and what measures must be taken to verify the subscriber's identity (these are typically less stringent than initial enrollment).
- **Certificate re-key** Alternatively, when a certificate reaches its end of lifetime, the certificate can be renewed with a new key pair. The section provides details on when you must renew with a new key pair, who can initiate the request, and what measures must be taken to verify the subscriber's identity (these are typically the same as initial enrollment).



**Note** Setting a schedule for renewal and re-key is an important task in this section. For example, some CPSs allow renewal without re-vetting only for a period of seven years for Medium assurance or DoD Class 3 certificates. The subscriber's identity during renewal is validated by the subscriber signing the request with his or her previous certificate (since the subscriber is the holder of the private key). In the seventh year, the subscriber must re-key and undergo the vetting process to re-establish his or her identity.

- **Certificate modification** Sometimes, a certificate must be re-issued because of the subscriber's name change or change in administrative role. This section describes *when* you can modify a certificate and how the registration process proceeds for the modification of the certificate.



**Note** Technically, it is not a modification. You cannot modify a certificate because it is a signed object. Think of it more as a replacement of a certificate.

- **Certificate revocation and suspension** Under which circumstances will the issuing party revoke or suspend an issued certificate? This section should detail the obligations of the certificate holder, as well as actions that can lead to certificate revocation. The section also includes information on what revocation mechanisms are supported by the CA. If CRLs are used, the section describes the publication schedule for the CRLs. If online revocation and status checking is implemented, the URL of the Web site is provided.
- **Certificate status services** If the CA implements certificate status-checking services, this section provides operational characteristics of the services and the availability of the services.

- **End of subscription** If a subscriber wishes to terminate her or his subscription, this section provides details on how the certificate is revoked. There may be multiple recommendations in this section detailing the different reasons that can require a subscriber to end his or her subscription. For example, an organization may choose to process the revocation request differently for an employee who is terminated than for an employee who retires.
- **Key escrow and recovery** If the CA provides private key escrow services for an encryption certificate, this section describes the policies and practices governing the key archival and recovery procedures. The section typically references other policies and standards defined by the organization.

## CPS Section: Facility, Management, and Operational Controls

This section describes physical, procedural, and personnel controls implemented at the CA for key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving. These controls can range from limiting which personnel can physically access the CA to ensuring that an employee is assigned only a single PKI management role. For a relying party, these controls are critical in the decision to trust certificates because poor procedures can result in a PKI that is more easily compromised without the issuing organization recognizing the compromise.

This section also provides details on other controls implemented in the management of the PKI. These include:

- **Security audit procedures** What actions are audited at the CA, and what managerial roles are capable of reviewing the audit logs for the CA?
- **Records archival** What information is archived by the CA? This can include configuration information as well as information about encryption private keys archived in the CA database. This section should detail the process necessary to recover private key material. For example, if the roles of certificate manager and key recovery agent are separated, a description of the roles and responsibilities of each role should be provided so the certificate holder is aware that a single person cannot perform private key recovery.
- **Key changeover** What is the lifetime of the CA's certificate, and how often is it renewed? This section should detail information about the certificate and its associated key pair. For example, is the key pair changed every time the CA's certificate is renewed or only when the original validity period of the CA certificate elapses?
- **Compromise and disaster recovery** What measures are taken to protect the CA from compromise? Under what circumstances would you decommission the CA rather than restore the CA to the last known good configuration? For example, if the CA is compromised by a computer virus, will you restore the CA to a state before the viral infection and revoke the certificates issued after the viral attack or decommission the CA? If a CA fails, what measures are in place to ensure a quick recovery of the CA and its CA database?

- **CA or RA termination** What actions are taken when the CA or registration authority (RA) is removed from the network? This section can include information about the CA's expected lifetime.

## CPS Section: Technical Security Controls

This section defines the security measures taken by the CA to protect its cryptographic keys and activation data. For example, is the key pair for the CA stored on the local machine profile on a two-factor device, such as a smart card, or on a FIPS 140-2 Level 2 or Level 3 hardware device, such as a hardware security module (HSM)? When a decision is made to trust another organization's certificates, the critical factor is often the security provided for the CA's private key.

This section can also include technical security control information regarding key generation, user validation, certificate revocation, archival of encryption private keys, and auditing.



**Warning** The technical security control section should provide only high-level information to the reader and not serve as a guide to an attacker regarding potential weaknesses in the CA's configuration. For example, is it safe to disclose that the CA's key pair is stored on a FIPS 140-2 Level 2 or Level 3 HSM? It is not safe to describe the CA's management team members or provide specific vendor information about the HSM.

## CPS Section: Certificate, CRL, and OCSP Profiles

This section is used to specify three types of information:

- **Information about the types of certificates issued by the CA** For example, are CA-issued certificates for user authentication, EFS, or code signing?
- **Information about CRL contents** This section should provide information about the version numbers supported for CRLs and what extensions are populated in the CRL objects.
- **OCSP profiles** This section should provide information on what versions of Online Certificate Status Protocol (OCSP) are used (for example, what RFCs are supported by the OCSP implementation) and what OCSP extensions are populated in issued certificates.

## CPS Section: Compliance Audit and Other Assessment

This section is relevant if the CP or CPS is used by a CA that issues certificates that are consumed by entities outside of your organization. The section details what is checked during a compliance audit, how often the compliance audit must be performed, who will perform the audit (is the audit performed by internal audit or by a third party?), what actions must be taken if the CA fails the audit, and who is allowed to inspect the final audit report.

## CPS Section: Other Business and Legal Matters

This section specifies general business and legal matters regarding the CP and CPS. The business matters include fees for services and the financial responsibilities of the participants in the PKI. The section also details legal matters, such as privacy of personal information recorded by the PKI, intellectual property rights, warranties, disclaimers, limitations on liabilities, and indemnities.

Finally, the section describes the practices for maintenance of the CPS. For example, what circumstances drive the modification of the CPS? If the CPS is modified, who approves the recommended changes? In addition, this section should specify how the modified CPS's contents are published and how the public is notified that the contents are modified.



**Note** In some cases, the actual modifications are slight, such as a recommended rewording by an organization's legal department. In these cases, the URL referencing the CPS need not be changed, just the wording of the documents referenced by the URL.

### What If My Current CP/CPS Is Based on RFC 2527?

Many of your organizations may have a CP or CPS based on RFC 2527 (the predecessor to RFC 3647). There is no immediate need to rewrite the CP or CPS to match the section names in RFC 3647. On the other hand, if you are in the process of drafting your CP or CPS now, I do recommend that what you write is based on the section names in RFC 3647.

Either way, RFC 3647 provides a great cheat sheet for you as you start your copy-and-paste adventure. Section 7, "Comparison to RFC 2527," provides a detailed table that shows the mappings between sections in RFC 2527 and RFC 3647. For example, in RFC 2527, compliance auditing is described in Section 2.7 and its subsections. In RFC 3647, the same subsections exist but are now recorded in Section 8. The table below summarizes the remapping of the sections regarding compliance auditing.

Section title	RFC 2527 section	RFC 3647 section
Compliance Audit	2.7	8.
Frequency of Entity Compliance Audit	2.7.1	8.1
Identity/Qualifications of Auditor	2.7.2	8.2
Auditor's Relationship to Audited Party	2.7.3	8.3
Topics Covered by Audit	2.7.4	8.4
Actions Taken as a Result of Deficiency	2.7.5	8.5
Communication of Results	2.7.6	8.6

## Case Study: Planning Policy Documents

You are the head of security for Fabrikam, Inc., a large manufacturing company. Your IT department has several PKI-related initiatives planned for the next 18 months, and you are responsible for the drafting of all related policy documents.

### Design Requirements

One of the applications planned by the IT department is the deployment of smart cards for both local and VPN authentication by all employees. During research for the smart card deployment, the IT department gathered the following information that will affect the policies you draft:

- Each employee will be issued a smart card on his or her first day with Fabrikam, Inc.
- Existing employees will receive their smart cards on an office-by-office basis. Members of the IT department will travel to each major regional office and deliver the smart cards to all employees in that region.
- Fabrikam has a high employee turnover. In any given month, as many as 1,000 employees leave Fabrikam and are replaced with roughly 1,200 new employees.

### Case Study Questions

1. What is the relationship between a CPS, certificate policy, and security policy?
2. In what document would you define the methods used to identify the new hires when they start with Fabrikam?
3. Will the identification validation requirements for existing employees differ from those implemented for new employees of Fabrikam?
4. The high turnover of employees must be addressed in the CPS. Specifically, what sections must be updated to define the measures taken when an employee is terminated or resigns from Fabrikam?
5. You are considering modeling your certificate policies after the United States FBCA certificate policy. What certificate class would best match your deployment of smart cards?

### Additional Information

- Microsoft Official Curriculum, course 2821: “Designing and Managing a Windows Public Key Infrastructure” ([www.microsoft.com/traincert/syllabi/2821afinal.asp](http://www.microsoft.com/traincert/syllabi/2821afinal.asp))
- ISO 27002—“Code of Practice for Information Security Management” (<http://www.27000-toolkit.com>)



- RFC 2196—“The Site Security Handbook” (<http://www.ietf.org/rfc/rfc2196.txt>)
- “X.509 Certificate Policy for the United States Department of Defense” (<http://iase.disa.mil/pki/dod-cp-v90-final-9-feb-05-signed.pdf>)
- RFC 2527—“Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” (<http://www.ietf.org/rfc/rfc2527.txt>)
- RFC 3647—“Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” (<http://www.ietf.org/rfc/rfc3647.txt>)
- The Information Security Policies/Computer Security Policies Directory (<http://www.information-security-policies-and-standards.com>)
- “Homeland Security Presidential Directive (HSPD)–12” (<http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html>)
- “X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)” ([http://www.cio.gov/fpkipa/documents/FBCA\\_CP\\_RFC3647.pdf](http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf))
- “Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003” (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.msp>)
- Certipath (<http://www.certipath.com/>)
- FIPS-201—“Personal Identity Verification (PIV) of Federal Employees and Contractors” (<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>)
- RFC 3739—“Internet X.509 Public Key Infrastructure Qualified Certificates Profile” (<http://www.ietf.org/rfc/rfc3739.txt>)

# Index

## A

- Abstract Syntax Notation One (ASN.1), 214
- access control
  - CA hierarchy, 168–170
  - defining network access policy, 632–633
  - defining VPN policy, 606–607, 616
  - defining wireless user policy, 634–635
  - security policies, 44
  - smart card support, 563
- ACRS (Automatic Certificate Request Settings)
  - best practices, 680
  - Domain Controller certificates, 671
  - functionality, 353, 368
- Active Directory Certificate Services (AD CS). *see also* Certificate Services management pack
  - auditing, 118–120, 184–185
  - backup considerations, 309–310
  - CA configuration measures, 189
  - CA hierarchy requirements, 83, 85
  - certificate manager restrictions, 293
  - certificate templates, 259, 264
  - disaster recovery considerations, 324
  - enterprise root CAs, 142–143
  - installing, 297
  - minimizing risk of failure, 86–87
  - monitoring, 179
  - offline policy CAs, 126–130
  - offline root CAs, 122–123
  - online issuing CAs, 135–139
  - Online Responder service, 217
  - reinstalling, 321–322
  - starting/stopping, 290
  - supported upgrade paths, 151–152
- Active Directory Domain Services (AD DS)
  - analyzing environment, 59–60
  - BDE support, 192
  - CA hierarchy requirements, 93–95
  - certificate enrollment, 352
  - certificate mapping, 496
  - certificate templates, 259, 274
  - CHAP support, 596
  - code signing, 652
  - credential roaming, 376
  - defining mapping, 498–500
  - Domain Controller certificates, 667–668
  - EFS support, 512
  - enterprise CAs, 68
  - failover clustering, 343–344
  - Key Recovery Agent certificates, 465
  - methods of creating trust, 383–384
  - modifying Cert Publishers group scope, 63–67
  - modifying permissions, 65–66
  - ms-PKI-AccountCredentials value, 376
  - ms-PKI-DPAPIMasterKeys value, 376
  - ms-PKI-RoamingTimeStamp value, 376
  - preparing environment, 59
  - publishing certificates and CRLs, 111–113, 133, 244, 297, 406
  - replication latency, 248
  - schema limitations, 104
  - securing e-mail, 589
  - smart card support, 535–538, 562
  - upgrading schemas, 60–63
  - wireless networking, 624
- Active Directory Lightweight Directory Services (AD LDS), 244
- ActiveX controls, 665–666
- AD DS. *see* Active Directory Domain Services
- AD LDS (Active Directory Lightweight Directory Services), 244, 246
- Add Read permission, 220
- Add Roles Wizard, 194, 217
- Administrator template, 259, 264, 385
- Adobe PDF
  - document signing, 659–660
  - verifying signatures, 663
- Advanced EFS Data Recovery (AEFSDR), 527
- Advanced Encryption Standard algorithm. *see* AES algorithm
- AEFSDR (Advanced EFS Data Recovery), 527
- AEP, 202, 288
- AES (Advanced Encryption Standard) algorithm
  - certificate templates, 272
  - CNG support, 16
  - defined, 6
  - EFS support, 511
  - encryption keys, 456–457
  - WPA2 support, 622
- AET SafeSign, 548
- AIA (Authority Information Access)
  - CA certificate distribution points, 117
  - CA configuration files, 105–107, 112
  - CA hierarchy requirements, 90
  - certificate validation, 235, 237
  - choosing CAs for e-mail, 578
  - disaster recovery documentation, 309

