

Netzwerksicherheit mit Windows Server 2003- Zertifikatdiensten (PKI)

Planung, Implementierung und Verwaltung

Netzwerksicherheit mit Windows Server 2003-Zertifikatdiensten (PKI)

Seminarunterlage – Artikelnr. PK-010405

Autor: Carlo Westbrook

Version: April 2005

Alle in dieser Seminarunterlage enthaltenen Programme, Darstellungen und Informationen wurden nach bestem Wissen erstellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund ist das in der vorliegenden Seminarunterlage enthaltene Material mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor und CertPro Limited übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Materials, oder Teilen davon, oder durch Rechtsverletzungen Dritter entsteht.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in dieser Seminarunterlage berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann verwendet werden dürften.

Die in diesem Dokument aufgeführten Namen tatsächlicher Firmen und Produkte sind möglicherweise Marken der jeweiligen Eigentümer und werden ohne Gewährleistung der freien Verwendbarkeit benutzt.

Dieses Werk ist urheberrechtlich geschützt.

Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Erlaubnis für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden (auch nicht zur Unterrichtsvorbereitung), unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen, usw.).

CertPro ist eine eingetragene Marke von Carlo Westbrook.

Copyright © 2005-2009 CertPro Limited.
Alle Rechte vorbehalten.

Inhaltsverzeichnis

Inhalt	Seite
Voraussetzungen.....	7
Kursbeschreibung.....	8 - 11
Rauminstallation	12
<i>Kapitel 1:</i>	
Grundlagen.....	13 -52
Einführung	15
Zweck einer PKI.....	16
Komponenten einer PKI.....	18
Zertifikate	20
Zertifikaterweiterungen.....	21
Lebensdauer digitaler Zertifikate.....	24
Zertifizierungsstelle (Certificate Authority, CA).....	25
Rollen in einer Zertifizierungsstellenhierarchie	26
Zertifikatsperrlisten	29 - 31
Basissperrliste	29
Deltasperrliste.....	30
Gründe für das Sperren von Zertifikaten	31
PKI-fähige Anwendungen	32
Zertifikatempfänger.....	34
PKI-Tools	36
Grundlagen der Kryptografie	38 - 48
Symmetrische Datenverschlüsselung	39
Asymmetrische Datenverschlüsselung	41
Asymmetrische Signatur	43
Kombination von asymmetrischer und symmetrischer Verschlüsselung.....	45
Digitale Signatur von Daten	46
Kombination aus asymmetrischer Signatur und Hashalgorithmus	48
Praktische Übung	49
Zusammenfassung	52
<i>Kapitel 2:</i>	
Entwerfen einer Zertifizierungsstellenhierarchie.....	53 - 80
Einführung	55
Arten von Zertifizierungsstellen	56
Struktur von Zertifizierungsstellen	57
Schichtenmodelle einer Zertifizierungsstellenhierarchie.....	59 - 63
Einschichtige Zertifizierungsstellenhierarchie	60
Zweischichtige Zertifizierungsstellenhierarchie	61
Dreischichtige Zertifizierungsstellenhierarchie	62
Vierschichtige Zertifizierungsstellenhierarchie.....	63
Bestimmen der Anforderungen für Anwendungen.....	64
Ermitteln der Zertifikatempfänger	66
Anforderungen an die Sicherheit	68
Räumliche Sicherheit für Offline-Zertifizierungsstellen	68
Zusätzliche Sicherheitsmaßnahmen für Online-Zertifizierungsstellen.....	68
Schutz des privaten Schlüssels der Zertifizierungsstelle.....	69
Zusammensetzung der PKI-Verwaltungsabteilung.....	70
Minimierung des Ausfallrisikos von Zertifizierungsstellen.....	72
Absichern und Optimieren einer Offline-Zertifizierungsstelle.....	73
Absichern und Optimieren einer Online-Zertifizierungsstelle.....	75

Gültigkeitsdauer von Zertifikaten	77
Veröffentlichungspunkte	78
Zusammenfassung	80

Kapitel 3:

Implementierung einer Zertifizierungsstellenhierarchie	81 - 130
Einführung	83
Die Datei CAPolicy.inf	84
Zertifikatverwendungserklärung (CPS)	87
Object Identifier (OID)	89
Einstellungen für eine Offline-Zertifizierungsstelle	91
Absicherung einer Offline-Zertifizierungsstelle	93
Sicherheitsmaßnahmen bei der Konfiguration	94
Sicherung von Geräten	97
Speicherung privater Schlüssel auf Smartcards	99
Hardware-Sicherheitsmodul (HSM)	100
Empfohlene Vorgehensweise zum Einrichten einer Offline-CA	102
Praktische Übung	103
Nachinstallationskonfiguration	106
Praktische Übung	113
Installieren einer untergeordneten Unternehmens-CA	116
Installieren eines Zertifikats einer untergeordneten Unternehmens-CA ...	119
Praktische Übung	120
Überprüfung der Installation	125
Vorbereitung einer Windows 2000-Gesamtstruktur	127
Zusammenfassung	129

Kapitel 4:

Verwaltung einer Zertifizierungsstelle	131 - 148
Einführung	133
PKI-Verwaltungsaufgaben	134
Rollentrennung	135
Aktivieren und Deaktivieren der Rollentrennung	136
Zuweisung von Standardrollen	137
Weitere PKI-Managementrollen	140
Erneuerung eines Zertifizierungsstellenzertifikats	143
Aktivierung der Überwachung der Zertifizierungsstelle	144
Praktische Übung	145
Zusammenfassung	148

