Schlüsselarchivierung und -wiederherstellung

Zertifizierte Sicherheit

von Marc Grote

Was versteckt sich hinter den Begriff PKI und wie wird bei Windows Server 2003 eine CA (Certificate Authority) implementiert? Hier gibt ein Profi detailliert Auskunft zu diesen wichtigen Sicherheitsthemen und beschreibt unter anderem auch die bis zu Windows 2003 fehlende Möglichkeit der zentralen Archivierung ausgestellter Zertifikate.

Mit der Einführung von Windows 2003 wurden die CA-Komponenten (Certificate Authority) des Windows-Servers von Microsoft erheblich erweitert und verbessert, sodass diese eine sinnvolle Inhouse-CA im Rahmen einer Microsoft basierten PKI (Public Key Infrastructure) abbilden können. Doch bevor näher auf diese Verbesserungen eingegangen wird, soll zunächst einmal der Begriff PKI näher erläutert werden.

So genannte PKIs (Public Key Infrastructures) bestehen aus Protokollen, Diensten, Organisation und Standards, die verschiedene Applikationen für die Public-Key-Verschlüsselung unterstützen. Sie stellen einer Organisation damit eine ganzheitliche Infrastruktur zur Implementierung von sicheren Diensten zur Verfügung. In einer PKI wird Benutzern, Computern und Diensten ein kryptographisches Schlüsselpaar zugewiesen, das sich aus einem Public- und einem Private-Key zusammensetzt. Die beiden Schlüssel stehen in einem mathematischen Verhältnis zueinander. Der Public-Key wird veröffentlicht, während der Private Key geheim gehalten wird.

Die Implementation einer Microsoft CA sieht zwei Arten von Zertifizierungsstellen vor, zu denen die Stammzertifizierungsstellen und die eigenständigen Zertifizierungsstellen gehören. Eine Stammzertifizierungsstelle ist in Active Directory integriert und stellt die flexibelste Form einer CA im Microsoft-Umfeld dar. Sie ist für den Inhouse-Einsatz mit erweiterten Möglichkeiten wie beispielsweise der automatischen Zertifikatseinschreibung, Key-Recovery und vielen anderen Tätigkeiten prädestiniert. Eine eigenständige Zertifizierungsstelle eignet sich insbesondere für die Verwendung in einer CA-Hierarchie als Offline-CA oder als CA für externe Vertragspartner und Lieferanten zur Einrichtung einer sicheren Infrastruktur. Solche Zertifizierungsstellen können auch kaskadiert werden. Dabei bildet die Root CA dann die Wurzel dieser Struktur, während unter ihr so genannte Intermediate CAs aufgebaut werden können. Diese Kette wird dann von so genannten „Issuing CAs" abgeschlossen, die Zertifikate für die allgemeine Verwendung ausstellen. Die PKI-Implementierung von Microsoft kann dabei in ganz unterschiedlichen Einsatzgebieten zum Einsatz kommen:

- S/MIME Implementation in Outlook 2000, XP und 2003,
- Smartcard-Anmeldung für Windows 2000 Professional und Windows XP Professional,
- EFS in Windows 2000 Professional, Windows XP Professional und Windows Server 2003,
- IPSEC, implementiert in Windows 2000 Professional und Windows XP Professional sowie Windows Server 2003,
- IPSec und VPN-Tunnel für Router sowie
- SSL/TLS-Implementation für Windows 2000- und Windows Server 2003-Webserver.

Es existieren noch weitere Verwendungszwecke wie beispielsweise die digitalen Signaturen für Treiber und Codesignaturen, auf sie wird im Rahmen dieses Artikels jedoch nicht näher eingegangen.

Microsoft hat mit der Markteinführung von Windows 2003 eine komplett überarbeitete CA zur Verfügung gestellt, die eine Vielzahl neuer Funktionen zur Verfügung stellt und einige Schwachstellen in der bisherigen Implementation einer CA unter Windows 2000 beseitigt. Je nach Version des Windows Servers 2003 stehen dabei unterschiedliche CA-Features zur Verfügung:

- Windows 2003 Server in der „Web-Version besitzt keine eigene CA.
- Windows 2003 Server in der Standardversion kann eine CA-Hierarchie aufbauen. Die Features sind jedoch mit denen in einer Windows-2000-CA vergleichbar.
- Der Windows Server 2003 in der Enterprise- und -Datacenter-Version, kann eine CA-Hierarchie aufbauen. In dieser Version sind auch die meisten Änderungen und Neuerungen zu finden.