- OCSP process, 215–216
- PKI Health Tool support, 170, 172
- publication options, 116
  - smart card logon, 562–563
- AIA container, 172, 172
- AirSnort application, 621
- Alacris idNexus, 413
- Aladdin eToken RTE, 548
- Algorithmic Research, 202
- algorithms
  - asymmetric encryption, 4, 6–9
    - CNG support, 16–17
    - defined, 4
    - digital signing process, 11
    - encryption process, 4
    - hash, 11–13
    - Suite B, 16–17
    - symmetric encryption, 4–6
- All Issuance policies, 399
- AllowPrivateExchangeKeyImport value, 549
- AllowPrivateSignatureKeyImport value, 549
- ambiguous chaining, 242
- American National Standards Institute (ANSI), 104
- ANSI (American National Standards Institute), 104
- application policies
  - bridge CAs, 391
  - certificate templates, 276, 278–283
  - custom, 398
  - defining, 397–398
  - determining OIDs, 397
  - purpose, 397
  - smart cards, 538
  - trusted certificates, 396–397
- applications
  - CA hierarchy requirements, 81–83, 90
  - certifying, 649–651
  - validating digital signatures, 660–663
- arcs, 104–105
- ASN.1 (Abstract Syntax Notation One), 214
- Assign permission, 601
- asymmetric encryption
  - algorithms, 9
    - defined, 3
    - process overview, 6–8
    - symmetric and, 9–10
- asymmetric signing, 8
- Auditor role
  - assigning, 85, 292
  - CIMC security levels, 287
  - implementing, 291
- audits
  - CA hierarchy requirements, 85, 144–146, 189
  - Certificate Services, 118–120, 184–185
  - CLM support, 415
  - CNG support, 13, 120
  - Common Criteria role settings, 287
  - configuring parameters, 290
  - CPS support, 53–54
  - disaster recovery documentation, 308
  - monitoring, 183–185
  - OCSP support, 37, 215
  - Online Responder service, 215, 223–224
  - scripting configuration settings, 190
- Authenticated Session template, 260, 626
- authentication. *see also specific authentication types*
  - best practices, 616, 643
  - certificate templates, 260–262
  - CLM server, 418
  - domain controllers, 667
  - IPsec support, 82
  - Key Recovery Agent certificates, 463
  - MAC filtering, 620
  - preventing other forms, 500–501
  - RADIUS, 172, 563, 597
  - smart card, 539, 541, 563
  - SQL Server, 431, 439
  - two-factor, 535
  - VPN options, 596–597, 600–602
  - Web servers, 476
  - Windows authentication, 439
- Authenticode, 647
- Authority Information Access. *see* AIA (Authority Information Access)
- Authority Information Access extension, 28
- Authority Key Identifier extension, 25, 240–242
- Authorization Agent (clmAuthAgent), 430
- Autoenroll permission
  - certificate enrollment, 353
  - certificate templates, 267, 274
  - Online Responder service, 220
  - RAS and IAS Server certificates, 625
  - User certificates, 628
  - VPN support, 601
  - 802.1x authentication, 626
- Autoenrollment Settings
  - best practices, 680
  - Domain Controller certificates, 671–672
  - EFS support, 509
  - functionality, 368–370
  - Windows 2000 limitations, 353
- automatic certificate enrollment
  - ACRS support, 368
  - Autoenrollment Settings, 368–370
- Automatic Certificate Request Settings. *see* ACRS (Automatic Certificate Request Settings)
- availability. *see* high availability
- Axalto Client Software, 548

**B**

- Backup Operator role
  - assigning, 292
  - CIMC security levels, 287
  - implementing, 291
  - responsibilities, 85
- backups. *see also* disaster recovery
  - CA considerations, 85
  - CA database, 290
  - Certificate Services, 309–310
  - evaluating methods, 323–324
  - high availability considerations, 231–232
  - NDES support, 694–695
  - remote shared folders, 314
- base CRLs
  - caching, 211
  - certificate revocation, 210, 212
  - choosing publication intervals, 248
  - CRL re-signing, 326
  - functionality, 33, 101
  - setting expiration indicator, 168
- Base Smart Card CSP (Microsoft), 535, 548–549, 552, 560
- basic constraints
  - bridge CAs, 391
  - CA configuration files, 102, 107–108
  - defining, 395–396
  - purpose, 395
  - X.509 version 3 certificate, 27
- Basic Constraints extension, 27
- Basic EFS certificates
  - certificate enrollment, 524
  - certificate templates, 260, 264, 510, 522–523
- BDE (BitLocker Disk Encryption), 190–192
- binding certificates, 488–489, 495
- BitLocker Disk Encryption (BDE), 190–192
- BLOB (binary large object), 291, 454
- bridge CAs
  - B2B trust support, 43
  - deployment example, 391–392
  - FBCA, 42–43, 47
  - functionality, 384, 389–390
- bulk encryption. *see* symmetric encryption
- Bulk Issuance Client, 550–551
- Bush, George W., 42

**C**

- C4 certification authority, 43
- CA administrator, 686
  - assigning roles, 292
  - certificate revocation, 210
  - CIMC security levels, 286–287
  - defining alternate, 289
  - implementing, 288–290

- management roles supporting, 296
- responsibilities, 85
- CA configuration files
  - CAPolicy.inf, 100–110
  - manipulating, 290
  - post-installation scripts, 100, 113–121
  - pre-installation scripts, 100, 110–113
- CA Exchange certificates
  - certificate template, 262, 455–456
  - encryption keys, 455–456
- CA hierarchy
  - 32-bit to 64-bit considerations, 152
  - AD DS requirements, 93–95
  - additional information, 400
  - application requirements, 81–83
  - business requirements, 91–92
  - CA configuration measures, 189–192
  - choosing architecture, 80
  - configuring trust, 686
  - determining access, 168–170
  - enabling auditing, 144–146
  - external requirements, 92–93
  - four-tier, 76
  - hardware security modules, 196–202
  - implementing, 99–100
  - organizing issuing CAs, 77–80
  - physical security measures, 192–193
  - security requirements, 83–84
  - single-tier, 73, 103
  - technical requirements, 84–91
  - three-tier, 75–76, 83, 103, 121–141
  - two-tier, 74–75, 135
  - verifying installation, 146
- CA Manager Agent (clmCAMngr), 430
- CA officer, 85
- CA Signature Algorithm field, 22
- CAB files, 647
- caching
  - CRL support, 211, 239–240
  - EFS options, 526
  - Online Responder support, 222
- CAMonitor.vbs script
  - event monitoring, 177–178
  - functionality, 176
  - implementing, 178–179
  - monitoring options, 176
  - notification options, 176–177
- CAPI. *see* CryptoAPI
- CAPI2 events
  - CertGetCertificateChain event, 250
  - CertOpenStore event, 250
  - CertRejectedRevocationInfo event, 250
  - CertVerifyCertificateChainPolicy event, 250
  - CertVerifyRevocation event, 250
  - common errors, 250–253

- correlation, 250
- CryptRetrieveObjectByUrlCache event, 250
- CryptRetrieveObjectByUrlWire event, 250
- X509Objects event, 250
- CAPICOM control, 353, 373–374, 524
- CAPolicy.inf file
  - application policies, 397
  - AuthorityInformationAccess section, 105–107
  - BasicConstraintsExtension section, 107–108
  - best practices, 401–402
  - certsrv\_server section, 108–109
  - ClockSkewMinutes option, 109
  - creating, 102
  - CRLDeltaOverlapPeriod option, 108
  - CRLDeltaOverlapUnits option, 109
  - CRLDeltaPeriod option, 108
  - CRLDeltaPeriodUnits option, 108
  - CRLDistributionPoint section, 105–107
  - CRLOverlapPeriod option, 108
  - CRLOverlapUnits option, 108
  - CRLPeriod option, 108
  - CRLPeriodUnits option, 108
  - disaster recovery documentation, 309
  - DiscreteSignatureAlgorithm option, 109
  - EnhancedKeyUsageExtension section, 107–106
  - enterprise root CAs, 141–142
  - file sections, 103–104
  - functionality, 100
  - information provided, 100–102
  - LoadDefaultTemplates option, 109
  - name constraints, 395
  - Notice line, 105
  - object identifiers, 103–105
  - offline policy CAs, 125–126
  - offline root CAs, 121–122
  - online issuing CAs, 134–135
  - PolicyStatementExtension section, 103
  - RenewalKeyLength option, 108
  - RenewalValidityPeriod option, 108
  - RenewalValidityPeriodUnits option, 108
  - sample contents, 102–103
  - Version section, 103
- card module, 548–549
- CAs (certification authorities)
  - auditing, 118–120
  - C4, 43
  - certificate chaining, 112
  - choosing for e-mail, 578–579
  - choosing key lengths, 89
  - CLM support, 427
  - configuring, 217–219
  - CPS support, 39
  - defining connection strings, 438–439
  - defining PKI management staff, 84–85
  - deploying enterprise CAs, 68
  - disaster recovery documentation, 308
  - FCPF, 43
  - Federal Bridge Certification Authority, 42–43
  - functionality, 29
  - hierarchical organization, 29–30
  - HSM deployment methods, 197–201
  - implementing NDES servers, 689–690
  - issuing, 21
  - key archival support, 465–466
  - locking down, 189
  - minimizing server roles, 189
  - monitoring script, 176–179
  - PKI Health Tool support, 168–170
  - protecting private keys, 83
  - publication point options, 90
  - reading configuration information, 289
  - renewing certificates, 24
  - securing private keys, 193
  - Suite B algorithms, 17
  - third-party, 672–676
  - upgrade considerations, 152–154
  - Web Server certificates, 478–479
- case sensitivity, 243
- CDP container, 171
- CDP (CRL Distribution Point)
  - CA administrator, 288
  - CA configuration files, 105–107
  - CA hierarchy requirements, 90–91
  - certificate validation, 237
  - choosing CAs for e-mail, 578
  - choosing publication points, 246
  - failover clustering, 341–342
  - PKI Health Tool support, 171
  - smart cards, 536, 562–563
- centralized registration model, 424–425
- CEP (Certificate Enrollment Protocol), 261
- CEP Encryption certificates, 260, 689, 695
- Cert Publishers group, 63–67
- Certenroll.dll, 353, 362, 374
- certificate-based authentication
  - connecting to Web sites, 503–504
  - creating certificate templates, 497–498
  - defining certificate mapping, 496–497
  - defining mapping in AD DS, 498–500
  - enabling Windows Server 2003, 500–501
  - enabling Windows Server 2008, 501–503
  - overview, 495–496
  - Web client certificate, 478
- certificate chains
  - ambiguous chaining, 242
  - building, 240–243
  - CA configuration files, 100, 112
  - certificate validation, 235–236, 243
  - evaluating exact match, 241
  - evaluating key match, 241–242

- evaluating name match, 242-243
- troubleshooting, 249, 255
- Web Server certificates, 494-495, 507
- X.509 certificates, 24, 26, 28
- certificate enrollment
  - automatic process, 367-374
  - certificate templates, 260, 263
  - choosing enrollment method, 354-355
  - credential roaming, 374-378
  - EFS support, 523-524
  - manual process, 357-367
  - methods supported, 352-354
  - performing, 447-449
  - publishing certificate templates, 355-357
  - RAS and IAS Server template, 627
  - SCEP process, 684-687
  - scripting, 353, 371-374, 628
  - signing certificates, 652-653
  - SPC support, 649-650
- Certificate Enrollment Control, 353, 373
- Certificate Enrollment Protocol (CEP), 261
- Certificate Enrollment Wizard
  - limitations, 524
  - pending requests, 459
  - requesting certificates, 357-358
  - signing certificates, 653
  - Web server requirements, 353
- Certificate Export Wizard, 462
- Certificate Import Wizard, 469
- Certificate Issuing and Management Components.
  - see* CIMC (Certificate Issuing and Management Components)
- Certificate Lifecycle Manager. *see* CLM (Certificate Lifecycle Manager)
- Certificate Lifecycle Manager Client, 419, 549-550
- Certificate Lifecycle Manager service
  - configuring, 435-436
  - functionality, 435
- Certificate Management Protocol, 405
- Certificate Manager, 85
- certificate managers
  - assigning roles, 292
  - best practices, 531
  - certificate revocation, 210
  - certificate templates, 276
  - Certutil utility, 468
  - CIMC security levels, 286-287
  - defining, 289
  - defining restrictions, 289
  - implementing, 290-291
  - implementing restrictions, 293-294
  - key archival, 454
  - key recovery, 457, 468
  - KRA role and, 301, 464
  - logging activity, 290
  - responsibilities, 85, 296, 415
  - restricting, 543
  - signing certificates, 653
- certificate mapping
  - defining in AD DS, 498-500
  - enabling Windows Server 2003, 500
  - enabling Windows Server 2008, 501-503
  - explicit, 495, 499-500
  - implicit, 496, 498
  - many-to-one mapping, 496-497
  - one-to-one mapping, 496-497
  - process overview, 495-496
  - smart card requirements, 537
- certificate policies
  - All Issuance policies, 399
  - based on RFC 2527, 54
  - bridge CAs, 392
  - CA configuration files, 103
  - comparing, 47
  - contents, 45
  - custom, 400
  - default, 399-400
  - defined, 39, 45, 398
  - dependencies, 39-40
  - digital signatures, 650-651
  - European Qualified Certificate, 399
  - example, 46-47
  - High Assurance policy, 399
  - implementing, 400-401
  - Low Assurance policy, 399
  - Medium Assurance policy, 399
  - Secure Signature Creation Device Qualified Certificate, 399
- Certificate Policies extension, 26
- Certificate Renewal function, 435
- Certificate Request Control, 374
- Certificate Request Wizard, 273, 464
- certificate requests
  - Certificate Enrollment Wizard, 357-360
  - Certificate Services Web Enrollment pages, 360-362, 364, 459
  - Certificates console, 372-373
  - completing pending, 362-364
  - creating, 675-676
  - enabling SAN extension, 675
  - Key Recovery Agent certificate, 464
  - reviewing, 365-367
  - SCEP process, 686-687
  - submitting, 364-365
  - Web Enrollment method, 360-362
  - Web Server certificates, 484-488, 490-493
  - Windows Internet Explorer, 459-460
- certificate revocation. *see also* CRLs (certificate revocation lists)
  - AffiliationChanged reason code, 34, 207

