



Workshop  
**Grundlagen der  
Microsoft  
Windows Server 2003-  
Zertifikatdienste (PKI)**

**Microsoft Windows Server 2003-Zertifikatdiensten (PKI)**  
Seminarunterlage – Artikelnr. PW-010505

Autor: Carlo Westbrook

Version: Mai 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.

CertPro ist eine eingetragene Marke von Carlo Westbrook.

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.).

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

# Inhaltsverzeichnis

| Inhalt  | Seite          |
|---|----------------|
| Voraussetzungen.....  | 6              |
| Zielgruppe.....   | 7              |
| Agenda .....  | 8              |
| Lernziel .....  | 9              |
| Zeitlicher Ablauf.....  | 10             |
| Rauminstallation .....  | 11             |
| <b>Einführung in die PKI.....</b>   | <b>12-25</b>   |
| Zweck einer PKI.....  | 13             |
| Komponenten einer PKI.....  | 14             |
| Zertifikate .....   | 15             |
| Lebensdauer digitaler Zertifikate.....  | 16             |
| Zertifizierungsstelle (Certificate Authority, CA) .....                       | 17             |
| Rollen in einer Zertifizierungsstellenhierarchie .....                        | 18             |
| Zertifikatsperrlisten .....   | 19             |
| PKI-fähige Anwendungen .....  | 20             |
| Zertifikatempfänger.....  | 21             |
| PKI-Tools .....   | 22             |
| <b>Praktische Übung .....</b>   | <b>23</b>      |
| <b>Grundlagen der Kryptografie .....</b>                                      | <b>26 - 34</b> |
| Einführung .....  | 27             |
| Symmetrische Datenverschlüsselung.....  | 28             |
| Asymmetrische Datenverschlüsselung.....                                       | 29             |
| Asymmetrische Signatur.....   | 30             |
| Kombination von asymmetrischer und symmetrischer Verschlüsselung....          | 32             |
| Digitale Signatur von Daten .....   | 33             |
| Kombination aus asymmetrischer Signatur und Hashalgorithmus .....             | 34             |
| <b>Entwerfen und Implementieren einer<br/>Zertifikatdiensthierarchie.....</b> | <b>35-74</b>   |
| Arten von Zertifizierungsstellen .....  | 36             |
| Struktur von Zertifizierungsstellen .....                                     | 37             |
| Schichtenmodelle einer Zertifizierungsstellenhierarchie.....                  | 38 - 42        |
| Einschichtige Zertifizierungsstellenhierarchie .....                          | 39             |
| Zweischichtige Zertifizierungsstellenhierarchie .....                         | 40             |
| Dreischichtige Zertifizierungsstellenhierarchie .....                         | 41             |
| Vierschichtige Zertifizierungsstellenhierarchie.....                          | 42             |
| Ermitteln von Anforderungen .....   | 43             |
| Minimierung des Ausfallrisikos .....  | 44             |
| Absichern und Optimieren einer Offline-Zertifizierungsstelle.....             | 45             |
| Absichern und Optimieren einer Online-Zertifizierungsstelle.....              | 46             |
| Gültigkeitsdauer von Zertifikaten .....                                       | 47             |
| Veröffentlichungspunkte .....   | 48             |
| Die Datei CAPolicy.inf.....   | 49             |
| Zertifikatverwendungserklärung (CPS).....                                     | 51             |
| Einstellungen für eine Offline-Zertifizierungsstelle.....                     | 53             |
| Sicherheitsmaßnahmen bei der Konfiguration.....                               | 54             |
| <b>Praktische Übung .....</b>   | <b>57</b>      |