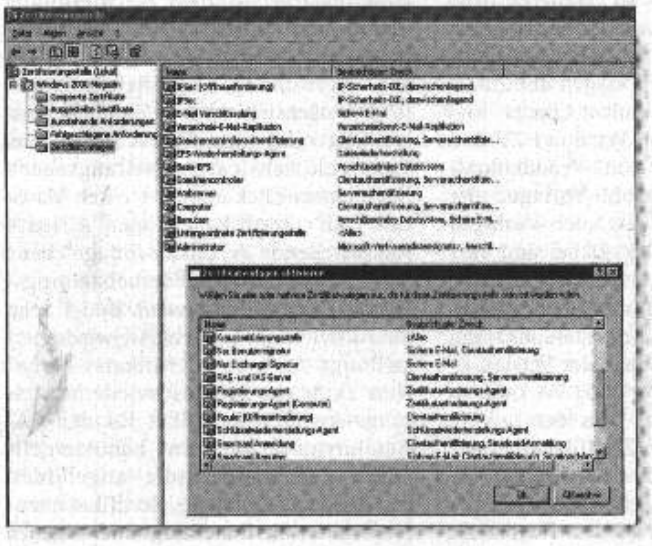

Bild 1. Die Zertifizierungsstelle auf dem Windows Server 2003: Hier die Aktivierung des Schlüsselwiederherstellungs-Agenten „Zertifikatsvorlage".

Dementsprechend beschreibt dieser Artikel ausführlich die CA-Funktionen einer Windows 2003 Enterprise-CA. Die PKI von Windows Server 2003 erfüllt die Anforderungen für FBCA-Interoperabilität (Federal Bridge CA) und unterstützt so genannte Cross CAs. Zudem wurde der Zertifizierungsstelle von Windows Server 2003 ein Feature „qualifizierte Unterordnung" hinzugefügt. Eine übergeordnete Zertifizierungsstelle ist nun in der Lage, bestimmte Einschränkungen auf eine untergeordnete Zertifizierungsstelle anzuwenden, wie beispielsweise Richtlinien, Namen- und Richtlinienbeschränkungen sowie Richtlinienzuordnungen. Dieses Feature kann in Situationen sinnvoll sein, in denen die übergreifende Zertifizierung einer Zertifizierungsstelle mit der Zertifizierungsstelle einer anderen Organisation erforderlich ist und Einschränkungen für die Zertifizierung gelten müssen.

Die Zertifizierungsstelle erlaubt die Definition verschiedener so genannter Betriebsrollen (Role Separation), damit die Verantwortlichkeiten und dementsprechend die Berechtigungen von Zertifizierungsstellenadministratoren und Zertifikatausstellern getrennt werden können. Außerdem ist es nun möglich, die Zertifizierungsstelle des Windows Server 2003 für die automatische Registrierung von Benutzer- und Computerzertifikaten (Certificate Autoenrollment) zu konfigurieren. Benutzer können bei der erstmaligen Anmeldung an einer Domäne Zertifikate verschiedenen Typs erhalten (beispielsweise für EFS, Signatur, E-Mail-Verschlüsselung oder Smartcardanmeldung). Zusätzlich kann die Zertifizierungsstelle in regelmäßigen Intervallen Delta-Zertifikatsperrlisten (Delta Revocation Lists) zu den Standard-CRL generieren. Damit wird die Leistung der Zertifikatsperrlistenveröffentlichung verbessert und die Netzwerklast reduziert, da nur die Änderungen aus der vorherigen Zertifikatsperrliste verteilt werden.

Eine weitere Änderung betrifft die Schlüsselarchivierung und -wiederherstellung (Key Archiving and -Recovery): Die Zertifizierungsstelle kann den privaten Schlüssel eines Benutzers archivieren, wenn er generiert wird. Dabei wird der Schlüssel mit dem öffentlichen Schlüssel der Zertifizierungsstelle verschlüsselt. Alle Wiederherstellungsagenten der Zertifizierungsstelle können den verschlüsselten Schlüssel entschlüsseln, damit dieser dem Benutzer zur Verfügung gestellt werden kann, falls der Benutzer den privaten Schlüssel verliert. Diese Vorgehensweise ist besonders in Unternehmensszenarien sinnvoll, weil der Verlust des Schlüssels häufig vorkommt. Sie ändert jedoch das Sicherheitsparadigma: Nun ist ein anderer Agent als der eigentliche Benutzer im Besitz des privaten Schlüssels. Deshalb muss die Schlüsselarchivierung und -wiederherstellung einwandfrei verwaltet werden, damit die Vertrauensstellungen nicht gefährdet sind. Mit Windows Server 2003 ist es nun auch möglich,