- CA administrators, 290
- CACompromise reason code, 34, 207
- certificate managers, 291
- certificate validation, 236–238
- CertificateHold reason code, 34, 207
- CessationOfOperation reason code, 34, 208
- checking in Windows Internet Explorer, 476–478
- CLM support, 415
- delta CRLs, 212
- enrollment considerations, 370
- identifying revoked certificates, 210–211
- KeyCompromise reason code, 34, 208
- managing configurations, 225–229
- OCSP support, 211–213, 215
- performing, 210, 449
- publication intervals, 247–248
- purpose, 207
- RemoveFromCRL reason code, 35, 208
- revocation policy, 208–209
- revocation reasons, 34–35, 207–208
- Superseded reason code, 34, 208
- timing, 207
- troubleshooting, 254–255
- Unspecified reason code, 35, 208
- Certificate Services. *see* Active Directory Certificate Services
- Certificate Services management pack
  - available views, 180–181
  - components, 179
  - Computer Groups node elements, 179–180
  - deploying, 182–183
  - functionality, 179
  - importing, 183
  - operations, 183
  - rule groups and rules, 180
  - verifying communications, 183
- Certificate Services Web Enrollment pages
  - best practices, 568
  - certificate requests, 360–362, 364, 459
  - deploying e-mail, 584
  - functionality, 352
  - signing certificates, 653
  - VPN support, 602
  - wireless networking, 629
- certificate stores
  - selecting certificates, 226
  - viewing, 174–175
- certificate subscribers, 415
- Certificate Template Manager role
  - creating OIDs, 299
  - creating templates, 298–299
  - delegating certificate permissions, 299–300
  - editing certificate templates, 300
  - responsibilities, 298
- certificate templates
  - additional information, 259
  - Autoenrollment Settings, 369
  - best practices, 282–283, 665
  - certificate enrollment, 356, 361
  - certificate mapping, 497–498
  - Certificate Services support, 259
  - CLM permissions, 417
  - CLM server, 430
  - code signing, 260, 442, 651–652
  - configuring response signing, 219–222
  - Cryptography tab, 271–273
  - custom, 433
  - default, 263–264
  - defining permissions, 440
  - delegating permissions, 298–300
  - disaster recovery documentation, 308
  - document signing, 652
  - domain controller, 667–670
  - e-mail support, 579–583
  - editing, 300
  - enrolling certificates, 263
  - Extensions tab, 277–283
  - General tab, 267–269, 580–581, 583
  - Insurance Requirements tab, 275–276
  - key archival support, 458, 466–467
  - key recovery, 463
  - modifying, 265, 297
  - modifying version 1 permissions, 265–266
  - modifying version 2 permissions, 266–271
  - modifying version 3 permissions, 266–267, 271–283
  - obtaining forest's private OID, 105
  - online blocks, 560
  - as profile template component, 414
  - publishing for enrollment, 355–357
  - registration models, 423–425
  - Request Handling tab, 269–273, 369, 580–581, 583
  - Security tab, 265–267, 369, 580
  - smart cards, 261, 269, 283, 537–538, 540–542, 554
  - Subject Name tab, 273–275, 580
  - Superseded Templates tab, 277
  - upgrading, 156
  - version 1, 259–261, 263, 265–266, 651
  - version 2, 261–262, 266–271, 356, 483, 541, 651–652
  - version 3, 262–263, 266–267, 271–283, 356
  - VPN support, 600–602
- certificate trust list. *see* CTL (certificate trust list)
- certificate validation
  - additional information, 235
  - building certificate chains, 240–243

- CAPI diagnostics, 249–255
- certificate discovery, 235
- changing default behavior, 238–240
- component testing, 236–237
- designing object publication, 243–248
- path validation, 235
- process overview, 235–240
- revocation checking, 236–238
- certificates. *see* digital certificates
- Certificates console, 357–359, 372–373, 464
- certification authorities. *see* CAs (certification authorities)
- Certification Authorities container, 171, 175
- Certification Authority console, 315–316, 468
- certification practice statement. *see* CPS (certification practice statement)
- CertifyID Guardian, 324
- Certipath, 43, 56, 391
- CertMgr.exe tool, 655
- certreq.exe utility, 353, 371–372, 404, 676
- Cert2spc.exe tool, 654
- Certutil.exe utility
  - benefits using, 100
  - best practices, 680
  - CA certificate distribution points, 117
  - certificate templates, 264
  - certificate validity periods, 118
  - checking certificate validity, 172–174
  - choosing auditing behavior, 287
  - clearing in-memory cache, 240
  - configuration naming context, 113–114
  - configuring audit parameters, 290
  - CRL distribution points, 116–117
  - CRL publication intervals, 114
  - CRL re-signing, 326
  - cross certification with constraints, 405
  - deleting CA database records, 289
  - enabling auditing for CAs, 120
  - enforcing role separation, 192, 295
  - enterprise root CAs, 144
  - failover clustering, 335, 342–343, 346
  - functionality, 165, 172
  - internal root CAs, 674
  - key archival support, 456
  - key recovery support, 468–469
  - NTAuthCertificates object, 674
  - offline policy CAs, 130–131
  - offline root CAs, 124–125
  - online issuing CAs, 140–141
  - performing manual backups, 311, 315–317
  - publishing certificates, 406
  - removing certificates, 678
  - replacing certificates, 678
  - restoring manual backups, 323
  - reviewing certificate requests, 365
  - scripting certificate template publishing, 357
  - scripting configuration settings, 190
  - subordinate CAs, 674
  - verifying certificate constraints, 406
  - verifying certificates, 677–678
  - viewing certificate stores, 174–175
- ChainCacheResynchFiletime value, 239
- CHAP (Challenge Handshake Authentication Protocol), 596
- CIFS (Common Internet File System), 245
- CMC (Certificate Issuing and Management Components)
  - Security Level 1, 286
  - Security Level 2, 286
  - Security Level 3, 286–287
  - Security Level 4, 287–288
- ciphertext
  - asymmetric signing, 8
  - defined, 5
  - encryption process, 4–5
  - symmetric encryption, 9
- Cisco IOS, 354, 685
- Cisco VPN 3000 series, 89
- Client Authentication certificates
  - application policies, 391
  - domain controllers, 668–669
  - EAP-TLS support, 624
  - logon process and, 626
- Client Computer certificate, 599, 622
- client/server model
  - CNG support, 17
  - implementing SSL, 482–483
  - VPN client, 610–613
  - VPN server, 608–610
- CLM Agent (clmAgent), 429–430, 471
- CLM Audit permission, 415, 427
- CLM (Certificate Lifecycle Manager). *see also* ILM (Identity Lifecycle Manager)
  - background, 413
  - best practices, 451–452
  - CA component installation, 436–439
  - centralized registration model, 424–425
  - certificate templates, 276
  - CLM roles, 415
  - configuring server, 429–436
  - custom workflows, 354
  - deploying code signing certificates, 439–449
  - deployment components, 417–419
  - disaster recovery, 324
  - HSM support, 431
  - identifying management policies, 419–421
  - installing server, 426–428
  - key recovery, 470–471
  - manager-initiated registration model, 423–424
  - permission assignment locations, 416–417



- planning deployment, 419
  - profile templates, 414
  - self-service registration model, 422–423
  - supported permissions, 415–416
- CLM Configuration Wizard, 429, 432–435
- CLM Enroll permission, 415–417, 427
- CLM Enrollment Agent permission, 415, 427
- CLM Exit module, 419, 431, 438
- CLM External SQL API, 435
- CLM Policy module, 419, 431, 437
- CLM Request Enroll permission, 415–417, 427
- CLM Request Recover permission, 415, 427
- CLM Request Renew permission, 415, 427
- CLM Request Revoke permission, 415, 427
- CLM Request Unblock Smart Card permission, 415, 427
- CLM roles, 415
- CLM server
  - agent accounts, 429–430
  - agent certificates, 430
  - Certificate Lifecycle Manager service, 435–436
  - CLM Configuration Wizard, 432–435
  - functionality, 418
  - hardware requirements, 426
  - infrastructure requirements, 427
  - installing, 428
  - preparing schemas, 427–428
  - SMTP server, 432
  - software requirements, 426
  - SQL Server authentication, 431
- CMAK (Connection Manager Administration Kit), 610
- CMC (Cryptographic Message Syntax), 405, 456, 676
- CNG (Cryptography Next Generation)
  - algorithms supported, 16–17
  - auditing support, 13, 120
  - certificate templates, 262, 273
  - changing hash algorithms, 159
  - defined, 3, 13
  - e-mail support, 580
  - encryption keys, 14–16, 455–456
  - features, 13–16
  - key recovery, 469
  - NDES support, 692
  - schema support, 60
  - smart card support, 538, 541
  - supported clients/applications, 17
- code signing
  - Authenticode, 647
  - best practices, 665–666
  - certificate templates, 260, 442, 651–652
  - defined, 647
  - functionality, 647–648
  - performing, 654–657
  - validating digital signatures, 660–663
- Code Signing certificates
  - best practices, 665–666
  - CA hierarchy requirements, 82
  - certificate templates, 260, 442, 651–652
  - certificate validation, 237
  - certifying applications, 649–651
  - creating profile templates, 440–447
  - defining permissions, 440
  - deploying, 651–654
  - Enroll management policy, 441–444
  - executing management policies, 447–449
  - Revoke management policy, 444–447
- commercial CAs
  - choosing for e-mail, 578
  - root CAs, 383, 387
  - signing certificates, 649–650, 665
  - Web Server certificates, 479, 489
- Common Criteria roles
  - assigning, 291–293
  - auditing settings, 287
  - CIMC Security Level 1, 286
  - CIMC Security Level 2, 286
  - CIMC Security Level 3, 286–287
  - CIMC Security Level 4, 287–288
  - disaster recovery considerations, 309
  - enforcing role separation, 85, 295–296, 697
  - holding multiple, 285
  - Windows implementation, 288–291
  - X.509 standard, 285
- Common Internet File System (CIFS), 245
- common root CAs
  - commercial root CAs, 383, 387
  - functionality, 383, 386
  - umbrella groups, 387
- Computer certificate
  - certificate templates, 260, 264
  - deploying, 627–628
  - permissions, 626
- Computer Groups node (Operations Manager 2007), 179–180
- Connection Manager, 610
- Connection Manager Administration Kit (CMAK), 610
- cookies, 363
- CPS (certification practice statement)
  - based on RFC 2527, 54
  - CA configuration files, 101, 103
  - Certificate, CRL, and OCSP Profiles section, 53
  - Certificate Life-Cycle Operational Requirements section, 50–52
  - Compliance Audit and Other Assessment section, 53
  - contents, 48
  - defined, 39, 47
  - dependencies, 39–40
  - Facility, Management, and Operational Controls section, 52–53

- format recommendation, 48–49
- Identification and Authentication section, 50
- Introduction section, 49
- OID support, 103
- Other Business and Legal Matters section, 54
- Publication and Repository Responsibilities section, 49
- Technical Security Controls section, 53
- three-tier CA hierarchy, 76
- viewing, 48
- Web Server certificates, 479
- credential roaming, 374–378, 584
- CRL Distribution Point. *see* CDP (CRL Distribution Point)
- CRL Distribution Points extension, 28
- CRL Sign extension, 26
- CRLs (certificate revocation lists). *see also* certificate revocation
  - additional information, 235
  - availability options, 326–327
  - base CRLs, 33
  - bridge CAs, 390
  - CA configuration files, 100–101
  - CA hierarchy requirements, 89
  - CA monitoring script, 176–177
  - caching considerations, 211, 239–240
  - certificate policies, 45
  - certificate validation, 236, 238
  - choosing publication points, 245
  - CSP support, 53
  - defined, 28, 33
  - delta CRLs, 33–34
  - disaster recovery, 307, 309
  - distribution point options, 116–117
  - examining stores, 170–172
  - failover clustering, 342–343
  - latency problems, 211
  - logging changes, 290
  - managing, 29
  - manipulating schedules, 289
  - OCSP support, 35–37
  - PKI Health Tool support, 170
  - publication intervals, 114, 248
  - publication point options, 114–116, 244–245
  - publishing to AD DS, 111–113, 133, 297
  - publishing to local computer store, 110–111
  - publishing updated, 120
  - re-signing, 326–327
  - single-tier CA hierarchy, 74
  - smart card limitations, 194
  - SSL support, 476–478
  - troubleshooting, 254
  - types, 33–34
- Cross, David, 43
- Cross Certification Authority certificate
  - acquiring partner's certificate, 404
  - basic constraints, 395–396
  - best practices, 401–402
  - bridge CAs, 391
  - creating trust between organizations, 384, 387–389, 391–392
  - generating, 403, 405
  - name constraints, 395
  - Policy.inf file, 404
  - submitting request, 405
  - verifying constraints, 406–407
- Cross Certification Authority template
  - defining settings, 278
  - publishing, 403
  - purpose, 262
  - signature requirements, 402
- Cross Certification Signing template
  - creating, 286
  - functionality, 402
  - publishing, 403
- crypt\_archivable flag, 453, 458, 467
- CryptoAPI
  - cached CRLs, 211
  - CertGetCertificateChain event, 250
  - certificate discovery, 235
  - certificate enrollment, 353, 373
  - certificate policies, 401
  - CertOpenStore event, 250
  - CertRejectedRevocationInfo event, 250
  - CertVerifyCertificateChainPolicy event, 250
  - CertVerifyRevocation event, 250
  - changing hash algorithms, 158–159
  - common errors, 250–253
  - CryptRetrieveObjectByUrlCache event, 250
  - CryptRetrieveObjectByUrlWire event, 250
  - e-mail support, 580
  - enabling diagnostics, 249
  - monitoring overview, 249–250
  - OCSP process, 216
  - SHA-1 support, 242
  - smart card support, 535
  - supported CAPI2 events, 249–250
  - X509Objects event, 250
- Cryptographic Message Syntax (CMC), 405, 455–457, 676
- cryptographic service providers. *see* CSPs (cryptographic service providers)
- cryptography. *see also* CNG; encryption; PKCS (Public Key Cryptography Standards)
  - certificate templates, 271–273
  - cryptographic agility, 13
  - digital signing of data, 11–13
  - Microsoft Strong Cryptographic Provider, 84
- Cryptography Next Generation. *see* CNG (Cryptography Next Generation)
- CSPs (cryptographic service providers)
  - best practices, 665

