

Inhalt

| | |
|-------------------------------------|----|
| Materialien zum Buch | 11 |
| Vorwort | 13 |
| Geleitwort des Fachgutachters | 15 |

1 Public Key Infrastructure und Certificate Authority

17

| | |
|---------------------------------------------------------------------------------------------|----|
| 1.1 Was ist ein Zertifikat? | 19 |
| 1.1.1 Symmetrische und asymmetrische Kryptografie | 19 |
| 1.1.2 Verschlüsselung und Signatur | 21 |
| 1.1.3 Eigenschaften eines Webserver-Zertifikats | 25 |
| 1.1.4 Zertifikate in Windows-Systemen | 34 |
| 1.1.5 Die Gültigkeit von Zertifikaten prüfen | 42 |
| 1.1.6 Häufige Fehlermeldungen bei der Verwendung von Zertifikaten | 53 |
| 1.2 Zertifizierungsstellen | 65 |
| 1.2.1 Aufgaben einer Zertifizierungsstelle | 65 |
| 1.2.2 Zertifizierungsstellen-Hierarchie | 65 |
| 1.2.3 Kommerzielle und private Zertifizierungsstellen | 69 |
| 1.2.4 Alleinstehende Zertifizierungsstellen und Unternehmenszertifizierungsstellen | 70 |
| 1.2.5 Aktualisierung der Stammzertifikat-Updates auf den Systemen | 70 |
| 1.3 Aufbau einer Infrastruktur für öffentliche Schlüssel | 73 |
| 1.4 Protokolle und Algorithmen | 75 |
| 1.4.1 Symmetrische Protokolle | 75 |
| 1.4.2 Asymmetrische Verfahren | 75 |
| 1.4.3 Dateiformate rund um Zertifikate | 77 |

2 Aufbau einer Windows-CA-Infrastruktur

87

| | |
|----------------------------------------------------------------------------------|----|
| 2.1 Notwendige Parameter und Rahmenbedingungen für eine CA-Installation | 88 |
| 2.1.1 Festlegen der Zertifikate, die ausgestellt werden | 96 |

| | | |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 2.2 | Installationsvoraussetzungen für eine CA | 98 |
| 2.2.1 | Security Compliance Manager | 98 |
| 2.2.2 | Security Compliance Toolkit | 104 |
| 2.3 | Notwendige Rechte für die Installation einer Zertifizierungsstelle | 105 |
| 2.4 | Installation der AD CS-Rolle | 113 |
| 2.4.1 | Installation der Rolle mithilfe der PowerShell | 121 |
| 2.4.2 | Installation der Rolle über das Windows Admin Center | 125 |
| 2.4.3 | Remoteserver-Verwaltungstools | 126 |
| 2.4.4 | CAPolicy.inf | 129 |
| 2.5 | Konfiguration einer einfachen CA-Infrastruktur | 136 |
| 2.5.1 | Konfiguration der Zertifizierungsstelle | 137 |
| 2.5.2 | Konfiguration der Zertifizierungsstelle mithilfe der PowerShell | 147 |
| 2.5.3 | Schnelle Überprüfung der Konfiguration und Anpassen der Konfiguration | 149 |
| 2.6 | Installation einer mehrstufigen CA-Infrastruktur | 160 |
| 2.6.1 | Installation der Offline-Stammzertifizierungsstelle | 162 |
| 2.6.2 | Die Umgebung für die Speicherung der Sperrlisten und der CA-Zertifikate vorbereiten | 185 |
| 2.6.3 | Installation der untergeordneten Unternehmenszertifizierungsstelle | 196 |
| 2.7 | Die Funktionsweise der installierten Umgebung prüfen | 223 |
| 2.8 | Installation einer Zertifizierungsstelle auf einem Windows Server Core | 226 |
| 2.9 | Zertifikatrichtlinie und Zertifikatverwendungsrichtlinie | 233 |
| 2.9.1 | Zertifikatrichtlinie | 233 |
| 2.9.2 | Zertifikatverwendungsrichtlinie | 234 |
| 2.9.3 | Sicherheitsrichtlinie | 237 |
| 2.9.4 | Verwendung der Dokumente im System | 237 |
| 2.10 | Verwendung von Hardware-Security-Modulen (HSMs) | 240 |
| 2.10.1 | Ein HSM für eine Zertifizierungsstelle verwenden | 241 |
| 2.10.2 | HSMs als Speicher für andere Zertifikate | 244 |
| 2.11 | Installation der zusätzlichen AD CS-Rollendienste | 248 |
| 2.11.1 | Installation und Konfiguration der Webregistrierung | 248 |
| 2.11.2 | Installation und Konfiguration des Zertifikatregistrierungsrichtlinien-Webdienstes (CEP) und des Zertifikatregistrierungs-Webdienstes (CES) | 256 |
| 2.11.3 | Installation und Konfiguration eines Online-Responders | 262 |
| 2.11.4 | Installation und Konfiguration des NDES | 272 |