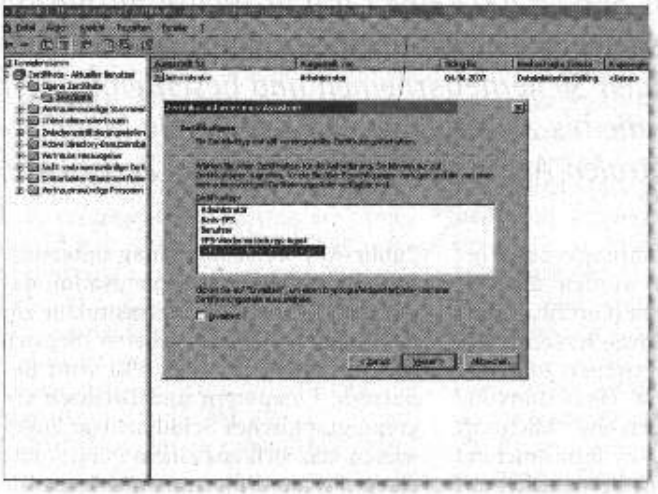

Bild 2. Ein Schlüsselwiederherstellungs-Agenten-Zertifikat für den CA-Administrator wird hier über eine benutzerdefinierte Zertifikatskonsole angefordert. Dazu ist die Erstellung einer eigenen Microsoft Management Console (MMC) erforderlich.

Zertifikatsvorlagen zu modifizieren, vorhandene Vorlagen zu kopieren und deren Verwendungszweck anzupassen. Windows 2000-Clients und -Zertifikatdienste können nur Vorlagen der „TAG-Version 1TAG" verwenden. Clients- und Zertifikatsdienste von Windows XP und der Windows Server 2003-Produktfamilie unterstützen sowohl Vorlagen der „TAGVersion 1TAG" als auch Vorlagen der „TAGVersion 2TAG". Dabei sind Vorlagen der Version 1 schreibgeschützt. Wenn sie jedoch dupliziert werden, handelt es sich bei dem Vorlagenduplikat um eine bearbeitbare Vorlage der Version 2.

Die Windows Server 2003 CA kann so konfiguriert werden, dass der private Schlüssel bestimmter Zertifikate bei deren Ausstellung archiviert wird. Archivierte private Schlüssel können im Falle eines Verlustes wiederhergestellt werden. Dieser Prozess ist in zwei Phasen implementiert: der Schlüsselarchivierung und der Schlüsselwiederherstellung.

Wie läuft eine solche Schlüsselarchivierung ab? Beim Abrufen eines Zertifikats sucht der Antragsteller die entsprechende Zertifikatvorlage, stellt die für diese Vorlage erforderlichen Informationen zusammen und stellt diese dann der Zertifizierungsstelle (CA) bereit. Diese Informationen enthalten zum Beispiel den Namen des Antragstellers, den öffentlichen Schlüssel und die unterstützen Kryptografie-Algorithmen. Wenn die Schlüsselarchivierung konfiguriert ist, stellt der Antragsteller der Zertifizierungsstelle außerdem seinen privaten Schlüssel bereit. Die Zertifizierungsstelle speichert diesen privaten Schlüssel in der CA-Datenbank, bis die Schlüsselwiederherstellung genutzt werden soll. Der private Schlüssel ausgestellter Zertifikate wird jedoch standardmäßig nicht archiviert. Von einer CA ausgestellte Zertifikate für eine elektronische Signatur können nicht archiviert werden.