- CA configuration files, 101
- certificate enrollment, 351, 361, 652
- Certificate Lifecycle Manager Client, 419
- certificate templates, 270–271
- changing hash algorithms, 159
- disaster recovery documentation, 309
- document signing, 652
- e-mail support, 580
- key archival, 458, 467
- Microsoft Strong Cryptographic Provider, 84
- PIN support, 84, 194
- private key support, 84, 194
- random number generators, 16
- signing certificates, 656
- smart card support, 535, 538, 548–549
- VPN support, 600
- Web Server certificates, 485
- wireless networking, 628
- CTL (certificate trust list)
  - certificate validation, 237
  - defining, 384–385
  - functionality, 383–384
- ctool.vbs script, 374

## D

- DACL (discretionary access control list), 263, 625
- Daemen, Joan, 6
- Data Decryption Field (DDF), 511, 514
- Data Encipherment extension, 26
- data encryption. *see* encryption
- Data Encryption Standard (DES) algorithm, 5
- Data Encryption Standard XORed (DESX) algorithm, 5, 511
- Data Encryption Toolkit for Mobile PCs, 527
- Data Key ID Works software, 550
- Data Protection API. *see* DPAPI (Data Protection API)
- data recovery. *see also* disaster recovery; key recovery
  - Advanced EFS Data Recovery, 527
  - best practices, 531
  - CA considerations, 85
  - CA database, 290
  - EFS support, 514–519
  - high availability considerations, 231–232
  - NDES support, 694–695
- data recovery agent (DRA), 512, 517–519
- Data Recovery Field (DRF), 512
- Datacard SP35 printing station, 550
- Datacard SP55 printing station, 550
- Datacard SP75 printing station, 550
- DCOM (Distributed Component Object Model), 176, 373, 454, 687
- DDF (Data Decryption Field), 511, 514
- Decipher Only extension, 26
- decryption. *see* encryption

- dedicated HSMs
  - choosing, 201–202
  - deployment methods, 198–200
  - functionality, 196
- DefaultPrivateKeyLenBits value, 549
- delegated registration model, 470
- delta CRLs
  - caching, 211
  - certificate revocation, 212
  - choosing publication intervals, 247–248
  - choosing publication points, 245
  - CRL re-signing, 326
  - functionality, 33–34, 101
  - identifying revoked certificates, 210
  - setting expiration indicator, 168
- Department of Defense (DoD), 46–47
- DES (Data Encryption Standard) algorithm, 5
- DESX (Data Encryption Standard XORed) algorithm, 5, 511
- device administrators, 685–687, 689
- Diffie-Hellman key agreement, 9, 16, 478
- digest, 11
- digital certificates
  - authentication support, 495–496
  - binding to Web sites, 488–489, 495
  - cache entries, 223
  - checking validity, 172–174
  - choosing publication points, 264
  - contents, 21
  - defined, 21
  - delegating permissions, 299–300
  - deploying, 221
  - deploying smart cards, 539
  - deploying VPNs, 595–600
  - determining access, 168–170
  - determining validity periods, 87–88
  - EAP-TLS requirements, 622–623
  - forcing propagation, 113
  - identifying recipients, 82–83
  - importing, 226–227, 518
  - Issuer field, 240, 243
  - issuing, 84, 351–352
  - NDES recovery, 695
  - organizing issues CAs, 77
  - preventing self-signed, 510
  - public keys, 3
  - publication point options, 114–117
  - publishing to AD DS, 111–113, 133, 297
  - publishing to local computer store, 110–111
  - qualified, 42
  - removing, 678
  - renewing, 24, 221–222, 295–297, 370
  - replacing, 678
  - security policies, 40

- Serial Number field, 240
- smart card requirements, 536–538
- SSL support, 478
- Subject field, 240, 496
- validity periods, 117–118, 237
- verifying, 677–678
- wireless networking, 627–629
  - 802.1x authentication, 622–626
  - X.509 version 1, 22–23
  - X.509 version 2, 23–24
  - X.509 version 3, 21, 24–29
- Digital Signature Algorithm. *see* DSA (Digital Signature Algorithm)
- Digital Signature extension, 26
- digital signatures. *see also* code signing; document signing
  - applying, 648
  - CA hierarchy requirements, 81
  - certificate templates, 260–261, 269
  - certificate validation, 237
  - hash algorithms, 11–13
  - process overview, 11
  - S/MIME process, 571–573, 588
  - security policies, 44, 647
  - Turkish Electronic Signature Law, 399
  - verifying, 648, 660–663
- Directive 1999/93/EC, 399
- Directory Email Replication template
  - Autoenrollment Settings, 389
  - Domain Controller certificates, 668–669
  - functionality, 262
  - issuance policies, 264
- directory name, 393
- Disable management policy, 420
- disaster recovery
  - Certificate Services failure, 324
  - choosing backup method, 309–310
  - determining backup versions, 318–319
  - developing required documentation, 308–309
  - evaluating backup methods, 323–324
  - failed services, 307
  - hardware failure, 307, 324
  - high availability, 326–327
  - HSM backups, 318
  - manual backups, 311, 315–317, 321–323
  - NDES support, 694–695
  - network infrastructure failure, 307
  - restoring backups, 319–323
  - server replacement, 324–325
  - system state backups, 310–312, 319
  - Windows server backups, 310, 312–315, 319–321
- discrete signatures
  - certificate templates, 273
  - defined, 109
  - implementing, 160
  - RSA support, 109
- discretionary access control list (DACL), 263, 625
- disk partitioning, 309
- Distributed Component Object Model (DCOM), 176, 373, 454, 687
- DLL files, 647
- DNS (Domain Name System)
  - certificate templates, 275
  - failover clustering, 344–345
  - ISA requirements, 483
  - LDAP support, 244
  - name constraint format, 393
  - SSL support, 476
  - VPN support, 598–600
  - Web Server certificates, 507
  - X.509 certificates, 27
- document signing
  - best practices, 665–666
  - certificate templates, 652
  - defined, 647
  - functionality, 648–649
  - performing, 657–660
  - validating digital signatures, 660–663
- Document Signing certificates
  - Adobe PDF, 659–660
  - best practices, 665–666
  - certificate templates, 652
  - certifying applications, 649–651
  - contents, 657
  - deploying, 651–654
  - Microsoft Office 2007, 658
- DoD (Department of Defense), 46–47
- Domain Admins group
  - AD DS requirements, 94
  - private key storage, 194
  - Read/Enroll permissions, 403
  - role overview, 296–297
  - updating schemas, 63
- Domain Controller Authentication template
  - Autoenrollment Settings, 389
  - Domain Controller certificates, 668–669
  - functionality, 262
  - issuance policies, 264
- Domain Controller certificates
  - best practices, 680
  - deploying, 671–672
  - functionality, 667
  - history, 667–669
  - managing, 677–678
  - Windows Server 2008 support, 670
- Domain Controller template, 260, 264
- domain controllers
  - CAs in other forests, 672–676
  - certificate templates, 260, 262
  - replicating schemas, 63

- smart cards, 537
  - third-party CAs, 672–676
  - upgrading, 59
  - Domain Name System. *see* DNS (Domain Name System)
  - domains
    - analyzing AD environment, 59
    - CA hierarchy requirements, 94–95
    - EFS data recovery, 516
    - issuing Web Server certificates, 484–489
  - DPAPI (Data Protection API)
    - Advanced EFS Data Recovery, 527
    - certificate policies, 398
    - credential roaming, 374–375
    - private key support, 352
  - DRA (data recovery agent), 512, 517–519
  - DRF (Data Recovery Field), 512
  - DSA (Digital Signature Algorithm)
    - certificate templates, 272
    - CNG support, 16
    - credential roaming, 375
    - defined, 9
  - Dun and Bradstreet rating, 649
  - Duplicate management policy, 420
- E**
- e-mail
    - best practices, 592
    - CA hierarchy requirements, 81
    - certificate templates, 261–262, 274
    - choosing certificate templates, 579–583
    - choosing certification authorities, 578–579
    - choosing deployment methods, 583–585
    - Domain Controller certificates, 667
      - between domain controllers, 667
      - name constraint formats, 394
      - S/MIME support, 571–574
      - securing, 571, 585–589
      - SSL ports, 575
      - SSL support, 574–578
    - EAP (Extensible Authentication Protocol), 596, 623–624
    - EAP-TLS authentication
      - best practices, 643
      - certificate requirements, 622–623
      - defined, 622
      - smart card support, 563
      - VPN support, 596, 600, 613
      - wireless networking, 622, 624
      - 802.1x authentication, 624
    - ECC (Elliptic Curve Cryptography)
      - certificate roaming, 375
      - certificate templates, 262
      - key recovery, 469
      - smart card limitations, 538
    - EFS Certificate Configuration Updater, 527
    - EFS (Encrypting File System)
      - best practices, 531–532
      - CA hierarchy requirements, 81
      - certificate enrollment, 523–524
      - certificate templates, 259–260, 283, 520–523
      - choosing encryption certificates, 510
      - CNG support, 17
      - data recovery, 514–519
      - decryption support, 513–514
      - disabling, 520
      - enabling, 519–520
      - functionality, 509
      - GPO support, 94
      - key recovery, 516, 519
      - local encryption process, 510–512
      - management features, 524–527
      - OID support, 509–510
      - organizing issues CAs, 78–79
      - remote encryption, 512–513
      - securing e-mail, 582
      - security policies, 40
    - EFS Recovery Agent certificate
      - best practices, 532
      - certificate enrollment, 523
      - certificate templates, 260, 264, 515, 521
      - defining agents, 517–519
      - importing, 518
      - obtaining, 517
      - securing private keys, 516, 518–519
    - EKU (Enhanced Key Usage)
      - application policies, 397
      - CA configuration files, 101, 107–106
      - certificate-based authentication, 495
      - certificate templates, 278
      - CTL support, 383
      - defining OCSP signing options, 228
      - Domain Controller certificates, 668
      - EFS support, 510
      - identifying certificate recipients, 82
      - Kerberos Authentication certificates, 669
      - key archival, 458
      - NDES support, 689
      - Online Responder service, 215
      - smart cards, 536
      - SSTP support, 600
      - Web Server certificates, 478
    - electronic signatures. *see* digital signatures
    - Elliptic Curve Cryptography. *see* ECC (Elliptic Curve Cryptography)
    - Encapsulating Security Payload (ESP), 598
    - Encipher Only extension, 26

- Encrypting File System. *see* EFS (Encrypting File System)
- encryption. *see also* key archival; private keys; public keys; symmetric encryption
  - algorithms, 4
  - asymmetric encryption, 3, 6–10
  - bulk, 5
  - certificate enrollment, 361
  - certificate templates, 269–270, 273, 279
  - choosing lengths, 89
  - CNG support, 14–16
  - credential roaming, 375
  - defined, 4
  - digital certificates, 21
  - disaster recovery documentation, 309
  - e-mail support, 573–574
  - HTTP limitations, 475
  - key recovery, 453–454, 457–458, 468–471
  - L2TP limitations, 598
  - process overview, 4
  - security policies, 44
  - wireless networks, 621
  - WPA support, 621
- EncryptionTemplate value, 690, 693
- EnforcePassword value, 692
- Enhanced Key Usage. *see* EKU (Enhanced Key Usage)
- Enhanced Key Usage extension, 28, 538
- Enroll management policy, 420, 441–444
- Enroll permission
  - CA Exchange certificates, 456
  - certificate enrollment, 353
  - certificate templates, 266, 440
  - CLM support, 417
  - Code Signing certificates, 650
  - creating trust between organizations, 402–403
  - deploying e-mail, 584
  - Key Recovery Agent certificates, 459
  - NDES support, 685, 689
  - RAS and IAS Server certificates, 625
  - User certificates, 628
  - VPN support, 601
  - Web Server certificates, 483–484
    - 802.1x authentication, 626
- enrollment, certificate. *see* certificate enrollment
- Enrollment Agent certificates
  - certificate templates, 260, 540
  - deploying smart cards, 539–540, 544–545
- Enrollment Agent (Computers) template, 260
- enrollment agents
  - assigning role, 301
  - best practices, 696
  - certificate templates, 260
  - CLM support, 415, 430
  - defining restrictions, 289
  - responsibilities, 300
  - restricting, 542
  - smart cards, 538
- Enrollment Services container, 171
- enroll.vbs script, 374, 584, 628
- Enterprise Admins group
  - Certificate Templates console, 105
  - installing Certificate Services, 136
  - private key storage, 194
  - Read/Enroll permissions, 403
  - role overview, 297
- enterprise CAs
  - certificate mapping, 498
  - certificate templates, 263
  - defined, 68
  - Domain Controller certificates, 667
  - implementing, 141–144
  - key archival, 465
  - Key Recovery Tool, 468
  - NDES support, 685
  - selecting certificates, 226
  - single-tier CA hierarchy, 73
  - smart cards, 537
  - three-tier CA hierarchy, 75
  - validity periods, 118
  - Web Server certificates, 483, 485
- enterprise root CAs
  - CAPolicy.inf file, 141–142
  - Certificate Services, 142–143
  - post-installation configuration, 144
- Enterprise Trust container, 384
- Error event, 180
- error handling. *see also* troubleshooting
  - CERT\_TRUST\_IS\_CYCLIC error flag, 251
  - CERT\_TRUST\_IS\_NOT\_SIGNATURE\_VALID error flag, 251
  - CERT\_TRUST\_IS\_NOT\_TIME\_VALID error flag, 251
  - CERT\_TRUST\_IS\_NOT\_VALID\_FOR\_USAGE error flag, 251
  - CERT\_TRUST\_IS\_OFFLINE\_REVOCATION error flag, 251
  - CERT\_TRUST\_IS\_PARTIAL\_CHAIN error flag, 251
  - CERT\_TRUST\_IS\_REVOCATION\_UNKNOWN error flag, 251
  - CERT\_TRUST\_IS\_REVOKED error flag, 251
  - CERT\_TRUST\_IS\_UNTRUSTED\_ROOT error flag, 251
  - connection strings, 439
  - httpStatusCode field, 251
  - PKI Health Tool, 170
- ESP (Encapsulating Security Payload), 598

