

Auf einen Blick

1	Public Key Infrastructure und Certificate Authority	15
2	Aufbau einer Windows-CA-Infrastruktur	85
3	Anpassung der Zertifizierungsstelle und Verteilen von Zertifikaten	297
4	Eine Windows-CA-Infrastruktur verwenden	391
5	Betrieb und Wartung einer Windows-CA-Infrastruktur	673

Inhalt

Materialien zum Buch	10
Vorwort	11
Geleitwort des Fachgutachters	13

1 Public Key Infrastructure und Certificate Authority 15

1.1 Was ist ein Zertifikat?	17
1.1.1 Symmetrische und asymmetrische Kryptografie	17
1.1.2 Verschlüsselung und Signatur	19
1.1.3 Eigenschaften eines Webserver-Zertifikats	24
1.1.4 Zertifikate in Windows-Systemen	32
1.1.5 Die Gültigkeit von Zertifikaten prüfen	40
1.1.6 Häufige Fehlermeldungen bei der Verwendung von Zertifikaten	51
1.2 Zertifizierungsstellen	63
1.2.1 Aufgaben einer Zertifizierungsstelle	63
1.2.2 Zertifizierungsstellen-Hierarchie	64
1.2.3 Kommerzielle und private Zertifizierungsstellen	67
1.2.4 Alleinstehende Zertifizierungsstellen und Unternehmenszertifizierungsstellen	68
1.2.5 Aktualisierung der Stammzertifikat-Updates auf den Systemen	69
1.3 Aufbau einer Infrastruktur für öffentliche Schlüssel	71
1.4 Protokolle und Algorithmen	73
1.4.1 Symmetrische Protokolle	73
1.4.2 Asymmetrische Verfahren	74
1.4.3 Dateiformate rund um Zertifikate	75

2 Aufbau einer Windows-CA-Infrastruktur 85

2.1 Notwendige Parameter und Rahmenbedingungen für eine CA-Installation	86
2.1.1 Festlegen der Zertifikate, die ausgestellt werden	94

2.2	Installationsvoraussetzungen für eine CA	95
2.2.1	Security Compliance Manager	95
2.2.2	Security Compliance Toolkit	101
2.3	Installation der AD CS-Rolle	103
2.3.1	Installation der Rolle mithilfe der PowerShell	111
2.3.2	Installation der Rolle über das Windows Admin Center	115
2.3.3	Remoteserver-Verwaltungstools	116
2.3.4	CAPolicy.inf	120
2.4	Konfiguration einer einfachen CA-Infrastruktur	126
2.4.1	Konfiguration der Zertifizierungsstelle	127
2.4.2	Konfiguration der Zertifizierungsstelle mithilfe der PowerShell	137
2.4.3	Schnelle Überprüfung der Konfiguration und Anpassen der Konfiguration	138
2.5	Installation einer mehrstufigen CA-Infrastruktur	150
2.5.1	Installation der Offline-Stammzertifizierungsstelle	152
2.5.2	Die Umgebung für die Speicherung der Sperrlisten und der CA-Zertifikate vorbereiten	175
2.5.3	Installation der untergeordneten Unternehmenszertifizierungsstelle	186
2.6	Die Funktionsweise der installierten Umgebung prüfen	213
2.7	Installation einer Zertifizierungsstelle auf einem Windows Server Core	216
2.8	Zertifikatrichtlinie und Zertifikatverwendungsrichtlinie	223
2.8.1	Zertifikatrichtlinie	223
2.8.2	Zertifikatverwendungsrichtlinie	224
2.8.3	Sicherheitsrichtlinie	227
2.8.4	Verwendung der Dokumente im System	227
2.9	Verwendung von Hardware-Security-Modulen (HSMs)	230
2.9.1	Ein HSM für eine Zertifizierungsstelle verwenden	231
2.9.2	HSMs als Speicher für andere Zertifikate	234
2.10	Installation der zusätzlichen AD CS-Rolledienste	238
2.10.1	Installation und Konfiguration der Webregistrierung	238
2.10.2	Installation und Konfiguration des Zertifikatregistrierungsrichtlinien-Webdienstes (CEP) und des Zertifikatregistrierungs-Webdienstes (CES)	246
2.10.3	Installation und Konfiguration eines Online-Responders	252
2.10.4	Installation und Konfiguration des NDES	262
2.11	Hochverfügbarkeit	266
2.11.1	Zertifizierungsstelle	267
2.11.2	Online-Responder	274

2.11.3	Registrierungsdienst für Netzwerkgeräte	275
2.11.4	Zertifikatregistrierungs-Webdienst und Zertifikatrichtlinien-Webdienst (CEP/CES)	275
2.11.5	Zertifizierungsstellen-Webregistrierung	275
2.12	PowerShell-Skripte für die Installation	275
2.12.1	Einstufige Umgebung	277
2.12.2	Mehrstufige Umgebung	278
2.13	Schritt-für-Schritt-Installationsanleitung	284
2.13.1	Einstufige Umgebung	284
2.13.2	Mehrstufige Umgebung	286

