ISA Server 2004 – ISA Server 2004 Zertifikatmanagement - Von Marc Grote

---

Die Informationen in diesem Artikel beziehen sich auf:
Microsoft ISA Server 2004

Dieser Artikel beschreibt die notwendigen Schritte für die Verwendung von Zertifikaten in Webserver- und Serververöffentlichungsregeln. Es wird hierbei auf die einzelnen Aspekte der Zertifikatbeantragung, Zertifikat-Export und -Import eingegangen, die Verwendung von Zertifikaten in Webserververöffentlichungen sowie einige Besonderheiten bei der Arbeit mit Zertifikaten gezeigt und etwas Grundlagenwissen vermittelt.
Dieser Artikel kann und will nicht alle Aspekte der sehr komplexen Materie der Kryptographie, PKI und des Zertifikatsmanagement ansprechen, sondern vielmehr exemplarisch an einigen Stellen auf häufige Stolperstellen bei der Arbeit mit Zertifikaten hinweisen.

Aus diesem Grund unterscheidet sich dieser Artikel etwas von der erfolgreichen Reihe der Step-by-Step Anleitungen auf www.msisafaq.de.

Dieser Artikel unterteilt sich in folgende Abschnitte:

- SSL-Zertifikatgrundlagen
- CA-Einrichtung
- Zertifikatbeantragung
- Zertifikat-Export und -Import
- Verwendung von Zertifikaten in Webserververöffentlichungen
- Fehlermeldung "500 Internal Server Error"
- Umgang des ISA Server mit Zertifikaten
- Wo können noch Zertifikate verwendet werden

SSL-Zertifikatgrundlagen

Der Hauptanwendungsbereich von SSL-Zertifikaten liegt in der sicheren Authentifizierung und Übertragung von Daten, sowie dem geschützten Zugriff auf Informationen.
Wenn Sie beispielsweise finanzielle Transaktionen auf Ihrer Website handhaben, benötigen Sie ein SSL-Zertifikat. Wenn Sie mit vertrauenswürdigen Kundendaten umgehen, sollten Sie den Einsatz eines SSL-Zertifikats durchaus in Betracht ziehen um der Sicherheit und dem Datenschutz Rechnung zu tragen.

Weitere Gründe die für den Einsatz eines digitalen Zertifikats sprechen:

- Um die Identität Ihrer Firma (oder Ihres Servers) online zu bestätigen und so für Vertrauen zu Ihren Mitarbeitern und externen Kunden zu sorgen.

- Um die an Ihre Website (oder zwischen Servern) übermittelten Daten mit Hilfe von SSL zu verschlüsseln.

Mit Hilfe der Authentisierung können sich die Benutzer davon überzeugen, dass das Unternehmen real existiert und der Verbindungsaufbau zum richtigen Server erfolgt. Zertifikate werden in verschiedene Klassen eingeteilt, so dass die Authentisierungsstufe eines Zertifikats als Qualitätsmerkmal dient - Je höher die angewendete Authentisierungsstufe, desto besser ist die Qualität des Zertifikats.

Einige Zertifizierungsstellen stellen vor der Ausstellung eines Zertifikats lediglich die

Grundüberprüfungen an (z. B. nur E-Mail Überprüfung bei Class1 Zertifikaten von z. B. Thawte Freemail), während vor Erwerb von anderen Zertifikaten ausführliche Prüfungen durchgeführt werden müssen (z. B. PostIdent-Verfahren, persönliche Anwesenheit bei der Zertifizierungsstelle erforderlich usw.)

Zertifikate haben nur eine begrenzte Gültigkeit, in der Regel in Jahren und müssen somit regelmäßig erneuert werden. Wenn ein Zertifikat (mit privatem Schlüssel) kompromittiert wird, abläuft oder aus diversen anderen Gründen nicht mehr verwendet werden darf, muss es einen Prozess geben, welcher dafür sorgt, dass dieses Zertifikat nicht mehr verwendet werden kann. Dieser Prozess heißt Zertifikatssperrung. In einer so genannten CRL (Certificate Revocation List) werden abgelaufene oder kompromittierte Zertifikate in regelmäßigen Abständen veröffentlicht. Clients, Server und diverse Verfahren laden die CRL und führen eine Überprüfung der Zertifikate gegen die CRL durch.