| | | |
|-------------|----------------------------------------------------------------------------------|-----|
| 2.12 | Hochverfügbarkeit | 276 |
| 2.12.1 | Zertifizierungsstelle | 277 |
| 2.12.2 | Online-Responder | 284 |
| 2.12.3 | Registrierungsdienst für Netzwerkgeräte | 285 |
| 2.12.4 | Zertifikatregistrierungs-Webdienst und Zertifikatrichtlinien-Webdienst (CEP/CES) | 285 |
| 2.12.5 | Zertifizierungsstellen-Webregistrierung | 285 |
| 2.13 | PowerShell-Skripte für die Installation | 285 |
| 2.13.1 | Einstufige Umgebung | 287 |
| 2.13.2 | Mehrstufige Umgebung | 288 |
| 2.14 | Schritt-für-Schritt-Installationsanleitung | 294 |
| 2.14.1 | Einstufige Umgebung | 294 |
| 2.14.2 | Mehrstufige Umgebung | 296 |

3 Anpassung der Zertifizierungsstelle und Verteilen von Zertifikaten 307

| | | |
|------------|-------------------------------------------------------------------|-----|
| 3.1 | Konfiguration einer Zertifizierungsstelle | 307 |
| 3.1.1 | Konfiguration der CA-Eigenschaften | 307 |
| 3.1.2 | Konfigurationen in der CA-Konsole | 327 |
| 3.1.3 | Konfiguration der Schlüsselarchivierung | 338 |
| 3.2 | Zertifikatvorlagen verwalten | 350 |
| 3.3 | Zertifikate an Clients verteilen | 372 |
| 3.3.1 | Autoenrollment über Gruppenrichtlinie | 372 |
| 3.3.2 | Manuelles Registrieren mithilfe der Zertifikatverwaltungskonsolle | 375 |
| 3.3.3 | Zertifikate mit der Kommandozeile registrieren | 388 |
| 3.3.4 | Einen Registrierungs-Agenten verwenden | 390 |
| 3.3.5 | Massenanforderung | 397 |
| 3.3.6 | Verwenden des Tools Certreq (GUI) | 400 |

4 Eine Windows-CA-Infrastruktur verwenden 403

| | | |
|------------|----------------------------------|-----|
| 4.1 | Zertifikate für Webserver | 403 |
| 4.1.1 | Wie funktioniert SSL? | 404 |