Bevor ein Administrator die Zertifizierungsdienste nutzen kann, müssen diese über die Systemsteuerung und die Applet Software installiert werden. Nach erfolgter Installation findet sich die Zertifizierungsstelle unter „Start - Alle Programme - Verwaltung - Zertifizierungsstelle". Der nächste Schritt ist dann die Ausstellung einer Zertifikatsvorlage vom Typ Schlüsselwiederherstellungsagent. Nach einem Klick mit der rechten Maustaste auf „Zertifikatvorlagen - Neu - Auszustellende Zertifikatsvorlage" kann der „Schlüsselwiederherstellungs-Agent" ausgewählt werden. Bild 1 zeigt die Aktivierung des Schlüsselwiederherstellungs-Agenten „Zertifikatsvorlage". Nun kann ein Schlüsselwiederherstellungs-Agenten-Zertifikat für den CA-Administrator über eine benutzerdefinierte Zertifikatskonsole angefordert werden. Um ein solches Zertifikat anzufordern, ist die Erstellung einer eigenen Microsoft Management Console (MMC) erforderlich, der das Zertifikats-Snap-In für das eigene Benutzerkonto hinzuge-

fügt werden muss. Nun muss ein neues Zertifikat vom Typ Schlüsselwiederherstellungs-Agent anfordert (Bild 2) und dem neuen Zertifikat ein Namen gegeben werden. Für dieses Szenario wurde in diesem Beispiel der Name KRA (Key Recovery Agent) ausgewählt. Nach erfolgter Anforderung des Zertifikates

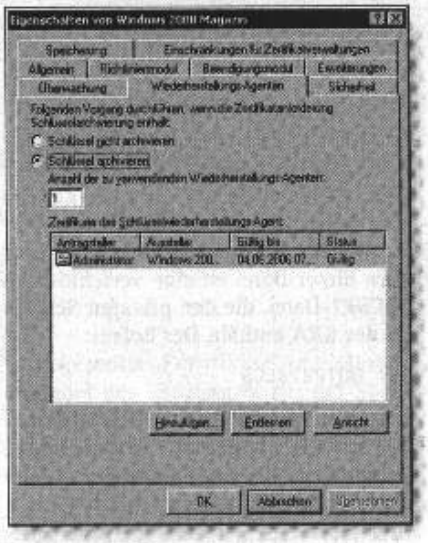

Bild 3. Die Aktivierung der Schlüsselarchivierung: Sie ist in den Eigenschaften des Zertifikatsservers im hier gezeigten Reiter „Wiederherstellungs-Agenten" zu finden.

muss dieses, aufgrund der nicht unerheblichen Bedeutung eines Schlüsselwiederherstellungs-Agenten, vom CA-Administrator manuell ausgestellt werden, um einen etwaigen Missbrauch zu verhindern. Dazu muss der Administrator das Zertifizierungsstellen-Snap-In starten und das KRA-Zertifikat im Container „Ausstehende Anforderungen" ausstellen. Jetzt kann die Schlüsselarchivierung für die Zertifizierungsstelle aktiviert werden. Dies ist in den Eigenschaften des Zertifikatsservers im Reiter „Wiederherstellungs-Agenten" zu finden, wo die Schlüsselarchivierung aktiviert werden muss. Die Windows 2003 Enterprise CA erlaubt die Einrichtung eines Vier-Augen-Prinzips zur Schlüsselwiederherstellung. Mit dieser Einstellung ist eine Schlüsselwiederherstellung nur möglich, wenn zum Beispiel zwei Wiederherstellungs-Agenten konfiguriert sind. Dann kann das Zertifikat des Schlüsselwiederherstellungs-Agenten ausgewählt werden (Bild 3). Nach erfolgter Installation müssen die Zertifikatdienste neu gestartet werden.