European Qualified Certificate, 399  
 EV (Extended Validation) certificate, 479  
 event monitoring, 177–178, 183–185  
 Exchange Enrollment Agent certificates, 260, 689, 695  
 Exchange Signature Only template, 260, 579, 581  
 Exchange User template, 261, 579, 582  
 Exclusive OR (XOR) function, 5  
 EXE files, 647  
 exit modules, configuring, 288–289  
 explicit mapping, 495, 499–500  
 exporting  
   Key Recovery Agent certificates, 461–462  
   private keys, 270, 361, 458, 461–462, 467  
 Extended Validation (EV) certificate, 479  
 Extensible Authentication Protocol (EAP), 596, 623–624

## F

failover clustering  
   AD configuration, 343–344  
   clustering guidelines, 327–328  
   configuring cluster, 339–341  
   creating cluster, 338–339  
   creating CRL objects, 342–343  
   defined, 327  
   installing, 337  
   installing first node, 330–334  
   installing second node, 334–336  
   modifying CDP, 341–342  
   modifying DNS name, 344–345  
   preparing environment, 328–330  
   testing, 345–346  
   validating configuration, 337–338  
 FBCA (Federal Bridge Certification Authority), 42–43, 47  
 FCPF certification authority, 43  
 Federal Bridge Certification Authority (FBCA), 42–43, 47  
 Federal Information Processing Standards (FIPS), 13, 16  
 Federal Public Key Infrastructure Architecture (FPKIA), 43  
 File Encryption Key (FEK), 511, 514  
 File Transfer Protocol (FTP), 394  
 FIPS 140-1 standard, 288  
 FIPS 140-2 standard, 83, 196, 198  
 FIPS 201 standard, 42, 56  
 FIPS (Federal Information Processing Standards), 13, 16  
 firewalls  
   Certificate Services management pack, 182  
   configuring rules, 182  
   ISA alternatives, 481

forests  
   analyzing AD environment, 59  
   CAs in, 672–676  
   certificates for RADIUS servers, 625  
   declaring configuration naming context, 113–114  
   Web Server certificates, 490  
 FPKIA (Federal Public Key Infrastructure Architecture), 43  
 Freshest CRL extension, 28  
 FTP (File Transfer Protocol), 394  
 Full Control permission, 266

## G

Galois message authentication code (GMAC), 16  
 gap analysis, 41  
 Gemplus GemSafe, 548  
 GeneralPurposeTemplate value, 686, 690, 693  
 Generic Routing Encapsulation (GRE), 595  
 GMAC (Galois message authentication code), 16  
 GPOs (Group Policy Objects)  
   ACRS support, 671  
   AD naming conventions, 94  
   Autoenrollment Settings, 389  
   best practices, 569  
   CA hierarchy requirements, 85  
   certificate validation, 238  
   CTL support, 384  
   deploying certificates, 627  
   EFS Recovery Agent certificates, 518  
   securing e-mail, 582  
   smart card support, 563  
   timeout issues, 253  
   802.1x authentication, 626  
 gpupdate command, 113  
 GRE (Generic Routing Encapsulation), 595  
 Group Policy  
   Autoenrollment Settings, 353, 368–370  
   best practices, 643  
   credential roaming, 376–378  
   defining CTLs, 384  
   defining smart card removal behavior, 563–564  
   defining smart card settings, 564–565  
   EFS support, 524–526  
   wireless networking, 640–641  
   802.1x authentication, 640–641  
 Group Policy Objects. *see* GPOs (Group Policy Objects)  
 groups  
   CLM permissions, 417  
   Code Signing certificates, 442  
   EFS data recovery, 516–517  
   online blocks, 560  
   registration models, 422, 424–425  
   smart cards, 554  
 groupType attribute, 67

**H**

hardware security module. *see* HSM (hardware security module)

hash algorithms

- certificate templates, 273
- changing for CNG CSP, 159
- changing for CryptoAPI version, 158–159
- CNG support, 17
- commonly used, 11
- defining OCSP signing options, 228
- digital signing and, 12–13
- process overview, 11

hash value, 11, 383

High Assurance policy, 399, 650

high availability. *see also* failover clustering

- disaster recovery, 326–327
- Online Responder service, 230–232

Howard, Michael, 649

HSM (hardware security module)

- backing up data, 318
- CA hierarchy security, 196–202
- categories, 196–197
- certificate policies, 398
- choosing, 201–202
- CLM server support, 431
- defining OCSP signing options, 228
- deployment methods, 197–201
- disaster recovery, 307
- failing over, 327
- functionality, 84, 196
- points of failure, 200–201
- private key storage, 192, 195

HSPD-12, 42, 56

HTTP GET method, 216

HTTP (Hypertext Transfer Protocol)

- CA configuration files, 105
- CA publication points, 90, 133–134, 244–245
- common errors, 251–252
- CRL re-signing, 327
- CRL support, 28
- encryption limitations, 475
- httpStatusCode field, 251
- name constraint formats, 394
- OCSP support, 36, 214

HTTP POST method, 216

HTTPS (Hypertext Transfer Protocol Secure)

- ISA support, 483
- OCSP support, 36
- SSL support, 475, 478
- SSTP support, 599

httpStatusCode field, 251

Hurst, Ryan, 36, 214

Hypertext Transfer Protocol. *see* HTTP (Hypertext Transfer Protocol)

Hypertext Transfer Protocol Secure. *see* HTTPS (Hypertext Transfer Protocol Secure)

**I**

IANA (Internet Assigned Numbers Authority), 104

IAS (Internet Authentication Service), 262, 603

ICEnroll interface, 373

ICertRequest2 COM interface, 374

Identity Lifecycle Manager. *see* ILM (Identity Lifecycle Manager)

IEEE 802.1x standard. *see* 802.1x authentication

IIS (Internet Information Services)

- CA hierarchy requirements, 83
- certificate-based authentication, 497, 500–501
- NDES support, 687
- OCSP support, 214
- offline root CAs, 122
- Web Server certificates, 483, 486, 490

IKE (Internet Key Exchange), 599

ILM (Identity Lifecycle Manager). *see also* CLM (Certificate Lifecycle Manager)

- best practices, 451–452, 474, 568
- CA component installation, 436–439
- centralized registration model, 424–425
- certificate templates, 276
- choosing KRA number to use, 466
- configuring server, 429–436
- custom workflows, 354
- deploying code signing certificates, 439–449
- deploying e-mail, 585
- disaster recovery, 324
- evaluation version, 427
- identifying management policies, 419–421
- installing server, 426–428
- key recovery, 470–471
- manager-initiated registration model, 423–424
- planning deployment, 419
- self-service registration model, 422–423
- signing certificates, 650
- smart card alternative options, 559–562
- smart card installation requirements, 547–551
- smart card profile templates, 551–559

IMAP4 (Internet Message Access Protocol), 574–575

implicit mapping, 496, 498

importing

- certificates from files, 226–227
- EFS Recovery Agent certificates, 518
- private keys, 469

Inhibit Any Policy extension, 28

initialization vector (IV), 621

intermediate CA, 31–32

International Organization for Standardization (ISO), 104



International Telecommunication Union (ITU), 104  
 Internet Assigned Numbers Authority (IANA), 104  
 Internet Authentication Service (IAS), 262, 603  
 Internet Explorer. *see* Windows Internet Explorer  
 Internet Information Services. *see* IIS (Internet Information Services)  
 Internet Key Exchange (IKE), 599  
 Internet Message Access Protocol (IMAP4), 574–575  
 Internet Protocol (IP), 27, 599  
 Internet Protocol security. *see* IPsec (Internet Protocol security)  
 Internet Security and Acceleration. *see* ISA (Internet Security and Acceleration)  
 Internet Server API (ISAPI), 214, 222, 683  
 Internetwork Operating System (IOS), 354, 685  
 IOCSAdmin interface, 225  
 IOCSRequestD interface, 225  
 IOS (Internetwork Operating System), 354, 685  
 IP addresses, 394, 483  
 IP (Internet Protocol), 27, 599  
 IPsec (Internet Protocol security)  
   authentication support, 82, 602  
   CA hierarchy requirements, 81  
   CA support, 29  
   certificate enrollment, 354  
   certificate templates, 261, 283  
   CNG support, 14, 17  
   ESP support, 598  
   SCEP process, 685  
   security policies, 40  
   wireless encryption, 621  
 IPsec template, 261, 602, 696  
 ISA (Internet Security and Acceleration)  
   OCSP support, 214  
   with server publishing, 481  
   with Web publishing, 481–483  
 ISAPI (Internet Server API), 214, 222, 683  
 ISO 17799/BS 7799, 41, 44  
 ISO (International Organization for Standardization), 104  
 ISO-ITU-T tree, 104  
 issuance policies, 276, 652  
 Issue and Manage Certificates permission  
   certificate managers, 85, 293  
   certificate revocation, 207  
   issuing CAs, 210  
 Issuer Alternative Name extension, 27  
 Issuer Name field, 22  
 Issuer Unique ID field, 24  
 issuing CAs  
   defined, 33  
   four-tier CA hierarchy, 76  
   implementing online, 132–141  
 Issue and Manage Certificates permission, 210

monitoring script, 176–179  
 organizing, 77–80  
 three-tier CA hierarchy, 75  
 two-tier CA hierarchy, 74–75  
 ITU (International Telecommunication Union), 104  
 IV (initialization vector), 621

**J**

JAR files, 647  
 Java applications  
   code signing, 647  
   key length support, 89

**K**

KDC (Kerberos Distribution Center), 669–670, 680  
 Kerberos authentication  
   CNG support, 17  
   enabling delegation, 434  
   smart card support, 535–536  
 Kerberos Authentication certificates  
   Autoenrollment Settings, 389  
   best practices, 680  
   certificate templates, 262, 264, 283, 669  
   domain controller support, 670  
 Kerberos Distribution Center (KDC), 669–670, 680  
 kernel mode, 14  
 Key Agreement extension, 26  
 key and name match, 241  
 key archival  
   AES support, 456–457  
   best practices, 473–474  
   CA Exchange certificates, 455–456  
   certificate templates, 466–467  
   CNG support, 455–456  
   defining key recovery agents, 459–464  
   enabling CAs, 465–466, 579  
   process overview, 454  
   requirements, 458–459  
   roles supported, 454  
   security policies, 453–454  
 Key Cert Sign extension, 26  
 Key Encipherment extension, 26  
 Key Management Service (KMS), 22, 260  
 key recovery  
   best practices, 473–474, 531  
   Certutil support, 468–469  
   custom certificate templates, 463  
   EFS support, 516, 519  
   ILM support, 470–471  
   process overview, 457–458  
   roles supported, 454  
   security policies, 453–454  
 key recovery agent. *see* KRA (key recovery agent)