Kapitel 5:

Planung und Implementierung der Notfallwiederherstellung	149 - 168
Einführung	151
Gründe für die Erstellung eines Notfall-Wiederherstellungsplans	152
Erforderliche Dokumentation	153
Auswahl einer Sicherungsmethode	154
Systemstatussicherung	154
Manuelle Sicherung	155
Durchführung einer Systemstatussicherung	156
Durchführung einer manuellen Sicherung	158
Wiederherstellungsmethoden	161
Praktische Übung	163
Praktische Übung	165
Zusammenfassung	167

Kapitel 6:

Entwurf von Zertifikatvorlagen	169 - 188
Einführung	171
Zertifikatvorlagen	172
Unternehmenszertifizierungsstellen und Zertifikatvorlagen	173
Speicherort der Definition von Zertifikatvorlagen	173
Zertifikatvorlagentypen	174
Vergleich von Vorlagen der Version 1 zu Version 2	174
Kategorien von Zertifikatvorlagen	176
Zertifikatvorlagen und Berechtigungen	178
Berechtigungen für Version 1-Zertifikatvorlagen	178
Berechtigungen für Version 2-Zertifikatvorlagen	179
Delegieren der Verwaltung von Zertifikatvorlagen	180
Praktische Übung	181
Aktualisierung von Zertifikatvorlagen	183
Praktische Übung	185
Empfehlungen für den Entwurf von Zertifikatvorlagen	187
Zusammenfassung	188

Kapitel 7:

Ausstellen von Zertifikaten	189 - 208
Einführung	191
Methoden zum Bereitstellen von Zertifikaten	192
Webbasierte Registrierung von Zertifikaten	194
Anforderung von Zertifikaten mit dem Zertifikatanforderungs-Assistent	196
Zertifikatregistrierung mit Certreq.exe	198
Methoden für die Aktivierung der automatischen Zertifikatregistrierung	199
Praktische Übung	202
Sperrungen von Zertifikaten	205
Praktische Übung	206
Zusammenfassung	208

Kapitel 8:

Archivierung der Verschlüsselungsschlüssel	209 - 230
Einführung	211
Gründe für das Wiederherstellen von privaten Schlüsseln	212
Dateiformat für das Exportieren von Schlüsseln und Zertifikaten	213
Tools für das Exportieren von Schlüsseln	214
Exportieren von Schlüsseln	215
Praktische Übung	216
Speicherorte privater Schlüssel auf Computern	218
Rollenvorteil bei der Schlüsselarchivierung	219
Aktivierung einer Zertifizierungsstelle für die Schlüsselarchivierung	220
Schlüsselwiederherstellungsprozess	223
Praktische Übung	225
Zusammenfassung	229

Kapitel 9:

Einsatz von Smartcards	231- 260
Einführung	233
Kombinierte Authentifizierung	234
Vorteile der Verwendung von Smartcards für die kombinierte Authentifizierung	235
Einsatzgebiete von Smartcards	236
Komponenten einer Smartcardinfrastruktur	237

Auswahl von Smartcards und Lesegeräten	239
Smartcardzertifikatvorlagen	241
Aktivieren von Smartcardzertifikatvorlagen.....	242
Methoden zur Zertifikatregistrierung	243
Konfiguration eines Registrierungs-Agenten	245
Registrierung eines Benutzers für ein Smartcardzertifikat.....	247
Gruppenrichtlinieneinstellungen für das Verwalten einer Smartcardinfrastruktur	249
Konfiguration von Gruppenrichtlinien für Smartcards	250
Behandeln häufiger Smartcardprobleme	252
Praktische Übung	253
Zusammenfassung	260

Kapitel 10:

Implementierung der SSL-Verschlüsselung

für Webserver	261 - 272
Einführung	263
SSL-Verschlüsselung	264
Funktionsweise der SSL-Verschlüsselung	265
Zertifikate für SSL	266
Ausstellung von Webserverzertifikaten.....	267
Praktische Übung	269
Zusammenfassung	272

Kapitel 11:

Sichere E-Mails

273 - 308	
Einführung	275
Sicherungsmethoden für E-Mails.....	276
Sicherung des Inhalts von E-Mail-Nachrichten	277
Digitale Signatur von E-Mails	277
Verfahrensweise der digitalen Signatur von E-Mails.....	278
Verschlüsselung von E-Mails	279
Wahl der Zertifizierungsstelle.....	280
Wahl der Zertifikatvorlage	281
Eine Zertifikatvorlage für Signatur und Verschlüsselung.....	282
Separate Zertifikatvorlagen	283
Wahl der Ausstellungsmethode für Zertifikate	285
Praktische Übung	286
Aktivierung sicherer E-Mail	289
Aktivierung von Outlook	290
Aktivierung von Outlook Express	291
Aktivierung von Outlook Web Access (OWA)	292
Versand sicherer E-Mails.....	293
Praktische Übung	295
E-Mail-Protokollsicherheit mit SSL.....	298
SSL-Ports für die E-Mail-Kommunikation	299
Installation und Aktivierung eines Webserver-Zertifikats	300
Aktivierung von SSL auf dem Exchange Server 2003	302
Aktivierung von SSL in der E-Mail-Anwendung	303
Praktische Übung	304
Zusammenfassung	308

Anhang A:

Wichtige Weblinks	309
--------------------------------	------------