Hierbei ist es ganz wichtig zu wissen, dass dieses Zertifikat „Key Recovery Agent" (KRA) nicht automatisch in den Zertifikatsspeicher des Benutzers eingetragen wird. Es muss in den Eigenschaften der Zertifizierungsstelle oder im Container „Ausgestellte Zertifikate" exportiert und in den Zertifikatsspeicher des KRA-Benutzers (in diesem Fall der Administrator) importiert werden. Wird dieser Schritt nicht ausgeführt, so ist die Wiederherstellung des Zertifikates mit Hilfe des „Key Recovery Tools" (KRT) oder CERTUTIL nicht möglich, weil kein KRA-Zertifikat im Zertifikatspeicher des KRA gefunden werden kann. Deshalb muss das Zertifikat nun über den Container „Ausgestellte Zertifikate" in der Zertifizierungsstelle exportiert werden. Dazu muss das Zertifikat „Schlüsselwiederherstellungs-Agenten" ausgewählt und im Reiter „Details" exportiert werden, indem man dort auf „In Datei kopieren" klickt. Man sollte hier den Vorschlägen des Assistenten folgen, der vorschlägt DER-codiert-binär X.509 (.CER) zu wählen und dann noch einen Pfad und Dateinamen für das zu exportierende Zertifikat auswählen. Der Import des Zertifikats in den Zertifikatsspeicher des Benutzers stellt dann den letzten Schritt dar: Dazu wird wiederum eine MMC geöffnet und das Zertifikats-Snap-In für den aktuellen Benutzer hinzugefügt. Anschließend wird das KRA-Zertifikat in den Container „Eigene Zertifikate" – „Zertifikate" importiert. Jetzt kann der Administrator damit anfangen, Zertifikate für seine Anwender auszustellen und für diese dann die Schlüsselarchivierung zu aktivieren. Dazu wird das Zertifizierungsstellen-SnapIn geöffnet, in dem dann die Konsole der Zertifikatsvorlagenverwaltung zu öffnen ist.

Wie bereits erwähnt, besteht eine Besonderheit einer Windows-2003-CA darin, dass hier die Möglichkeit existiert, neben so genannten v1-Zertifikatvorlagen auch v2-Zertifikatvorlagen auszustellen. v1- und v2-Zertifikatvorlagen können dupliziert und deren Eigenschaften angepasst werden, jedoch ist nur eine Windows 2003 Enterprise- und –Datacenter CA dazu in der Lage, auch v2-Zertifikatvorlagen auszustellen.

Microsoft Certification Authorities unterstützen zwei Arten von Templates: Version 1 und Version 2. Version-1-Templates bieten Legacy-Unterstützung für Windows 2000 CAs. Solche V1-Templates werden per Default erstellt, können jedoch nicht modifiziert und entfernt werden. Durch die Duplizierung eines v1-Templates entsteht dann aber ein v2-Template. Nur Windows 2003 Enterprise und –Datacenter unterstützen zusätzlich zu den v1- auch die v2-Templates. Sie sind nur in einer Enterprise-CA-Konfiguration verfügbar, weil sie Active Directory benötigen. Diese V2-Funktonalität ist beispielsweise dann notwendig, wenn es darum geht, die Schlüsselarchivierung zu aktiveren. Als Beispiel soll nun die Zertifikatvorlage „Exchange-Benutzer" ausgewählt werden. Im Kontextmenü kann dann auf „Doppelte Vorlage" geklickt werden. Anschließend wird hier der neuen Vorlage der Namen „E-Mail Verschlüsselung" gegeben. Wird danach auf den Reiter „Anforderungsverarbeitung" geklickt, so kann anschließend das Feld „Privaten Schlüssel für die Verschlüsselung archivieren" ausgewählt werden. Die neue Zertifikatsvorlage für die Zertifizierungsstelle muss nun noch veröffentlicht werden, damit Clients das neue Zertifikat anfordern können. Für eine unternehmensweite Verteilung des neuen Zertifikats empfiehlt sich die automatische Zertifikatsregistrierung über die Gruppenrichtlinien des Windows 2003 Active Directory. Die automatische Zertifikatseinschreibung ist jedoch nicht Fokus dieses Artikels.

Hier soll als nächster Schritt ein E-Mail Verschlüsselungszertifikat für den Benutzer W2KMAG angefordert werden, wofür zwei Möglichkeiten zur Verfügung stehen: Die Anforderung eines Zertifikates über eine MMC oder über die webbasierte Zertifikatseinschreibung. Der Autor bevorzugt die Anforderung von Zertifikaten für Benutzer über den Internet Explorer, weil hierzu keine umständliche Konfiguration erforderlich ist und die Benutzer das „Look and Feel" von Webseiten in der Regel gewohnt sind. Der Aufruf der webbasierten Zertifikatseinschreibung erfolgt durch Eingabe der folgenden URL:

```
http://servername/certsrv.
```

Nun ist es mithilfe des ausgestellten Zertifikats möglich, E-Mails zu verschlüsseln und diese zur sicheren Kommunikation mit anderen Personen zu verwenden. Die Konfiguration von Outlook und Exchange zur Verwendung von E-Mail Verschlüsselung liegt außerhalb des Fokus dieses Artikels. An dieser Stelle ist es wichtig anzumerken, dass die Schlüsselarchivierung nicht für Zertifikate ausgestellt werden kann, deren Zweck nur die Signaturverwendung ist.