Standard Datei-Suffixe

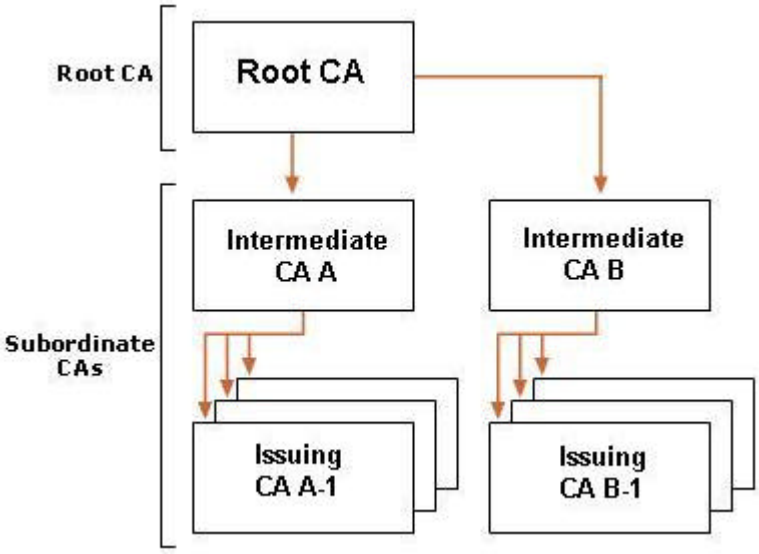
Schlüssel	Beschreibung
PCKS #12	Privater Informationsaustausch
.PFX	Privater Informationsaustausch
.P12	Privater Informationsaustausch
PCKS #7	Syntaxstandard kryptografischer Meldungen
.P7B	Syntaxstandard kryptografischer Meldungen
.SST	Microsoft serieller Zertifikatsspeicher
.CER	DER-kodiert-binär X.509 Base-64-codiert-X.509
.PFX	Privater Informationsaustausch PCKS #12
.CRL	Certification Revocation List
.P7C	Digitale ID-Datei
.P7M	PCKS #7 MIME-Nachricht
.P7R	PCKS #7 Zertifikat
.P7S	PCKS #7 Signatur

CA-Einrichtung

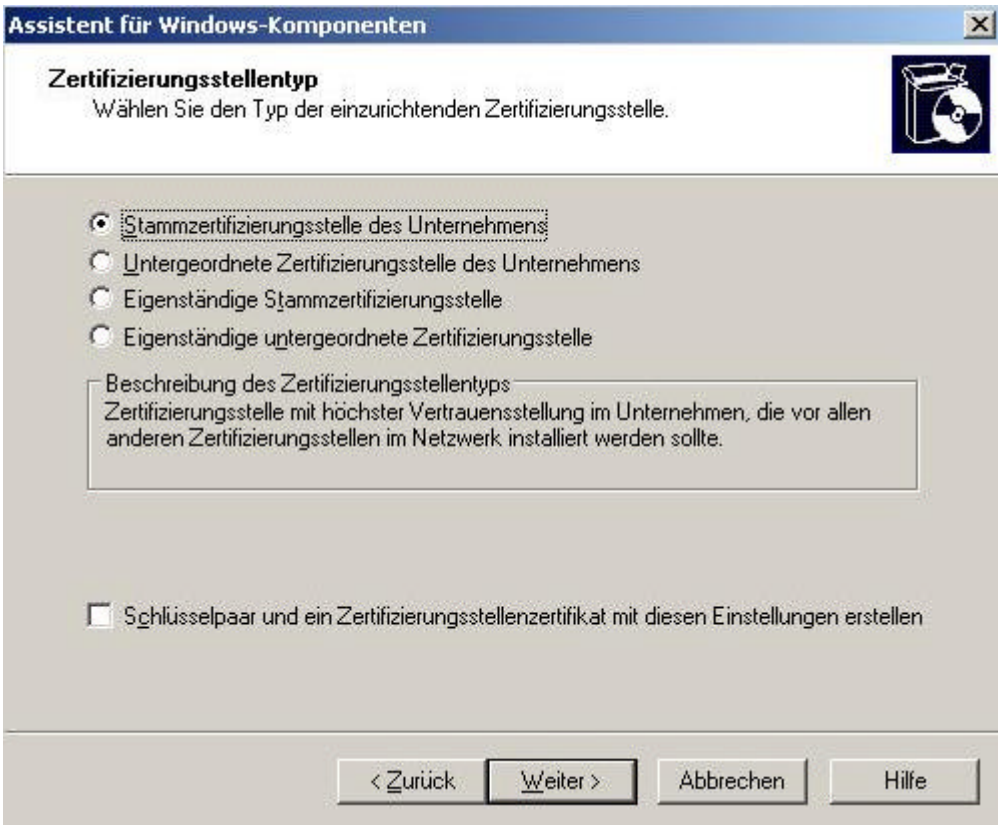
Microsoft bietet mit seiner Windows Server Familie die Möglichkeit zur Installation einer eigenen CA (Certificate Authority). Eine CA ist das Basisgerüst einer PKI (Public Key Infrastructure). Mit Hilfe einer CA können Sie Zertifikate ausstellen, aber noch wesentlich mehr. Lesen Sie hier mehr über die Windows 2003 PKI. Die Entscheidung, ob eine Inhouse PKI verwendet werden soll oder lieber kommerzielle Zertifikate für bestimmte Zwecke verwendet werden sollen, ist eine sehr wichtige Entscheidung, welche hier nicht näher erläutert werden kann. Generell gilt die Implementierung einer Inhouse PKI als sehr zeit- und kostenaufwändig.