- Key Recovery Agent certificates
    - best practices, 473, 531
    - certificate enrollment, 523
    - certificate templates, 262, 459, 521
    - choosing KRA number, 466
    - exporting, 461–462
    - installing, 461, 464
    - smart card-based, 463–464
    - software-based, 459–462
  - Key Recovery Tool, 468
  - key service provider (KSP), 13, 120
  - Key Usage extension, 26
  - KMS (Key Management Service), 22, 260
  - KRA container, 171
  - KRA (key recovery agent)
    - assigning role, 301–302
    - CA monitoring script, 176, 178
    - certificate managers, 291, 301, 464
    - certificate templates, 262, 278
    - Certutil utility, 468
    - choosing number to use, 466
    - CLM server support, 430
    - defining, 289, 459–464
    - deploying smart card-based certificates, 463–464
    - deploying software-based certificates, 459–462
    - key archival, 454, 458
    - key recovery, 457, 468–469
    - KRA container, 171
    - responsibilities, 301
  - KSP (key service provider), 13, 120
- L**
- latency, 211, 248
  - Layer 2 Tunneling Protocol (L2TP), 82, 598–599
  - Layer Two Forwarding (L2F), 598
  - LDAP Data Interchange Format (LDIF), 62
  - LDAP (Lightweight Directory Access Protocol)
    - certificate templates, 274
    - common errors, 252
    - Domain Controller certificates, 667
    - name constraints, 394
    - publication point options, 90, 244–245
    - X.509 certificates, 27–28
  - LDAP/S (Secure LDAP), 667–669
  - LDIF (LDAP Data Interchange Format), 62
  - LeBlanc, David, 649
  - legacy applications, 16
  - L2F (Layer Two Forwarding), 598
  - Lightweight Directory Access Protocol. *see* LDAP (Lightweight Directory Access Protocol)
  - local Administrators group
    - analyzing AD environment, 59
    - CA hierarchy requirements, 84, 95
    - configuring Online Responder service, 222
    - failover clustering, 345
    - installing Certificate Services, 136
    - installing PKI Health Tool, 166
    - limiting membership, 192, 194
    - private key storage, 194
    - publishing to local computer store, 110
    - role overview, 296–297
    - Web Server certificates, 484
  - local machine store
    - identifying certificate recipients, 82
    - private key storage, 193–194
    - publishing root CA certificate, 132
    - Web Server certificates, 494–495
  - local registration authority (LRA), 538
  - local security authority (LSA)
    - CNG support, 15
    - EFS support, 511, 514–515
  - Low Assurance policy, 399
  - LRA (local registration authority), 538
  - LSA (local security authority)
    - CNG support, 15
    - EFS support, 511, 514–515
  - L2TP (Layer 2 Tunneling Protocol), 82, 598–599
- M**
- MAC addresses, 620
  - MAC filtering, 620
  - Makecert.exe tool, 654
  - MakeCTL.exe tool, 654
  - Manage AD Containers dialog box, 170–172
  - Manage CA permissions, 210, 217
  - Manage Online Responder permission, 225, 227
  - management policies
    - CLM support, 417
    - Code Signing certificates, 442–444, 447–449
    - Disable management policy, 420
    - Duplicate management policy, 420
    - Enroll management policy, 420, 441–444
    - identifying, 419–421
    - Offline Unblock management policy, 420
    - online blocks, 560
    - Online Updates management policy, 420
    - as profile template component, 414
    - Recover on Behalf management policy, 420
    - Recovery management policy, 420
    - registration models, 423–425
    - Renew management policy, 421
    - Replace management policy, 421
    - Retire management policy, 421
    - Revoke management policy, 421, 444–447
    - smart cards, 554–557
    - Suspend and Reinstate management policy, 421
    - Temporary Cards management policy, 421
    - Unblock management policy, 421

manager-initiated registration model, 423–424

manual backups

- choosing, 311
- HSM backups, 318
- performing, 315–317
- restoring, 321–323

manual certificate enrollment

- Certificate Enrollment Wizard, 357–360
- completing pending requests, 362–364
- submitting certificate requests, 364–365
- Web Enrollment method, 360–362

many-to-one certificate mapping, 496–497

mapping, certificate. *see* certificate mapping

master boot record (MBR), 191

MBR (master boot record), 191

MD5 (Message Digest 5) algorithm

- certificate templates, 273
- CHAP support, 596
- defined, 11
- NDES support, 684

Medium Assurance policy, 399, 650

message digest, 11

Message Digest 5 algorithm. *see* MD5 (Message Digest 5) algorithm

message integrity check (MIC), 621

MIC (message integrity check), 621

Microsoft Base Smart Card CSP, 535, 548–549, 552, 560

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), 596

Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2), 596, 613, 623

Microsoft Enhanced Cryptographic Provider, 651

Microsoft Exchange Server, 575

Microsoft Identity Integration Server (MIIS), 413

Microsoft Identity Lifecycle Manager. *see* ILM (Identity Lifecycle Manager)

Microsoft Internet Explorer. *see* Windows Internet Explorer

Microsoft .NET Framework, 550

Microsoft Office

- best practices, 665
- document signing, 658
- verifying signatures, 662

Microsoft Point-to-Point Encryption (MPPE), 595

Microsoft SQL Server

- authentication, 431, 439
- CLM server support, 427
- creating logins, 437–438

Microsoft Strong Cryptographic Provider, 84

Microsoft Trust List Signing certificate, 385

Microsoft Visual Basic for Applications, 656–657

MIIS (Microsoft Identity Integration Server), 413

mini-driver, 548–549

monitoring script for CAs, 176–179

MPPE (Microsoft Point-to-Point Encryption), 595

MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 596

MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2), 596, 613, 623

ms-Clm-Data attribute, 427

ms-Clm-Profile-Template class, 427

ms-Clm-Service-Connection-Point class, 427

MSI files, 647

MSP files, 647

## N

name constraints

- bridge CAs, 391
- defining, 394–395
- formats supported, 392–394
- processing, 393
- purpose, 392
- X.509 version 3 certificate, 27

Name Constraints extension, 27

naming conventions, 94

National Institute of Standards and Technology (NIST), 6, 42

Native Windows Tools, 568

nCipher, 202, 318, 654

NDES Administration Web portal, 692

NDES (Network Device Enrollment Services)

- best practices, 696–697
- CEP Encryption certificates, 260
- certificate enrollment, 684–687
- clustering limitations, 327
- configuring, 692–695
- functionality, 354
- history, 683–684
- implementing servers, 687–692
- new features, 683–684
- SCEP support, 683

network-attached HSMs

- choosing, 201–202
- deployment methods, 198–200
- functionality, 197

network interface card (NIC), 620

network load balancing, 480–481

Network News Transfer Protocol (NNTP), 574–575

Network Policy Server. *see* NPS (Network Policy Server)

Network Service account, 214, 220, 684

networks. *see also* wireless networking

- common retrieval errors, 250–253
- infrastructure failures, 307

NIC (network interface card), 620

- NIST (National Institute of Standards and Technology), 6, 42
  - NLB clusters, 480–481
  - NNTP (Network News Transfer Protocol), 574–575
  - non-repudiation, 11
  - Non-Repudiation extension, 26
  - nonce extension, 228
  - Nortel Contivity devices, 89
  - NPS (Network Policy Server)
    - configuring, 603–608
    - RADIUS support, 624, 627, 629
    - smart card support, 563
  - NSA (National Security Agency), 16
  - NTAuth object, 536
  - NTAuthCertificates object
    - Certutil support, 175
    - defining, 674
    - PKI Health Tool support, 172
- O**
- object identifiers. *see* OIDs (object identifiers)
  - OCSP (Online Certificate Status Protocol). *see also*
    - Online Responder service
    - auditing support, 37, 215
    - CA hierarchy requirements, 89
    - caching considerations, 239–240
    - certificate revocation, 211–213, 215
    - certificate templates, 263, 279
    - certificate validation, 236–238
    - components, 213
    - configuring from command line, 219
    - CSP support, 53
    - functionality, 35, 214–215
    - OCSP client, 36, 213
    - process overview, 215–216
    - publication point options, 246
    - revocation providers, 215
    - schema support, 60
    - signing responses, 215, 219–222
    - troubleshooting, 254–255
    - Web proxy cache, 214
  - OCX files, 647
  - offline CAs
    - disaster recovery considerations, 324
    - HSM deployment methods, 199–200
  - offline policy CAs
    - CAPolicy.inf file, 125–126
    - Certificate Services, 126–130
    - post-installation configuration, 130–131
    - pre-installation configuration, 125
  - offline root CAs
    - creating CAPolicy.inf file, 121–122
    - installing Certificate Services, 122–123
    - post-installation configuration, 124–125
  - Offline Unblock management policy, 420
  - offline unblocks, 560–562
  - OIDs (object identifiers)
    - additional information, 400
    - application policies, 397
    - CA configuration files, 103
    - certificate policies, 400–401
    - certificate templates, 276, 278
    - certificate validation, 236
    - CTL support, 383
    - defined, 25, 104
    - delegating permissions, 299
    - document signing, 652
    - EFS support, 509–510
    - identifying certificate recipients, 82
    - key archival, 458
    - obtaining, 104–105
    - Web Server certificates, 478
    - X.509 certificates, 26–28
  - one-to-one certificate mapping, 496–497
  - online CAs
    - disaster recovery considerations, 323
    - HSM deployment methods, 199–200
    - Web Server certificates, 485
  - Online Certificate Status Protocol. *see* OCSP (Online Certificate Status Protocol)
  - online issuing CAs
    - CAPolicy.inf file, 134–135
    - Certificate Services, 135–139
    - post-installation configuration, 139–141
    - pre-installation configuration, 132–134
  - Online Responder service
    - auditing support, 215, 223–224
    - autoenroll permission, 220
    - certificate revocation, 215, 247
    - configuring, 222–225
    - configuring CAs, 217–219
    - configuring certificate templates, 219–222
    - default virtual directory, 219
    - high availability, 230–232
    - high availability support, 230–232
    - installing, 217
    - managing revocation configurations, 225–229
    - Network Service privileges, 220
    - process overview, 36–37, 214–216
    - revocation providers, 215
    - schema support, 60
    - security settings, 224–225
    - signing, 215
    - Web proxy settings, 214, 222–223
  - online unblocks, 560
  - Online Updates function, 435
  - Online Updates management policy, 420
  - operating systems
    - certificate enrollment constraints, 356
    - certificate revocation, 237

- key recovery, 453
- publication intervals, 248
- Operations Manager 2007, 179–180
- Operations Manager Agent, 182
- organizational units (OUs), 95
- Outlook 2003, 585–586
- Outlook 2007, 580, 586–588
- OWA, 588

## P

- PAP (Password Authentication Protocol), 596
- parent CAs, 31
- Password Authentication Protocol (PAP), 596
- passwords
  - agent accounts, 429
  - BDE support, 192
  - NDES support, 684
  - one-time, 420
  - PKCS #12 considerations, 462
  - private keys, 194, 582
  - SCEP process, 685
- path validation
  - CAPI2 events, 249–250
  - CERT\_TRUST\_IS\_CYCLIC error flag, 251
  - CERT\_TRUST\_IS\_NOT\_SIGNATURE\_VALID error flag, 251
  - CERT\_TRUST\_IS\_NOT\_TIME\_VALID error flag, 251
  - CERT\_TRUST\_IS\_NOT\_VALID\_FOR\_USAGE error flag, 251
  - CERT\_TRUST\_IS\_OFFLINE\_REVOCATION error flag, 251
  - CERT\_TRUST\_IS\_PARTIAL\_CHAIN error flag, 251
  - CERT\_TRUST\_IS\_REVOCATION\_UNKNOWN error flag, 251
  - CERT\_TRUST\_IS\_REVOKED error flag, 251
  - CERT\_TRUST\_IS\_UNTRUSTED\_ROOT error flag, 251
  - common errors, 250–251
  - defined, 235
- PCI (Peripheral Component Interconnect), 196
- PCI-X (PCI-Extended), 196
- PEAP (Protected EAP), 622–624, 643
- perimeter network, 93, 245, 256
- Peripheral Component Interconnect -Extended (PCI-X), 196
- Peripheral Component Interconnect (PCI), 196
- permissions. *see also specific permissions*
  - centralized registration model, 425
  - certificate mapping, 496
  - certificate template version 1, 265–266
  - certificate template version 2, 266–271

- certificate template version 3, 266–267, 271–283
- CLM supported, 415–417
- Code Signing certificates, 440
- creating certificate templates, 298–299
- creating OIDs, 299
- defining for smart cards, 554
- disaster recovery documentation, 308
- Enroll management policy, 442
- Issue and Manage Certificates, 85, 207, 210, 293
- manager-initiated registration model, 423–424
- modifying CA, 290
- modifying in Active Directory, 65–66
- NDES implementation, 688–689
- offline unblocks, 561
- online blocks, 560
- Revoke policy, 445
- self-service registration model, 422–423
- verifying, 210
- VPN support, 601
- Write, 265–266
- personal identification number. *see* PIN (personal identification number)
- Personal Identity Verification (PIV), 42
- Personal Information Protection and Electronic Documents Act (Canada), 92
- PIN (personal identification number)
  - best practices, 569
  - CSP support, 84, 194
  - smart cards, 415, 463, 538, 544–545, 552–553, 656
  - TPM chips, 191
  - two-factor authentication, 535
  - unblocking, 559–562
- Pintool.exe program, 562
- PIV (Personal Identity Verification), 42
- PKCS (Public Key Cryptography Standards)
  - additional information, 304
  - certificate requests, 364, 367
  - discrete signatures, 109, 160
  - exporting certificates, 461
  - importing private keys, 469
  - key recover, 519
  - KRA support, 301, 458
  - password considerations, 462
  - private keys, 192
  - SCEP support, 683
  - Web Server certificates, 489, 494–495
- PKI Health Tool
  - defining global options, 167–168
  - error handling, 170
  - functionality, 165–166
  - installing, 166–167
- PKINIT (Public Key Initialization), 536, 538, 670