Der zweite wichtige Schritt ist sicher die Schlüsselwiederherstellung. So können Antragsteller ihren privaten Schlüssel auf verschiedene Weisen verlieren, beispielsweise durch versehentliches Löschen oder aber auch durch bewussten Missbrauch. Möglicherweise möchte ein Administrator auch den Schlüssel eines bestimmten Antragstellers wiederherstellen, um auf die durch diesen Schlüssel geschützten Daten zuzugreifen. Die Schlüsselwiederherstellung kann immer verwendet werden, wenn der Schlüsselarchivierungsprozess den privaten Schlüssel des Antragstellers gespeichert hat. Beim Schlüsselwiederherstellungsprozess muss ein Administrator das verschlüsselte Zertifikat und den privaten Schlüssel abrufen. Daran anschließend muss ein Schlüsselwiederherstellungs-Agent (Key Recovery Agent, KRA) diesen an die Zertifizierungsstelle senden. Wenn eine korrekt signierte Schlüsselwiederherstellungsanforderung empfangen wird, werden dem Anfordernden das Zertifikat und der private Schlüssel des Antragstellers bereitgestellt. Anschließend verwendet der Anfordernde den Schlüssel nach Bedarf oder überträgt diesen sicher an den Antragsteller, der ihn dann weiterverwenden kann. Da der private Schlüssel nicht zwangsläufig gefährdet wird, sind keine erneute Zertifizierung oder erneute Eingaben erforderlich.

Hat ein Benutzer das Zertifikat mit dem privaten Schlüssel zur E-Mail-Verschlüsselung „verloren", so ist er nicht mehr in der Lage, seine E-Mails zu verschlüsseln. Wesentlich gravierender ist in diesem Fall aber die Tatsache, dass nun auch keine E-Mails mehr entschlüsselt werden können. Ohne eine zentrale Schlüsselarchivierung wäre jetzt guter Rat teuer. Mithilfe der automatischen Zertifikatsarchivierung von Windows 2003 ist das Zertifikats-Recovery jedoch ein leichtes Unterfangen, dessen technischer Ablauf im folgenden Abschnitt geschildert wird. Dabei wird hier davon ausgegangen, dass der private Schlüssel eines Benutzers verloren gegangen ist oder korrumpiert wurde. Dann wird die Seriennummer des Zertifikats durch den Zertifikats-Manager ermittelt. Dieser extrahiert den privaten Schlüssel und das Zertifikat aus der CA-Datenbank. Das Export-Format ist „PKCS#7", es ist mit dem öffentlichen Schlüssel des KRA Zertifikats verschlüsselt. Der Zertifikats-Manager kann das Key Recovery Tool (KRT.EXE) oder auch CERTUTIL -Getkey nutzen, um das PKCS7#-File zu erstellen. Die PKCS#7-Datei wird dann zum KRA transportiert. Weil diese Datei verschlüsselt ist, kann nur der KRA den privaten Schlüssel und das Zertifikat entschlüsseln. Er entschlüsselt das Zertifikat und den privaten Schlüssel von der verschlüsselten PKCS#7-Datei auf einer Recovery-Workstation, wobei die Extraktion d mit CERTUTIL-RECOVERKEY oder KRT.EXE durchgeführt wird. Anschließend werden der private Schlüssel und das Zertifikat in einer PKCS#12-Datei gespeichert. Der KRA sendet dann diese PKCS#12-Datei an den Benutzer, welcher das Zertifikat und den privaten Schlüssel in den Zertifikatsspeicher importieren kann. Für das Key-Recovery steht grundsätzlich der Einsatz der zwei Tools „CERTUTIL.EXE" und „KRT.EXE" zur Verfügung. Dabei ist „CERTUTIL" Bestandteil jeder Implementation einer Windows-2003-CA und dient der Verwaltung dieser CA über die Kommandozeile. Obwohl beim Einsatz von CERTUTIL nach Meinung des Autors sehr kryptische Kommandos zum Einsatz kommen, stellt dieses Programm ein sehr mächtiges Tool zur CA-Verwaltung dar. Mit Erscheinen der Windows 2003 Resource Kit Tools steht den Administratoren mit dem Key Recovery Tool (KRT.EXE) aber auch ein grafisches Utility zur Schlüsselwiederherstellung zur Verfügung. KRT verwendet ein grafisches Frontend, das dann im Hintergrund wieder CERTUTIL aufruft. Wie läuft nun eine Wiederherstellung mit CERTUTIL.EXE ab? Dazu muss zunächst der folgende Befehl von der Kommandostelle aus eingegeben werden:

```
CERTUTIL -GETKEY <Seriennummer>
OUTPUTBLOB
```