3 Anpassung der Zertifizierungsstelle und Verteilen von Zertifikaten 297

3.1	Konfiguration einer Zertifizierungsstelle	297
3.1.1	Konfiguration der CA-Eigenschaften	297
3.1.2	Konfigurationen in der CA-Konsole	317
3.1.3	Konfiguration der Schlüsselarchivierung	327
3.2	Zertifikatvorlagen verwalten	340
3.3	Zertifikate an Clients verteilen	361
3.3.1	Autoenrollment über Gruppenrichtlinie	361
3.3.2	Manuelles Registrieren mithilfe der Zertifikatverwaltungskonsole ...	364
3.3.3	Zertifikate mit der Kommandozeile registrieren	377
3.3.4	Einen Registrierungs-Agenten verwenden	379
3.3.5	Massenanforderung	386

4 Eine Windows-CA-Infrastruktur verwenden 391

4.1	Zertifikate für Webserver	391
4.1.1	Wie funktioniert SSL?	392
4.1.2	Die Zertifizierungsstelle vorbereiten	400
4.1.3	Anfordern und Ausrollen eines Webserver-Zertifikats	406
4.2	Clientzertifikate zur Authentifizierung an einem Webserver	428
4.3	Zertifikate für Domänencontroller	434
4.3.1	Domänencontroller	434
4.3.2	Domänencontrollerauthentifizierung	435

4.3.3	Kerberos-Authentifizierung	436
4.3.4	LDAP over SSL	438
4.3.5	Verzeichnis-E-Mail-Replikation	445
4.4	EFS verwenden	447
4.4.1	EFS konfigurieren	448
4.4.2	Zusammenfassung und Fakten zum Einsatz von EFS	461
4.5	BitLocker und die Netzwerkentsperrung	461
4.5.1	BitLocker für Betriebssystemlaufwerke	462
4.5.2	BitLocker für zusätzliche Festplattenlaufwerke	474
4.5.3	BitLocker To Go für Wechseldatenträger	476
4.5.4	Zertifikate und BitLocker	482
4.5.5	BitLocker Netzwerkentsperrung	495
4.5.6	BitLocker verwalten	504
4.6	Smartcard-Zertifikate verwenden	510
4.6.1	Physische Smartcards	510
4.6.2	Virtuelle Smartcards	525
4.6.3	SCAMA – Smart Card based Authentication Mechanism Assurance	533
4.7	Den WLAN-Zugriff mit Zertifikaten absichern	539
4.7.1	Netzwerkrichtlinienserver	540
4.7.2	WLAN-Authentifizierung mit Protected-EAP	547
4.7.3	WLAN mit Clientzertifikaten	558
4.8	Verwendung von 802.1x für LAN-Verbindungen	565
4.9	Den VPN-Zugang mit Zertifikaten absichern	571
4.10	Zertifikate zur Absicherung von Netzwerkkommunikation mit IPSec verwenden	586
4.11	Zertifikate für Exchange verwenden	601
4.12	S/MIME verwenden	608
4.13	Die Codesignatur verwenden	629
4.13.1	Signatur von PowerShell-Skripten	632
4.13.2	Signatur von Makros	636
4.13.3	Signatur von ausführbaren Dateien	638
4.14	Zertifikate bei den Remotedesktopdiensten verwenden	641
4.14.1	Konfiguration von Remotedesktop (Admin-Modus)	641
4.14.2	Konfiguration der Remotedesktopdienste (Terminalserver-Modus)	648
4.14.3	Zertifikate für RemoteApps	655

4.15	Zertifikate für Hyper-V	658
4.16	Zertifikate für das Windows Admin Center	661
4.17	CEP und CES	662
4.18	Zertifikate für VMware	667

5 Betrieb und Wartung einer Windows-CA-Infrastruktur 673

5.1	Überwachung der Zertifizierungsstelle	673
5.1.1	Funktionsüberwachung	673
5.1.2	Auditing	675
5.2	Ein CA-Zertifikat erneuern	675
5.3	Sicherung und Wiederherstellung	682
5.3.1	Backup und Restore einer CA	683
5.3.2	Aktivieren des Mailversands zur Nachverfolgung der ausgestellten Zertifikate	688
5.3.3	Notfallsignatur einer Sperrliste	689
5.4	Eine Zertifizierungsstelle migrieren	691
5.5	Eine Zertifizierungsstelle entfernen	693
5.6	Wartungsaufgaben an der Datenbank	695
5.7	Mimikatz	697
5.8	Zertifikatmanagement mit dem Microsoft Identity Manager (MIM)	701
5.9	Sonstiges	702
5.9.1	Zertifikate im Zertifikatspeicher eines Systems finden, die bald ablaufen	702
5.9.2	Skript zum Löschen von Zertifikaten aus der CA-Datenbank	703
5.9.3	Skript zur Warnung vor ablaufenden Zertifikaten in der CA-Datenbank	703
5.9.4	PowerShell-Modul mit zusätzlichen Optionen für die Zertifizierungsstelle	703
Glossar		707
Index		719