- Point-to-Point Tunneling Protocol (PPTP), 82, 595–597
  - policy CAs
    - functionality, 31–32
    - offline, 125–131
    - three-tier CA hierarchy, 75
  - Policy Constraints extension, 28
  - Policy Mappings extension, 27
  - Policy.inf file
    - application policies, 397
    - best practices, 401–402
    - certificate policies, 400
    - implementing, 404
    - name constraints, 395
  - POP3 (Post Office Protocol version 3), 574–575
  - PPTP (Point-to-Point Tunneling Protocol), 82, 595–598
  - private CAs, 578–579
  - Private Key Usage Period extension, 26
  - private keys
    - asymmetric encryption, 6–8
    - best practices, 531
    - CA configuration files, 108
    - CA Exchange certificates, 456
    - certificate enrollment, 352
    - certificate mapping, 496
    - certificate policies, 45, 399
    - certificate templates, 262, 270
    - certificate validation, 237
    - CRL reasons, 34
    - crypto folder paths, 15
    - CSP support, 84
    - digital certificates, 21
    - DPAPI support, 352
    - e-mail support, 582
    - EFS Recovery Agent certificate, 516, 518–519
    - exporting, 270, 361, 458, 461–462, 467
    - failover clustering, 333–335
    - importing, 469
    - key archival, 467
    - key recovery, 453–454, 468
    - Key Recovery Agent certificates, 459
    - Network Service access, 220–221
    - passwords, 194, 582
    - protecting, 83, 463
    - retrieving, 290–291
    - SCEP process, 685
    - security considerations, 3, 40, 193
    - smart cards, 536–538
    - stored on HSMs, 192
    - stored on local machine store, 193–194
    - stored on smart cards, 194, 649
    - symmetric encryption, 10
    - Web Server certificates, 481
    - profile templates
      - best practices, 569
      - CLM permissions, 417
      - Code Signing certificates, 442
      - components, 414
      - creating, 440
      - creating for smart cards, 551
      - defining details, 440–441, 551–553
      - Enroll management policy, 441–444
      - online blocks, 560
      - registration models, 422, 424–425
      - smart card enrollment definition, 553–557
  - Protected EAP (PEAP), 622–624
  - Proxy Requests permission, 225
  - proxy servers, 252
  - Public Key Cryptography Standards. *see* PKCS (Public Key Cryptography Standards)
  - Public Key Initialization (PKINIT), 536, 538, 670
  - public keys
    - asymmetric encryption, 6–8
    - CA configuration files, 108
    - CA Exchange certificates, 456
    - certificate enrollment, 352
    - digital certificates, 3, 21
    - FPKIA support, 43
    - retrieving, 10
    - SCEP process, 685
    - symmetric encryption, 10
  - publication intervals
    - choosing, 247–248
    - CRL support, 114
  - publication points
    - certificate and CRL support, 114–117, 244–245, 264
    - choosing, 245–246
    - HTTP support, 90, 133–134, 244–245
    - LDAP support, 90, 244–245
    - OCSP support, 246
    - SSL restrictions, 244
    - troubleshooting, 248
- ## Q
- qualified certificates, 42, 60
  - Qualified Subordination application policy, 402
- ## R
- RA (registration authority)
    - Alacris idNexus, 413
    - certificate enrollment, 354
    - certificate policies, 39
    - certificate templates, 260
    - CNG limitations, 692

- local registration authority, 538
- SCEP process, 684
- RADIUS (Remote Authentication Dial-In User Service)
  - best practices, 616
  - deploying certificates, 627
  - NTAuthCertificates object, 172
  - PEAP support, 623
  - smart card support, 563
  - user certificates, 626
  - VPN support, 597, 604–608
  - WPA support, 622
  - 802.1x authentication, 623–625, 629–635
- random number generators, 16
- RAS and IAS Server template
  - best practices, 616
  - certificate enrollment, 627
  - functionality, 262
  - RADIUS server, 604–605
  - VPN server authentication, 601–602
  - wireless networking, 624–626
- RAS (Remote Access Service), 262
- RC2 algorithm, 6
- RC4 algorithm, 6, 620
- Read & Execute permission, 514
- Read NTFS permission, 514
- Read permission
  - CA Exchange certificates, 456
  - certificate enrollment, 353
  - certificate templates, 265–266, 440
  - CLM support, 416–417
  - Code Signing certificates, 650
  - cross certification, 402–403
  - deploying e-mail, 584
  - Key Recovery Agent certificates, 459
  - NDES support, 685, 689
  - Online Responder service, 224
  - RAS and IAS Server certificates, 625
  - User certificates, 628
  - VPN support, 601
  - Web Server certificates, 483–484
  - 802.1x authentication, 626
- Recover on Behalf management policy, 420
- recovery. *see* data recovery; disaster recovery; key recovery
- recovery disc (Windows), 319–320
- Recovery management policy, 420
- registration authority. *see* RA (registration authority)
- registration models
  - centralized registration model, 424–425
  - delegated registration model, 470
  - manager-initiated registration model, 423–424
  - self-service registration model, 422–423
- registry settings
  - AllowPrivateExchangeKeyImport value, 549
  - AllowPrivateSignatureKeyImport value, 549
  - backing up, 310
  - CA Exchange templates, 456
  - certificate verification, 655
  - ChainCacheResynchFiletime value, 239
  - DefaultPrivateKeyLenBits value, 549
  - disaster recovery documentation, 309
  - EFS encryption certificates, 510
  - EncryptionTemplate value, 690, 693
  - EnforcePassword value, 692
  - GeneralPurposeTemplate value, 686, 690, 693
  - key archival, 456
  - Microsoft Base Smart Card CSP, 549
  - modifying for NDES, 692–694
  - NDES recovery, 694
  - OCSP configuration, 36
  - RequireOnCardPrivateKeyGen value, 549
  - RoleSeparationEnabled value, 295
  - SignatureTemplate value, 690, 692
  - TransactionTimeoutMilliseconds value, 549
- regsvr32 command, 61
- relative distinguished names, 393–394
- remote access
  - defining network policy, 632–633
  - defining VPN policy, 606–607, 616
  - defining wireless user policy, 634–635
  - requiring smart cards, 563
- Remote Access Service (RAS), 262
- Remote Authentication Dial-In User Service. *see* RADIUS (Remote Authentication Dial-In User Service)
- remote procedure call (RPC), 177
- remote shared folders, 314
- Renew management policy, 421
- Repadm.exe tool, 62
- Replace management policy, 421
- Replication Monitor, 62
- Request Certificates permission, 689
- RequireOnCardPrivateKeyGen value, 549
- Restricted Groups, 194
- Retire management policy, 421
- revocation, certificate. *see* certificate revocation
- revocation providers, 215, 227
- Revoke management policy, 421, 444–447
- RFC 822, 23
- RFC 2196, 41, 56
- RFC 2527, 54, 56
- RFC 2560
  - additional information, 38, 234, 257
  - OCSP client, 36
  - Online Responder service, 229
  - RFC 5019 comparison, 36

- RFC 2595, 593
  - RFC 2633, 571, 593
  - RFC 2661, 617
  - RFC 3193, 598, 617
  - RFC 3207, 593
  - RFC 3280
    - additional information, 38, 234, 257
    - caching CRLs, 211
    - CRL revocation reasons, 35
    - X.509 version 1 certificates, 22
    - X.509 version 2 certificates, 24
    - X.509 version 3 certificates, 27
  - RFC 3546, 214, 234, 258
  - RFC 3647
    - additional information, 56, 234, 258, 452
    - CPS format recommendation, 48–49
    - revocation policy, 208–209
    - RFC 2527 comparison, 54
  - RFC 3739, 42, 56, 60
  - RFC 4346, 575, 593
  - RFC 4556, 670, 680
  - RFC 5019
    - additional information, 38, 234, 258
    - OCSP client, 36, 213
    - RFC 2560 comparison, 36
  - Rijmen, Vincent, 6
  - Rijndael algorithm, 6
  - Rivest Shamir Adleman algorithm. *see* RSA algorithm
  - Rivest's Cipher version 2 (RC2) algorithm, 6
  - RoleSeparationEnabled value, 295
  - root CAs. *see also* common root CAs
    - adding certificates, 111
    - adding CRLs, 111
    - CA configuration files, 101
    - certificate templates, 261
    - certificate validation, 237
    - functionality, 30–31
    - implementing enterprise, 141–144
    - implementing offline, 121–125, 141–144
    - single-tier CA hierarchy, 73
    - three-tier CA hierarchy, 75
    - trusting, 674
    - two-tier CA hierarchy, 74
    - Web Server certificates, 476, 479, 494–495, 507
  - Root Certification Authority template, 261
  - Router template, 261
  - Routing and Remote Access role service, 608–610
  - RPC (remote procedure call), 177
  - RSA (Rivest Shamir Adleman) algorithm
    - certificate templates, 272
    - credential roaming, 375
    - CRL checking, 478
    - defined, 9
    - discrete signatures, 109
    - EFS support, 511
    - SCEP process, 685
  - rule groups, 180
- ## S
- S/MIME
    - certificate templates, 260, 283
    - CNG support, 17
    - e-mail CAs, 578–579
    - e-mail digital signing process, 571–573
    - e-mail encryption process, 573–574
    - organizing issuing CAs, 79
    - securing e-mail, 571, 585–589
    - security policies, 44
  - SafeNet, 202, 318
  - salt, 6
  - Sarbanes-Oxley Act (2002), 42
  - SCCC (Smart Card Certification Center), 548
  - SCEP (Simple Certificate Enrollment Protocol)
    - certificate enrollment, 354, 684–687
    - certificate templates, 260
    - functionality, 60, 683
    - implementing NDES servers, 689
    - NDES support, 683
  - schema operations master, 61
  - schemas
    - AD DS limitations, 104
    - analyzing AD environment, 60
    - applying updates, 60–63
    - CLM deployment, 427–428
    - modifying Cert Publishers group scope, 63–67
    - support for new features, 60
    - upgrading, 155–156
  - Schlumberger smart card, 655
  - SCP (service connection point)
    - CLM permissions, 416–417
    - Code Signing certificates, 442
    - online blocks, 560
    - registration models, 422, 424–425
    - smart cards, 554
  - screen subnet, 93, 245, 256
  - scripting
    - certificate enrollment, 353, 371–374, 628
    - digital signature support, 647
    - e-mail deployment, 584
  - SCSI (Small Computer System Interface), 196, 328
  - secedit command, 113
  - Secure Hash Algorithm 1. *see* SHA1 (Secure Hash Algorithm 1)
  - Secure LDAP, 669
  - Secure LDAP (LDAP/S), 667–668



- Secure Signature Creation Device Qualified Certificate, 399
- Secure Socket Layer protocol. *see* SSL protocol
- Secure Socket Tunneling Protocol. *see* SSTP (Secure Socket Tunneling Protocol)
- security. *see also* encryption; security policies
  - CA configuration measures, 189–192
  - CA hierarchy requirements, 83–84
  - digital signatures, 647
  - hardware security modules, 196–202
  - NDES support, 684
  - Online Responder settings, 224–225
  - physical security measures, 192–193
  - private keys, 193
  - securing e-mail, 571
  - Web Server certificates, 507
  - wireless networks, 620–622
- Security Configuration Wizard, 189, 697
- security policies
  - access control, 44
  - asset classification, 44
  - B2B trust, 43
  - business continuity management, 44
  - CA hierarchy requirements, 83–85
  - Certipath, 43
  - change management, 44
  - communications, 44
  - defined, 39
  - dependencies, 39–40
  - designing, 40–41
  - digital signing, 44, 647
  - effects of external, 42–43
  - encryption, 44
  - environmental security, 44
  - Federal Bridge Certification Authority, 42–43
  - FIPS 201 standard, 42
  - key archival and recovery, 453–454
  - operations management, 44
  - organizational security, 44
  - personnel security, 44
  - physical security, 44, 83
  - PKI-related, 44–45
  - qualified certificates, 42
  - resources for developing, 41
  - Sarbanes-Oxley Act, 42
  - three-tier CA hierarchy, 75
  - Web Server certificates, 479
  - wireless communication, 44
- security zones, 549, 568, 648
- self-service registration model, 422–423
- Serian Number field, 22
- server authentication
  - CAPolicy.inf file, 101
  - EAP-TLS support, 623
  - PEAP support, 623
  - SSL support, 500
  - SSTP support, 602
  - VPN support, 601–602
- Server Authentication certificates
  - application policies, 391
  - CA hierarchy, 101, 107
  - domain controllers, 667–669
  - smart cards, 563
- Server certificate, 623
- Server Message Blocks (SMBs), 264
- Server Principal Name (SPN)
  - certificate templates, 275
  - verifying, 434–435, 438
- service accounts, 689–690, 694
- service administrator, 688–689, 697
- service connection point. *see* SCP (service connection point)
- SetReg.exe tool, 655
- SHA1 (Secure Hash Algorithm 1)
  - certificate templates, 273
  - certificate validation, 242
  - CNG support, 17
  - defined, 11
- shared folders, 314
- SID (security identifier), 15
- Siemens HiPath Security Card API, 548
- Signature Value field, 23
- SignatureTemplate value, 690, 692
- signing wizard, 654
- SignTool.exe tool, 654–656, 662
- Simple Certificate Enrollment Protocol (SCEP)
  - certificate enrollment, 354
  - certificate templates, 260
  - functionality, 60
- Simple Mail Transfer Protocol. *see* SMTP (Simple Mail Transfer Protocol)
- SMAC software, 620
- Small Computer System Interface (SCSI), 196, 328
- Smart Card Certification Center (SCCC), 548
- smart card printing station, 550–551
- Smart Card User certificate, 546–547
- smart cards
  - Active Directory environment, 535
  - additional information, 549
  - authentication, 539, 541
  - base CSPs, 535, 548–549
  - best practices, 532, 568–569, 617, 665
  - CA hierarchy requirements, 82, 84
  - certificate requirements, 536–538
  - certificate templates, 261, 269, 283, 540–542
  - CLM support, 415, 419, 439
  - CNG support, 17
  - code signing, 655