Zertifizierungsstellen können kaskadiert werden um den Anforderungen in Punkto Sicherheit, Flexibilität und Skalierbarkeit Rechnung zu tragen. Man spricht dann von folgenden CAs:

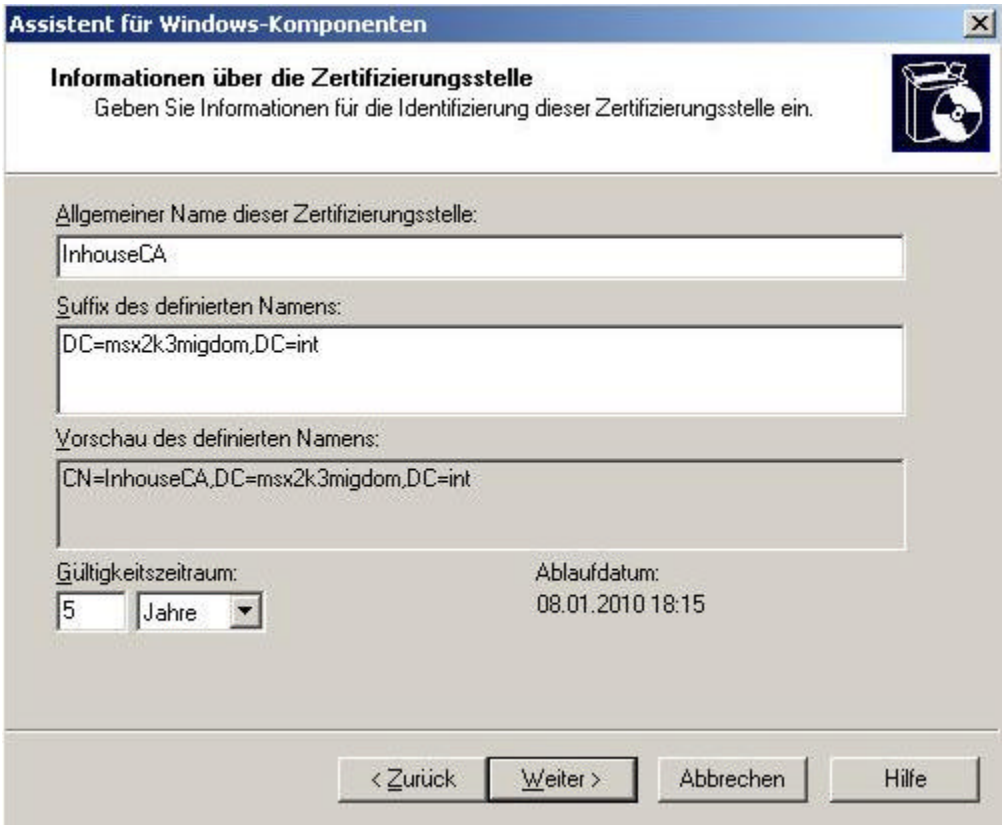
- RootCA
- IntermediateCA
- IssuingCA



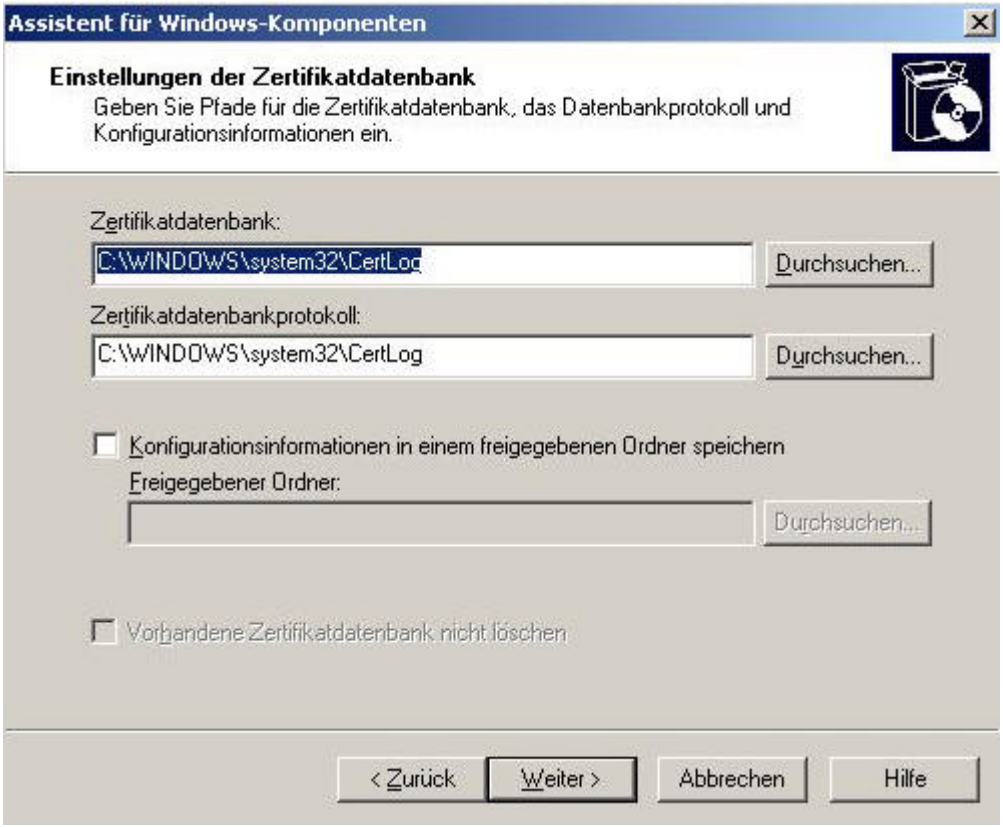
In diesem Artikel wird anhand von einigen Screenshots die oberflächliche Einrichtung einer CA gezeigt. Zur Installation einer CA klicken Sie auf **Start - Systemsteuerung - Software - Windows Komponenten Hinzufügen / Entfernen** und wählen in den Komponenten **Zertifikatdienste** aus. Für diesen Artikel wird eine **Stammzertifizierungsstelle des Unternehmens** installiert.



Vergeben Sie einen Namen für die Zertifizierungsstelle und den Gültigkeitszeitraum.