| | | |
|-------------|----------------------------------------------------------------------------------------|------------|
| 4.1.2 | Die Zertifizierungsstelle vorbereiten | 412 |
| 4.1.3 | Anfordern und Ausrollen eines Webserver-Zertifikats | 418 |
| 4.2 | Clientzertifikate zur Authentifizierung an einem Webserver | 440 |
| 4.3 | Zertifikate für Domänencontroller | 446 |
| 4.3.1 | Domänencontroller | 447 |
| 4.3.2 | Domänencontrollerauthentifizierung | 447 |
| 4.3.3 | Kerberos-Authentifizierung | 449 |
| 4.3.4 | LDAP over SSL | 450 |
| 4.3.5 | Verzeichnis-E-Mail-Replikation | 457 |
| 4.4 | EFS verwenden | 460 |
| 4.4.1 | EFS konfigurieren | 461 |
| 4.4.2 | Zusammenfassung und Fakten zum Einsatz von EFS | 473 |
| 4.5 | BitLocker und die Netzwerkentsperrung | 473 |
| 4.5.1 | BitLocker für Betriebssystemlaufwerke | 474 |
| 4.5.2 | BitLocker für zusätzliche Festplattenlaufwerke | 487 |
| 4.5.3 | BitLocker To Go für Wechseldatenträger | 488 |
| 4.5.4 | Zertifikate und BitLocker | 494 |
| 4.5.5 | BitLocker Netzwerkentsperrung | 507 |
| 4.5.6 | BitLocker verwalten | 516 |
| 4.6 | Smartcard-Zertifikate verwenden | 522 |
| 4.6.1 | Physische Smartcards | 523 |
| 4.6.2 | Virtuelle Smartcards | 537 |
| 4.6.3 | SCAMA – Smart Card based Authentication Mechanism Assurance | 545 |
| 4.7 | Den WLAN-Zugriff mit Zertifikaten absichern | 551 |
| 4.7.1 | Netzwerkrichtlinienserver | 552 |
| 4.7.2 | WLAN-Authentifizierung mit Protected-EAP | 559 |
| 4.7.3 | WLAN mit Clientzertifikaten | 570 |
| 4.8 | Verwendung von 802.1x für LAN-Verbindungen | 577 |
| 4.9 | Den VPN-Zugang mit Zertifikaten absichern | 583 |
| 4.10 | Zertifikate zur Absicherung von Netzwerkkommunikation mit IPSec verwenden | 599 |
| 4.11 | Zertifikate für Exchange verwenden | 613 |
| 4.12 | S/MIME verwenden | 621 |

| | | |
|-------------|--------------------------------------------------------------------|-----|
| 4.13 | Die Codesignatur verwenden | 642 |
| 4.13.1 | Signatur von PowerShell-Skripten | 645 |
| 4.13.2 | Signatur von Makros | 650 |
| 4.13.3 | Signatur von ausführbaren Dateien | 652 |
| 4.14 | Zertifikate bei den Remotedesktopdiensten verwenden | 654 |
| 4.14.1 | Konfiguration von Remotedesktop (Admin-Modus) | 654 |
| 4.14.2 | Konfiguration der Remotedesktopdienste (Terminalserver-Modus) | 661 |
| 4.14.3 | Zertifikate für RemoteApps | 669 |
| 4.15 | Zertifikate für Hyper-V | 671 |
| 4.16 | Zertifikate für das Windows Admin Center | 674 |
| 4.17 | CEP und CES | 675 |
| 4.18 | Zertifikate für die Active Directory-Verbunddienste (AD FS) | 680 |
| 4.19 | Zertifikatverteilung über Intune | 682 |
| 4.20 | Zertifikate für VMware | 682 |

5 Betrieb und Wartung einer Windows-CA-Infrastruktur 689

| | | |
|------------|------------------------------------------------------------------------------|-----|
| 5.1 | Überwachung der Zertifizierungsstelle | 689 |
| 5.1.1 | Funktionsüberwachung | 689 |
| 5.1.2 | Auditing | 691 |
| 5.1.3 | Weiterleitung der Windows-Ereignisprotokolle | 691 |
| 5.1.4 | Reporting über die Zertifizierungsstelle | 694 |
| 5.2 | Ein CA-Zertifikat erneuern | 695 |
| 5.3 | Sicherung und Wiederherstellung | 702 |
| 5.3.1 | Backup und Restore einer CA | 703 |
| 5.3.2 | Aktivieren des Mailversands zur Nachverfolgung der ausgestellten Zertifikate | 708 |
| 5.3.3 | Notfallsignatur einer Sperrliste | 708 |
| 5.4 | Eine Zertifizierungsstelle migrieren | 711 |
| 5.5 | Eine Zertifizierungsstelle entfernen | 712 |

| | | |
|---------------|----------------------------------------------------------------------------|------------|
| 5.6 | Wartungsaufgaben an der Datenbank | 715 |
| 5.7 | Zertifikatmanagement mit dem Microsoft Identity Manager (MIM) | 717 |
| 5.8 | Sicherheit rund um die Zertifizierungsstelle | 718 |
| 5.8.1 | Zugriff auf private Schlüssel | 718 |
| 5.8.2 | Angriffe gegen eine Microsoft-Zertifizierungsstelle | 725 |
| 5.8.3 | Tools zur Überprüfung der Konfiguration | 742 |
| Glossar | | 747 |
| Index | | 759 |