Mit diesem Befehl wird dann eine Datei mit dem Namen „OUTPUTBLOB" erzeugt. Dabei handelt es sich um eine PKCS#7-Datei, in der die KRA-Zertifikate sowie das Benutzerzertifikat und die Zertifikatkette enthalten sind. Der Kern dieser Datei ist eine verschlüsselte PKCS#7-Datei, die den privaten Schlüssel des KRA enthält. Der Befehl:

```
Dir OUTPUTBLOB
```

Zeigt dann den „OUTPUTBLOB" an. Sollte nichts angezeigt werden, so ist vermutlich die Seriennummer falsch eingegeben worden. Mit

```
CERTUTIL -RECOVERKEY OUTPUTBLOB
W2KMAG.PFX
```

wird der private Schlüssel aus dem OUTPUTBLOB in der Datei W2KMAG.PFX wiederhergestellt. PCKS-Dateien mit der Endung „.PFX" (Private File Exchange) enthalten einen privaten Schlüssel. Die Output-Datei wird dann mit einem Kennwort verschlüsselt. Dazu muss man nach der entsprechenden Aufforderung ein neues Kennwort angeben und dieses anschließend bestätigen.

Eine solche Wiederherstellung ist aber auch mit dem Werkzeug „KRT.EXE" möglich. Dazu müssen die Windows 2003 Resource Kit Tools installiert werden. Diese sind unter der folgenden Adresse zu finden:

```
http://www.microsoft.com/downlo-
ads/details.aspx?FamilyID=9d467a6
9-57ff-4ae7-96ee-
b18c4790cffd&DisplayLang=en
```

Nach dem Start des Tools KRT.EXE kann die Certification Authority (CA) ausgewählt werden. In dem Feld „Search Criteria" stehen diverse Möglichkeiten zur Verfügung, um das wiederherzustellende Zertifikat zu ermitteln. Wir wählen in diesem Artikel die „Certificate Serial Number". Die Seriennummer des Zertifikates kann ermittelt werden, indem die Zertifikatsserverkonsole gestartet wird. Dort kann dann im Container

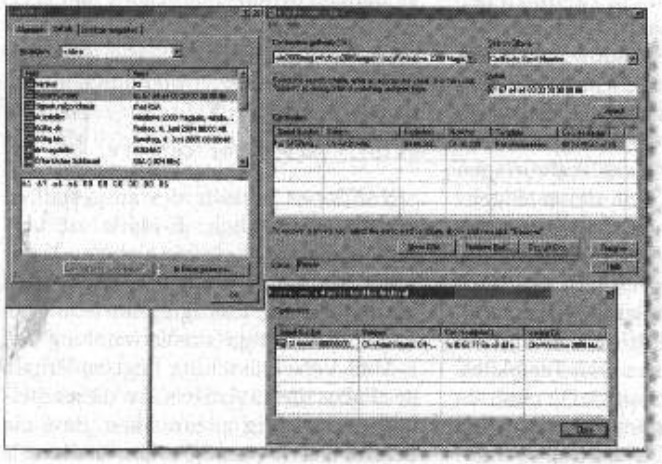

Bild 4. Wiederherstellung auf die grafische Art: Das Werkzeug „KRT.EXE" aus dem Windows 2003 Resource Kit Tools.