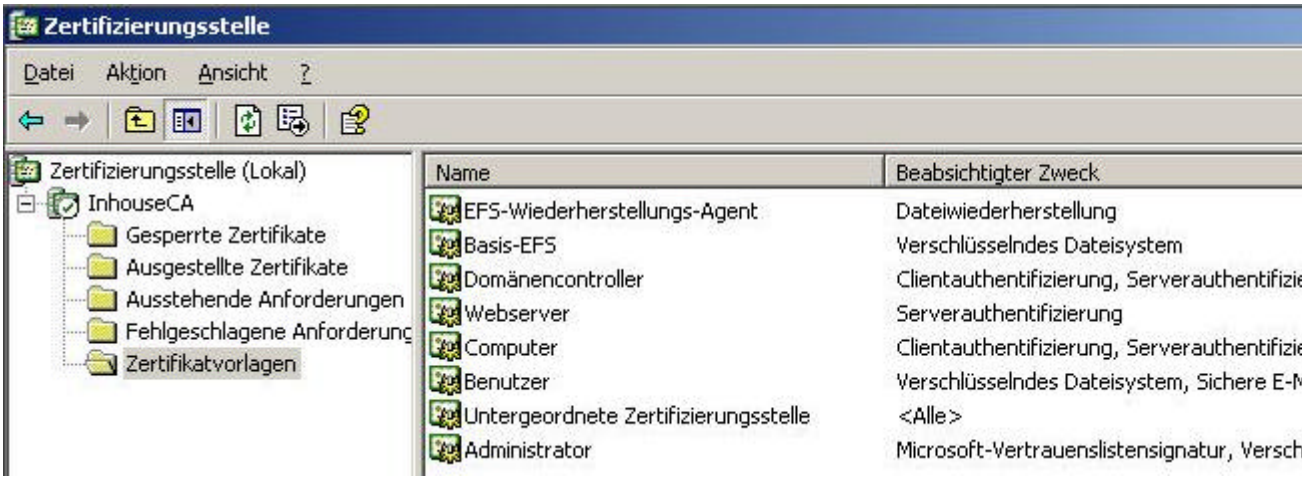


Bei der Frage nach dem Speicherort für die Zertifikatdatenbank und das Zertifikatdatenbankprotokoll wird in diesem Artikel keine Änderung vorgenommen. Bei einer Implementierung in Ihren Unternehmen, sollten Sie die Datenbank und die Protokolle auf unterschiedliche Datenträger legen.



Nach erfolgter Installation der Zertifizierungsstelle können Sie die CA mit Hilfe des

Zertifizierungsstellen SnapIns verwalten.



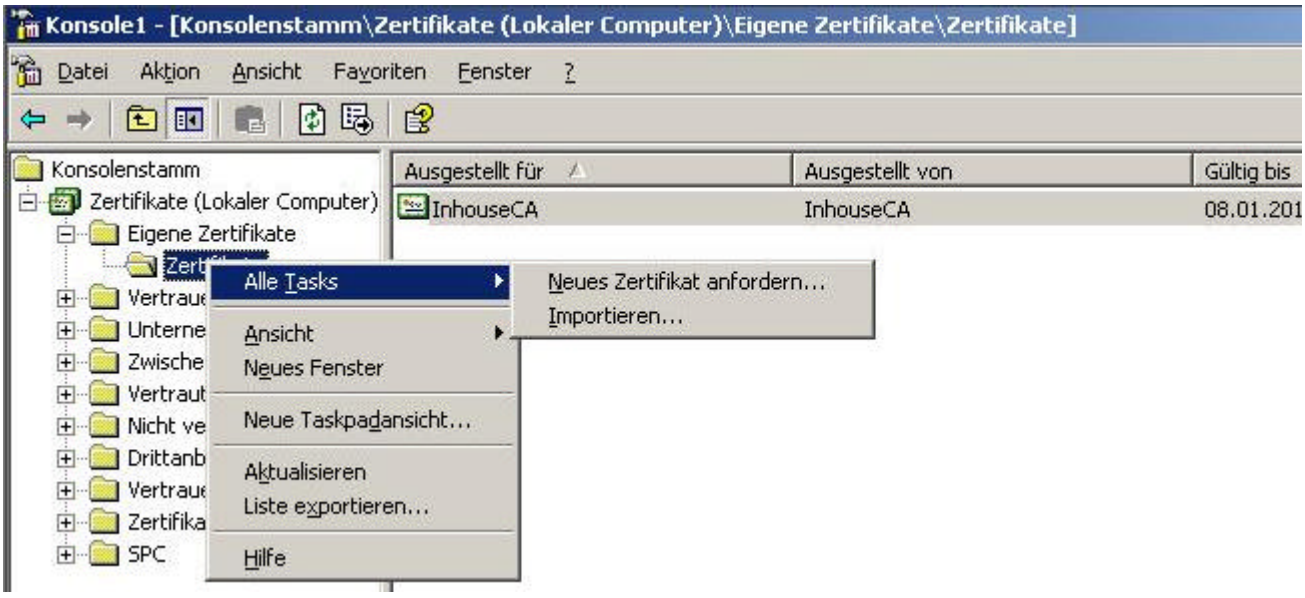
Zertifikatbeantragung

Je nach Verwendungsart, können Sie Zertifikate von einer Zertifizierungsstelle mit Hilfe einer Zertifikat Management Konsole beantragen oder etwas komfortabler, mit Hilfe einer Webseite.

