

## 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

---

<b>1.1 Was ist ein Zertifikat?</b> .....	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
<b>1.2 Zertifizierungsstellen</b> .....	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
<b>1.3 Aufbau einer Infrastruktur für öffentliche Schlüssel</b> .....	71
<b>1.4 Protokolle und Algorithmen</b> .....	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

---

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

<b>2.2</b>	<b>Installationsvoraussetzungen für eine CA</b> .....	95
2.2.1	Security Compliance Manager .....	95
2.2.2	Security Compliance Toolkit .....	101
<b>2.3</b>	<b>Installation der AD CS-Rolle</b> .....	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
<b>2.4</b>	<b>Konfiguration einer einfachen CA-Infrastruktur</b> .....	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
<b>2.5</b>	<b>Installation einer mehrstufigen CA-Infrastruktur</b> .....	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
<b>2.6</b>	<b>Die Funktionsweise der installierten Umgebung prüfen</b> .....	213
<b>2.7</b>	<b>Installation einer Zertifizierungsstelle auf einem Windows Server Core</b> .....	216
<b>2.8</b>	<b>Zertifikatrichtlinie und Zertifikatverwendungsrichtlinie</b> .....	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
<b>2.9</b>	<b>Verwendung von Hardware-Security-Modulen (HSMs)</b> .....	230
2.9.1	Ein HSM für eine Zertifizierungsstelle verwenden .....	231
2.9.2	HSMs als Speicher für andere Zertifikate .....	234
<b>2.10</b>	<b>Installation der zusätzlichen AD CS-Rollendienste</b> .....	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
<b>2.11</b>	<b>Hochverfügbarkeit</b> .....	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
<b>2.12</b>	<b>PowerShell-Skripte für die Installation</b> .....	275
2.12.1	Einstufige Umgebung .....	277
2.12.2	Mehrstufige Umgebung .....	278
<b>2.13</b>	<b>Schritt-für-Schritt-Installationsanleitung</b> .....	284
2.13.1	Einstufige Umgebung .....	284
2.13.2	Mehrstufige Umgebung .....	286
<b>3</b>	<b>Anpassung der Zertifizierungsstelle und Verteilen von Zertifikaten</b> .....	297
<b>3.1</b>	<b>Konfiguration einer Zertifizierungsstelle</b> .....	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
<b>3.2</b>	<b>Zertifikatvorlagen verwalten</b> .....	340
<b>3.3</b>	<b>Zertifikate an Clients verteilen</b> .....	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
<b>4</b>	<b>Eine Windows-CA-Infrastruktur verwenden</b> .....	391
<b>4.1</b>	<b>Zertifikate für Webserver</b> .....	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
<b>4.2</b>	<b>Clientzertifikate zur Authentifizierung an einem Webserver</b> .....	428
<b>4.3</b>	<b>Zertifikate für Domänencontroller</b> .....	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
<b>4.4</b>	<b>EFS verwenden .....</b>	<b>447</b>
4.4.1	EFS konfigurieren .....	448
4.4.2	Zusammenfassung und Fakten zum Einsatz von EFS .....	461
<b>4.5</b>	<b>BitLocker und die Netzwerkentsperrung .....</b>	<b>461</b>
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
<b>4.6</b>	<b>Smartcard-Zertifikate verwenden .....</b>	<b>510</b>
4.6.1	Physische Smartcards .....	510
4.6.2	Virtuelle Smartcards .....	525
4.6.3	SCAMA – Smart Card based Authentication Mechanism Assurance .....	533
<b>4.7</b>	<b>Den WLAN-Zugriff mit Zertifikaten absichern .....</b>	<b>539</b>
4.7.1	Netzwerkrichtlinienserver .....	540
4.7.2	WLAN-Authentifizierung mit Protected-EAP .....	547
4.7.3	WLAN mit Clientzertifikaten .....	558
<b>4.8</b>	<b>Verwendung von 802.1x für LAN-Verbindungen .....</b>	<b>565</b>
<b>4.9</b>	<b>Den VPN-Zugang mit Zertifikaten absichern .....</b>	<b>571</b>
<b>4.10</b>	<b>Zertifikate zur Absicherung von Netzwerkkommunikation mit IPSec verwenden .....</b>	<b>586</b>
<b>4.11</b>	<b>Zertifikate für Exchange verwenden .....</b>	<b>601</b>
<b>4.12</b>	<b>S/MIME verwenden .....</b>	<b>608</b>
<b>4.13</b>	<b>Die Codesignatur verwenden .....</b>	<b>629</b>
4.13.1	Signatur von PowerShell-Skripten .....	632
4.13.2	Signatur von Makros .....	636
4.13.3	Signatur von ausführbaren Dateien .....	638
<b>4.14</b>	<b>Zertifikate bei den Remotedesktopdiensten verwenden .....</b>	<b>641</b>
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

<b>4.15</b>	<b>Zertifikate für Hyper-V .....</b>	<b>658</b>
<b>4.16</b>	<b>Zertifikate für das Windows Admin Center .....</b>	<b>661</b>
<b>4.17</b>	<b>CEP und CES .....</b>	<b>662</b>
<b>4.18</b>	<b>Zertifikate für VMware .....</b>	<b>667</b>
<b>5</b>	<b>Betrieb und Wartung einer Windows-CA-Infrastruktur .....</b>	<b>673</b>
<b>5.1</b>	<b>Überwachung der Zertifizierungsstelle .....</b>	<b>673</b>
5.1.1	Funktionsüberwachung .....	673
5.1.2	Auditing .....	675
<b>5.2</b>	<b>Ein CA-Zertifikat erneuern .....</b>	<b>675</b>
<b>5.3</b>	<b>Sicherung und Wiederherstellung .....</b>	<b>682</b>
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
<b>5.4</b>	<b>Eine Zertifizierungsstelle migrieren .....</b>	<b>691</b>
<b>5.5</b>	<b>Eine Zertifizierungsstelle entfernen .....</b>	<b>693</b>
<b>5.6</b>	<b>Wartungsaufgaben an der Datenbank .....</b>	<b>695</b>
<b>5.7</b>	<b>Mimikatz .....</b>	<b>697</b>
<b>5.8</b>	<b>Zertifikatmanagement mit dem Microsoft Identity Manager (MIM) .....</b>	<b>701</b>
<b>5.9</b>	<b>Sonstiges .....</b>	<b>702</b>
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