|   |                |
|---|----------------|
| Nachinstallationskonfiguration .....  | 60             |
| <b>Praktische Übung</b> .....   | <b>64</b>      |
| Installieren einer untergeordneten Unternehmens-CA .....                    | 67             |
| Installieren eines Zertifikats einer untergeordneten Unternehmens-CA .....  | 68             |
| <b>Praktische Übung</b> .....   | <b>69</b>      |
| Überprüfung der Installation .....  | 74             |
| <br>  |                |
| <b>Administration einer PKI im Überblick.....</b>                           | <b>75-141</b>  |
| PKI-Verwaltungsaufgaben .....   | 76             |
| Rollentrennung .....  | 77             |
| Aktivieren und Deaktivieren der Rollentrennung.....                         | 78             |
| Zuweisung von Standardrollen.....   | 79             |
| Weitere PKI-Managementrollen.....   | 81             |
| Erneuerung eines Zertifizierungsstellenzertifikats .....                    | 84             |
| Aktivierung der Überwachung der Zertifizierungsstelle.....                  | 85             |
| <b>Praktische Übung</b> .....   | <b>86</b>      |
| Notfallwiederherstellung .....  | 89             |
| Erstellung eines Notfall-Wiederherstellungsplans.....                       | 90             |
| Auswahl einer Sicherungsmethode .....                                       | 91             |
| Durchführung einer Systemstatussicherung .....                              | 92             |
| Durchführung einer manuellen Sicherung.....                                 | 94             |
| Wiederherstellungsmethoden .....  | 97             |
| <b>Praktische Übung</b> .....   | <b>99</b>      |
| <br>  |                |
| <b>Zertifikatvorlagen und Zertifikate.....</b>                              | <b>102-126</b> |
| Zertifikatvorlagen .....  | 103            |
| Zertifikatvorlagentypen.....  | 105            |
| Kategorien von Zertifikatvorlagen .....                                     | 106            |
| Zertifikatvorlagen und Berechtigungen .....                                 | 108            |
| Delegieren der Verwaltung von Zertifikatvorlagen .....                      | 109            |
| <b>Praktische Übung</b> .....   | <b>110</b>     |
| Aktualisieren von Zertifikatvorlagen .....                                  | 112            |
| <b>Praktische Übung</b> .....   | <b>113</b>     |
| Ausstellen von Zertifikaten.....  | 115-126        |
| Methoden zum Bereitstellen von Zertifikaten .....                           | 116            |
| Webbasierte Registrierung von Zertifikaten .....                            | 117            |
| Anforderung von Zertifikaten mit dem Zertifikatanforderungs-Assistent.....  | 118            |
| Zertifikatregistrierung mit Certreq.exe.....                                | 119            |
| Aktivierung der automatischen Zertifikatregistrierung.....                  | 120            |
| <b>Praktische Übung</b> .....   | <b>121</b>     |
| Sperrern von Zertifikaten.....  | 124            |
| <b>Praktische Übung</b> .....   | <b>125</b>     |
| <br>  |                |
| <b>Archivierung der Verschlüsselungsschlüssel.....</b>                      | <b>127-141</b> |
| Gründe für das Wiederherstellen von privaten Schlüsseln .....               | 128            |
| Dateiformat für das Exportieren von Schlüsseln und Zertifikaten .....       | 129            |
| Tools für das Exportieren von Schlüsseln.....                               | 130            |
| <b>Praktische Übung</b> .....   | <b>131</b>     |
| Speicherorte privater Schlüssel auf Computern .....                         | 133            |
| Rollenverteilung bei der Schlüsselarchivierung .....                        | 134            |
| Aktivierung einer Zertifizierungsstelle für die Schlüsselarchivierung ..... | 135            |
| <b>Praktische Übung</b> .....   | <b>136</b>     |
| Schlüsselwiederherstellungsprozess .....                                    | 140            |

---

|  |                |
|--|----------------|
| <b>Einsatz von Smartcards .....</b>                                    | <b>142-160</b> |
| Kombinierte Authentifizierung .....                                    | 143            |
| Vorteile der Verwendung von Smartcards .....                           | 144            |
| Einsatzgebiete für Smartcards .....                                    | 145            |
| Komponenten einer Smartcard-Infrastruktur .....                        | 146            |
| Smartcard-Zertifikatvorlagen .....                                     | 147            |
| Aktivieren von Smartcard-Vorlagen .....                                | 148            |
| Methoden zur Zertifikatregistrierung .....                             | 149            |
| Konfiguration eines Registrierungs-Agenten .....                       | 150            |
| Registrieren eines Benutzers für ein Smartcardzertifikat.....          | 151            |
| Konfiguration von Gruppenrichtlinien für die Smartcard-Verwendung..... | 152            |
| Behandeln häufiger Probleme bei der Smartcard-Verwendung .....         | 153            |
| <b>Praktische Übung .....</b>  | <b>154</b>     |
| <br>   |                |
| <b>Implementierung der SSL-Verschlüsselung</b>                         |                |
| <b>für Webserver .....</b>   | <b>161-168</b> |
| Funktionsweise der SSL-Verschlüsselung .....                           | 162            |
| Zertifikate für SSL-Verschlüsselung .....                              | 164            |
| Ausstellung von Webserver-Zertifikaten .....                           | 165            |
| <b>Praktische Übung .....</b>  | <b>166</b>     |
| <br>   |                |
| <b>Weitere Informationen.....</b>                                      | <b>169-172</b> |
| Wichtige Weblinks .....  | 170            |
| Kurshinweis .....  | 171            |
| Fragen .....   | 172            |