- default deployment model issues, 547
- defining removal behavior, 563–564
- defining settings, 564–565
- deploying e-mail, 585
- deploying KRA certificates, 463–464
- deploying with Windows Vista, 539–547
- deployment planning steps, 538–539
- disabling temporary, 435
- document signing, 652
- Enrollment Agent certificates, 539–540, 544–545
- enrollment definition, 553–557
- hardware considerations, 535
- ILM alternative options, 559–562
- ILM installation requirements, 547–551
- ILM profile templates, 551–559
- Kerberos authentication, 535–536
- key archival, 458
- key recovery, 453
- PIN support, 415, 463, 538, 544–545, 552–553, 656
- private key storage, 194, 649
- processing enrollment, 557–559
- requiring at specific computers, 563
- requiring for interactive logon, 562–563
- requiring for remote access, 563
- restricting certificate managers, 543
- restricting enrollment agents, 542
- Smart Card User certificate, 546–547
- software considerations, 535
- Smartcard Logon template, 261
- Smartcard User template, 261
- SMBs (Server Message Blocks), 264
- SMTP (Simple Mail Transfer Protocol)
  - CA monitor scripts, 177
  - CLM support, 427, 432
  - Domain Controller certificates, 667–668
  - e-mail support, 574
  - SSL port, 575
  - verifying service, 433
- SPC (Software Publishing Certificate), 649–650
- SPN (Server Principal Name)
  - certificate templates, 275
  - verifying, 434–435, 438
- SQL Server (Microsoft)
  - authentication, 431, 439
  - CLM server support, 427
  - creating logins, 437–438
- SRK (Storage Root Key), 190–191
- SSL (Secure Socket Layer) protocol. *see also* Web Server certificates
  - CA hierarchy requirements, 81
  - certificate mapping, 500
  - certificate requirements, 478
  - certificate templates, 261, 283
  - CNG support, 14, 17
  - CRL checking, 476–478
  - e-mail support, 574–578
  - enabling, 576–578
  - enabling on Web sites, 489
  - functionality, 475–476
  - IIS support, 486
  - implementing between client/server, 482–483
  - implementing end-to-end, 482
  - NDES support, 696
  - ports for e-mail protocols, 575
  - publication point restrictions, 244
  - RC4 algorithm, 6
  - security policies, 40
  - Web server implementation, 475
- SSTP (Secure Socket Tunneling Protocol)
  - authentication support, 602
  - VPN support, 82, 599–600
- Storage Root Key (SRK), 190–191
- Subject Alternate Name extension
  - certificate mapping, 496, 498, 507, 537
  - code signing, 650
  - description, 27
  - enabling, 675
  - Kerberos Authentication certificates, 669
  - name constraints, 393
  - RADIUS servers, 625
  - S/MIME requirements, 580
- Subject Alternative Name attribute
  - Code Signing certificates, 650
  - Domain Controller certificates, 668–669
- Subject Dir Attribute extension, 27
- Subject field
  - certificate mapping, 496, 498, 507
  - CLM policy modules, 437
  - code signing, 650
  - discrete signatures, 109
  - Domain Controller certificates, 668
  - issuing CAs, 240, 242
  - Kerberos Authentication certificates, 669
  - name constraints, 393
  - noncritical extensions, 27
  - RADIUS servers, 625
  - S/MIME requirements, 580
- Subject Information Access extension, 29
- Subject Key Identifier extension, 26, 240, 242
- Subject Name field, 23
- Subject Public Key Info field, 23
- Subject Unique ID field, 24
- subordinate CAs
  - adding certificates, 111, 674
  - adding CRLs, 111
  - CA configuration files, 101
  - certificate templates, 261, 264

- commercial CAs, 387
- functionality, 31
- publishing certificates, 112
- Subordinate Certification Authority template, 261, 264
- Suite B algorithms
  - CNG support, 16–17
  - defined, 16
- Suspend and Reinstate management policy, 421
- symmetric encryption
  - AES support, 456
  - algorithms, 4–6
  - asymmetric and, 9–10
  - certificate templates, 270, 272
  - CRL checking, 478
  - defined, 3
  - key archival, 467
  - process overview, 4–5
  - WEP support, 621
- SYS files, 647
- SYSKEY, 516, 531, 532
- system state backups
  - choosing, 310
  - performing, 311–312
  - restoring, 319

## T

- TCP (Transmission Control Protocol)
  - LDAP support, 668
  - PPTP support, 595
  - SSL support, 481, 575
- Temporal Key Integrity Protocol (TKIP), 621
- Temporary Cards management policy, 421
- 3DES algorithm. *see* Triple DES algorithm
- timeout errors, 252–253
- timestamping
  - best practices, 665
  - CTL support, 385
  - signing certificates, 653–654, 656, 660
- TKIP (Temporal Key Integrity Protocol), 621
- TLS (Transport Layer Security) protocol. *see also*
  - EAP-TLS authentication
  - additional information, 575
  - CNG support, 14
  - OCSP support, 214
  - securing e-mail, 571
  - VPN support, 596
- TPM (Trusted Platform Module), 15, 190–191
- trace logging, 694
- TransactionTimeoutMilliseconds value, 549
- Transmission Control Protocol. *see* TCP (Transmission Control Protocol)
- Transport Layer Security protocol. *see* TLS (Transport Layer Security) protocol

- Triple DES (3DES) algorithm
  - certificate templates, 272
  - defined, 6
  - encryption keys, 456
- troubleshooting
  - CAPI monitoring overview, 249–250
  - enabling CAPI diagnostics, 249
  - HTTP errors, 251–252
  - LDAP errors, 252
  - network retrieval errors, 250–253
  - path validation errors, 250–251
  - proxy server issues, 252
  - revocation check failures, 254–255
  - timeout errors, 252–253
  - trace logging, 694
- Trust List Signing templates, 261, 385
- Trusted Platform Module (TPM), 15, 190–191
- Trusted Root Certification Authority store, 479
- Trusted Sites security zone, 549, 568
- Turkish Electronic Signature Law, 399
- two-factor authentication, 535

## U

- UDP (User Datagram Protocol), 598
- Unblock management policy, 421
- Uniform Resource Identifier (URI), 394
- Uniform Resource Locator. *see* URL (Uniform Resource Locator)
- universal serial bus (USB), 535
- Unsigned Driver Installation Group Policy, 665
- upgrading PKI
  - 32-bit to 64-bit considerations, 152
  - deploying new CAs, 152–154
  - in-place upgrade, 157
  - migrating then upgrading, 155
  - post-upgrade operations, 158–160
  - upgrade paths, 151–152
  - upgrading certificate templates, 156
  - upgrading schema, 155–156
  - upgrading then migrating, 154–155
- UPN (User Principal Name)
  - certificate templates, 275, 597
  - implicit mapping, 496
  - key archival, 468
  - name constraint formats, 394
  - RADIUS support, 624
  - smart cards, 536–537
  - X.509 certificates, 27
- URI (Uniform Resource Identifier), 394
- URL (Uniform Resource Locator)
  - CDP ordering issues, 246
  - name constraint formats, 394
  - SSL support, 475
- URLScan application filter, 481

U.S. Federated Bridge Certification Authority, 391  
 usage command, 685  
 USB (universal serial bus), 535  
 User certificate  
   certificate templates, 261, 264  
   deploying, 628–629  
   EAP-TLS authentication, 622, 626  
   VPN support, 597  
 User Datagram Protocol (UDP), 598  
 User Principal Name. *see* UPN (User Principal Name)  
 user rights  
   certificate mapping, 496  
   CLM permissions, 417  
   Code Signing certificates, 442  
   disaster recovery documentation, 308  
   Managing Auditing and Security Log, 85, 119  
   online blocks, 560  
   registration models, 422, 424–425  
   Restore Files and Directories, 85  
   smart cards, 554  
 User Signature Only template, 261  
 userCertificate attribute, 64–65  
 Utimaco, 202

## V

Validity Period field, 22  
 VBA (Visual Basic for Applications), 656–657  
 VBD files, 647  
 VEK (Volume Encryption Key), 190–191  
 VeriSign certification authority, 92, 481, 489  
 version 2, 356  
 Version field, 22, 24, 29  
 virtual directories, 219, 684  
 virtual private networks. *see* VPNs (virtual private networks)  
 Visual Basic for Applications (VBA), 656–657  
 Volume Encryption Key (VEK), 190–191  
 Volume Shadow Copy (VSS), 314  
 VPNs (virtual private networks)  
   authentication options, 596–597, 600–602  
   best practices, 616–617  
   CA hierarchy requirements, 82  
   certificate deployment, 595–600  
   certificate templates, 600–602  
   creating client connection, 610–613  
   functionality, 82, 595  
   L2TP support, 82, 598–599  
   NPS configuration, 603–608  
   organizing issuing CAs, 79  
   Routing and Remote Access role service, 608–610  
   security policies, 44  
   SSTP support, 599–600  
   wireless encryption, 621  
 VSS (Volume Shadow Copy), 314

## W

WAN (wide area network), 77  
 WAPs (wireless access points)  
   best practices, 643  
   configuring, 635–636  
   MAC filtering, 620  
   rogue, 620  
   unauthorized connections, 620  
   WEP support, 621  
   802.1x authentication, 623–624  
 Warning event, 180  
 wbadm.exe utility, 318–319  
 Web acceleration devices, 495  
 Web Client certificates, 478  
 Web Pool Agent (clmWebPool), 430, 434–435  
 Web proxy settings (Online Responder),  
   214, 222  
 Web publishing, 481–483  
 Web Server Certificate Wizard, 484, 494  
 Web Server certificates  
   best practices, 507, 616  
   certificate templates, 261, 264, 483  
   choosing providers, 478–479  
   CRL checking, 476–478  
   installing, 575–576  
   ISA with server publishing, 481  
   ISA with Web publishing, 481–483  
   issuing to domain members, 483–489  
   issuing to non-forest members, 484, 489–495  
   issuing to third-party Web Servers, 484, 495  
   placement considerations, 479–483  
   SSL support, 475–476, 478  
 Web servers  
   authenticating, 476  
   best practices, 507  
   Certificate Services Web Enrollment pages, 352  
   certificate templates, 261  
   clustered, 480–481  
   HTTP support, 475  
   ISA with server publishing, 481  
   ISA with Web publishing, 481–483  
   single, 480  
   SSL implementation, 475  
   validating identity, 475  
 Web sites  
   binding certificates, 488–489, 495  
   certificate mapping, 497  
   connecting to, 503–504  
   enabling SSL, 489  
 WEP (Wired Equivalent Privacy), 620–621, 643  
 Wi-Fi Alliance, 621–622  
 Wi-Fi Protected Access (WPA), 621–622  
 wide area network (WAN), 77  
 WIN\_CRYPT\_ENABLE flag, 580

## Windows 2000

- Autoenrollment Settings, 353
- Domain Controller certificates, 671
- issuing Web Server certificates, 484–486, 493–494
- remote EFS encryption, 512–513
- smart card requirements, 536–537

## Windows authentication, 439

## Windows Internet Explorer

- certificate-based authentication, 503–504
- certificate enrollment, 363–367
- certificate requests, 459–460
- code signing, 82, 446, 648
- creating profile templates, 551
- CRL checking, 476–478
- Key Recovery Agent certificates, 461
- OCSP support, 214
- verifying signatures, 660–661

## Windows Load Balancing Service (WLBS), 35

## Windows RE (Windows Recovery Environment), 319

## Windows recovery disc, 319–320

## Windows Recovery Environment (Windows RE), 319

## Windows Server 2003

- certificate mapping, 500
- certificate templates, 668
- Domain Controller certificates, 671
- EFS encryption, 515–518
- issuing Web Server certificates, 484–486, 493–494
- smart card requirements, 536–537

## Windows Server 2008

- certificate mapping, 501–503
- Domain Controller certificates, 670–671
- EFS encryption, 515–518
- issuing Web Server certificates, 486–489, 494–495
- KDC validation, 669
- Kerberos Authentication certificates, 669
- smart card requirements, 537–538
- wireless networking, 641

## Windows server backups

- choosing, 310
- installing, 311–312
- one-time only, 314–315
- performing, 312–315
- restoring, 319–321
- scheduling, 312–313

## Windows Vista

- deploying smart cards, 539–547
- EFS management, 524–526, 532
- KDC validation, 669

- remote EFS encryption, 513
- signing certificates, 653
- smart card requirements, 537–538
- VPN client connection, 611–612
- wireless networking, 638–640

## Windows XP

- remote EFS encryption, 512–513
- signing certificates, 653
- smart card requirements, 536–537
- VPN client connection, 610–611
- wireless networking, 619, 636–637

## Wired Equivalent Privacy (WEP), 620–621, 643

wireless access points. *see* WAPs (wireless access points)

## wireless networking

- best practices, 643
- certificate templates, 283
- deploying certificates, 627–629
- Group Policy support, 640–641
- network access policy, 632–633
- protecting communications, 620–622
- security policies, 44
- threats introduced, 619–620
- 802.1x authentication, 622–626, 629–641
- Wireless User certificate, 628–629

## WiSeKey, 324

## WLBS (Windows Load Balancing Service), 35

## Workstation Authentication template, 262, 626–628

## WPA2, 621–622

## WPA-Enterprise, 622

## WPA (Wi-Fi Protected Access), 621–622

## Write permission, 265–266

**X**

## 802.1x authentication

- best practices, 643
- CA hierarchy requirements, 81
- configuring RADIUS server, 629–635
- connecting to wireless networks, 636–640
- Group Policy support, 640–641
- planning certificates, 622–626
- WPA-Enterprise dependency, 622

## X.509 version 1 certificate, 22–23, 236

## X.509 version 2 certificate, 23–24, 236

## X.509 version 3 certificate

- building certificate chains, 240
- certificate extensions, 25–29, 240–242
- certificate validation, 236
- overview, 24

## Subject Alternative Name field, 496

## Xenroll.dll, 353, 362, 374

## XOR (Exclusive OR) function, 5