„Ausgestellte Zertifikate" die Seriennummer des Zertifikates aus der Spalte „Seriennummer" entnommen werden. Diese ermittelte Seriennummer wird dann im Feld „Value" eingegeben, anschließend kann man auf „Search" klicken und im Feld „Certificates" wird dann das wiederherzustellende Zertifikat angezeigt. Mit einem Klick auf „Recover" soll dann das Zertifikat wiederhergestellt werden. Im folgenden Fenster muss der Pfad zu dem wiederherzustellenden Zertifikat angeben werden. Nun wird eine Datei erstellt, die aus der Seriennummer des Zertifikats und dem Suffix .PFX (Private File Exchange) besteht. Ein Beispiel wäre der Dateiname „6167a4a4000000000006.pfx". Die Eingabe eines Kennwortes zum Schutz des Zertifikates vor Missbrauch ist zwingend. Das Bild 4 zeigt die Verwendung des Key Recovery Tools. Dieses Zertifikat muss dem Benutzer noch zur Verfügung gestellt werden. Der Autor empfiehlt den Transport auf einem sicheren Weg und rät von einer unverschlüsselten Übertragung per E-Mail ab, weil der private Schlüssel des Benutzers im wiederhergestellten Zertifikat gespeichert ist. Befindet sich das Zertifikat schließlich auf dem PC des Benutzers, so kann es dieser durch einen einfachen Doppelklick installieren. Anhand der Zertifikatseigenschaften wird der richtige Zertifikatsspeicher automatisch gewählt.

Auch hier wieder ein ganz wichtiger Hinweis für die Praxis: Sollte bei der Verwendung des Key Recovery Tools (KRT) von Windows 2003 keine konfigurierte CA angezeigt werden, obwohl eine CA installiert ist, liegt das daran, dass KRT.EXE die englischsprachige Version von CERTUTIL.EXE verwendet. Auch wer einen deutschen Windows 2003 Server einsetzt, muss in diesem Fall eine englischsprachige Version von CERTUTIL.EXE verwenden. Beim Austausch der CERTUTIL.EXE ist unbedingt auch der DLLCACHE zu beachten, der die Datei sonst wieder ersetzen würde. Die „neue" Datei muss sowohl in das Verzeichnis DLLCACHE als auch in das SYSTEM32-Verzeichnis kopiert werden.

Eine zentrale Zertifikatsarchivierung birgt jedoch auch einige Gefahren. Da wäre zum einen die Bedrohung durch Daten- oder Hardware-Diebstahl. Man muss sich vorstellen, dass der CA-Server gestohlen wird oder ein Angreifer Zugriff auf die archivierten Zertifikate erlangt. Die gesamte PKI wäre damit auf einem Schlag kompromittiert und alle ausgestellten Zertifikate würden ihren Bestimmungszweck verlieren. Die Folgen davon wären sicher fatal. Der Administrator müsste jedes Zertifikat erneut ausstellen und auch Verfahren, die von Zertifikaten abhängig sind, eventuell komplett erneut konfigurieren. Gegen Daten- oder Hardware-Diebstahl sollte man sich, wie bei allen wichtigen Serversystemen, grundsätzlich mit Zugangs- und Zugriffskontrollsystemen schützen. Allerdings stellt auch der CA-Administrator (Key Recovery Agent) selbst ein weiteres Bedrohungspotential dar. Da der KRA Zugriff auf sämtliche archivierten Zertifikate hat, wäre es für diesen eine leichte Aufgabe, verschlüsselte Information zu entschlüsseln und so an geheime Informationen zu gelangen. Um das Bedrohungspotential „Administrator" zu reduzieren, helfen organisatorische Maßnahmen wie die Einstellung von vertrauenswürdigen Administratoren nur nach eingehender Prüfung, die regelmäßige Kontrolle der CA durch einen Datenschutzbeauftragten, die Einrichtung des Vier-Augen-Prinzips für die Wiederherstellungsagenten oder auch die so genannte Role-Separation. Dabei handelt es sich um ein neues Feature einer Windows 2003 Enterprise CA, bei deren Verwendung die einzelnen CA-Verwaltungsaufgaben an verschiedene Benutzer delegiert werden können. Aber auch die „Role Separation" kann jederzeit durch einen lokalen Administrator (und damit auch durch den Domänen Administrator) deaktiviert werden. Ebenso kann dieser Personenkreis die CA-Rollen verändern. Abschließend soll nicht unerwähnt bleiben, dass auch hier die Grundlage jeder Sicherungsmaßnahme natürlich ein ordnungsgemäßes und funktionierendes Backup ist. *(fms)*

Der Autor

Marc Grote ist MVP (Microsoft Most Value Professional), Microsoft Certified System Engineer und Microsoft Certified Trainer und arbeitet als Consultant und Trainer. Sein Spezialgebiet ist die Security im Microsoft Windows Server Umfeld und die Implementation von Messagingsystemen mit Exchange 2000 / 2003. Weitere Informationen erhalten Sie auf seiner Webseite: http://www.it-training-grote.de.