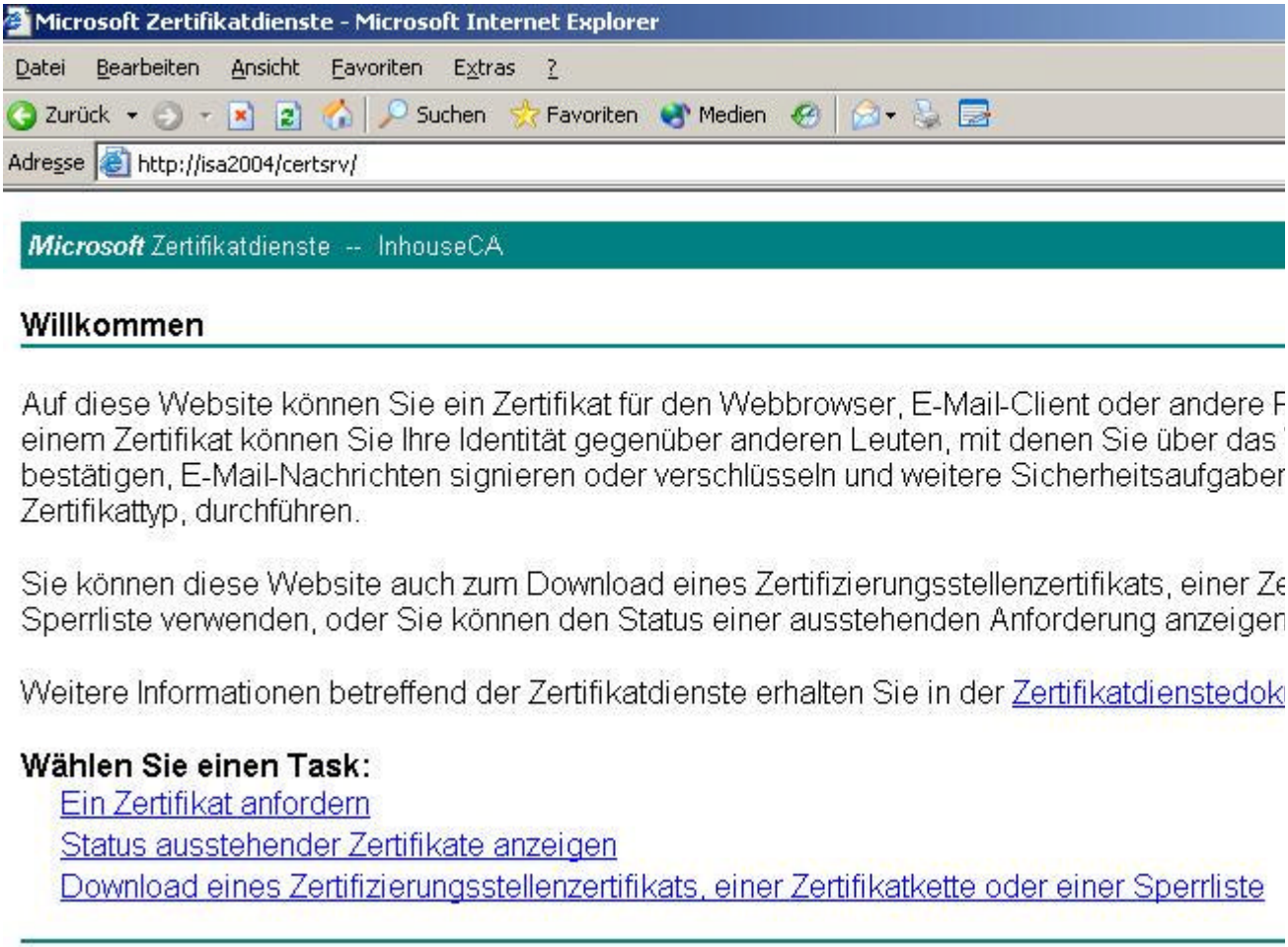
Um ein Zertifikat per MMC zu beantragen, müssen Sie eine neue Zertifikats-Management-Konsole erstellen. Klicken Sie dazu auf **Start - Ausführen - MMC**. Klicken Sie dann auf **Datei** - **Snap-In hinzufügen/entfernen** und wählen in der Liste der verfügbaren Snap-Ins **Zertifikate** aus.
Wenn Sie über administrative Berechtigungen verfügen, können Sie folgende Zertifikatsspeicher öffnen:

- Eigenes Benutzerkonto
- Dienstkonto
- Computerkonto

Ein normaler Benutzer kann nur das Zertifikats SnapIn für das eigene Benutzerkonto öffnen.



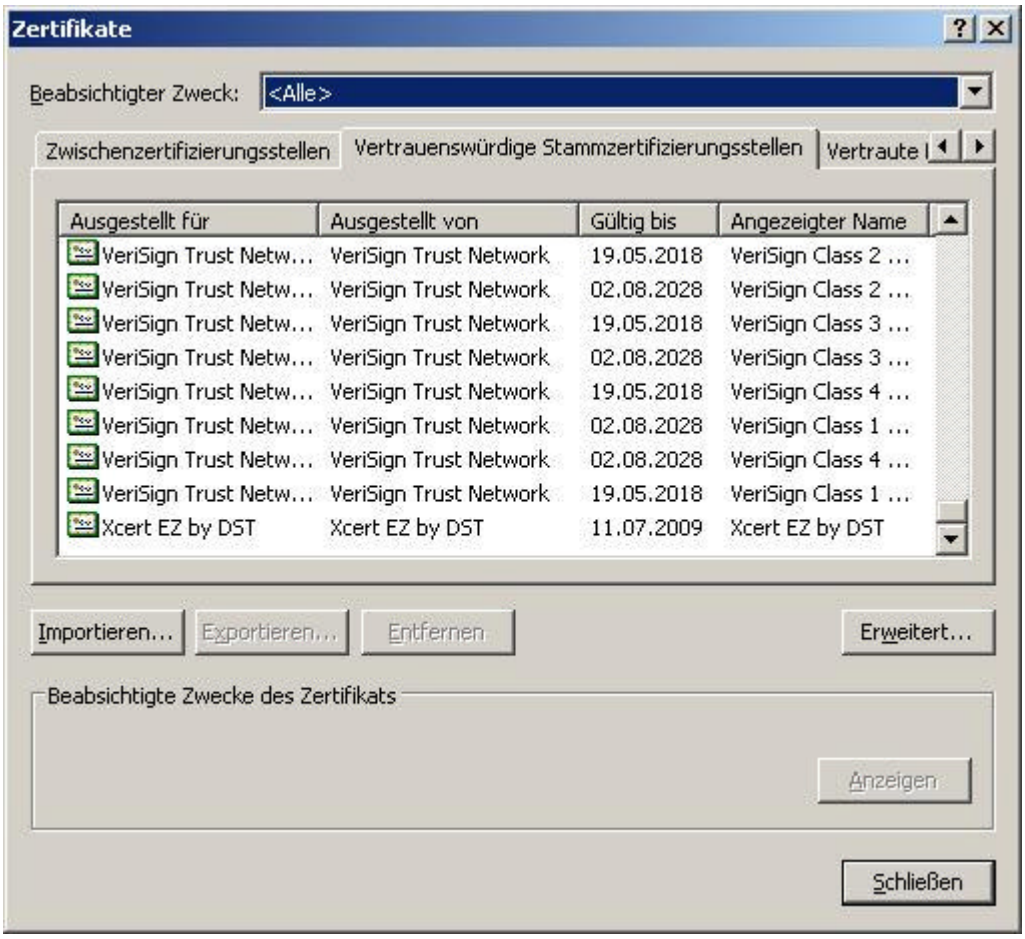
Wesentlich komfortabler ist die Anforderung von Zertifikaten über eine Webseite. Bei der Installation einer Windows 2000/2003 CA wird eine neue Webseite auf dem IIS installiert, mit deren Hilfe Benutzer komfortabel Zertifikate anfordern können. Der Aufruf der Webseite erfolgt durch Eingabe von HTTP://CASERVERNAME/CERTSRV.



Hinweis:

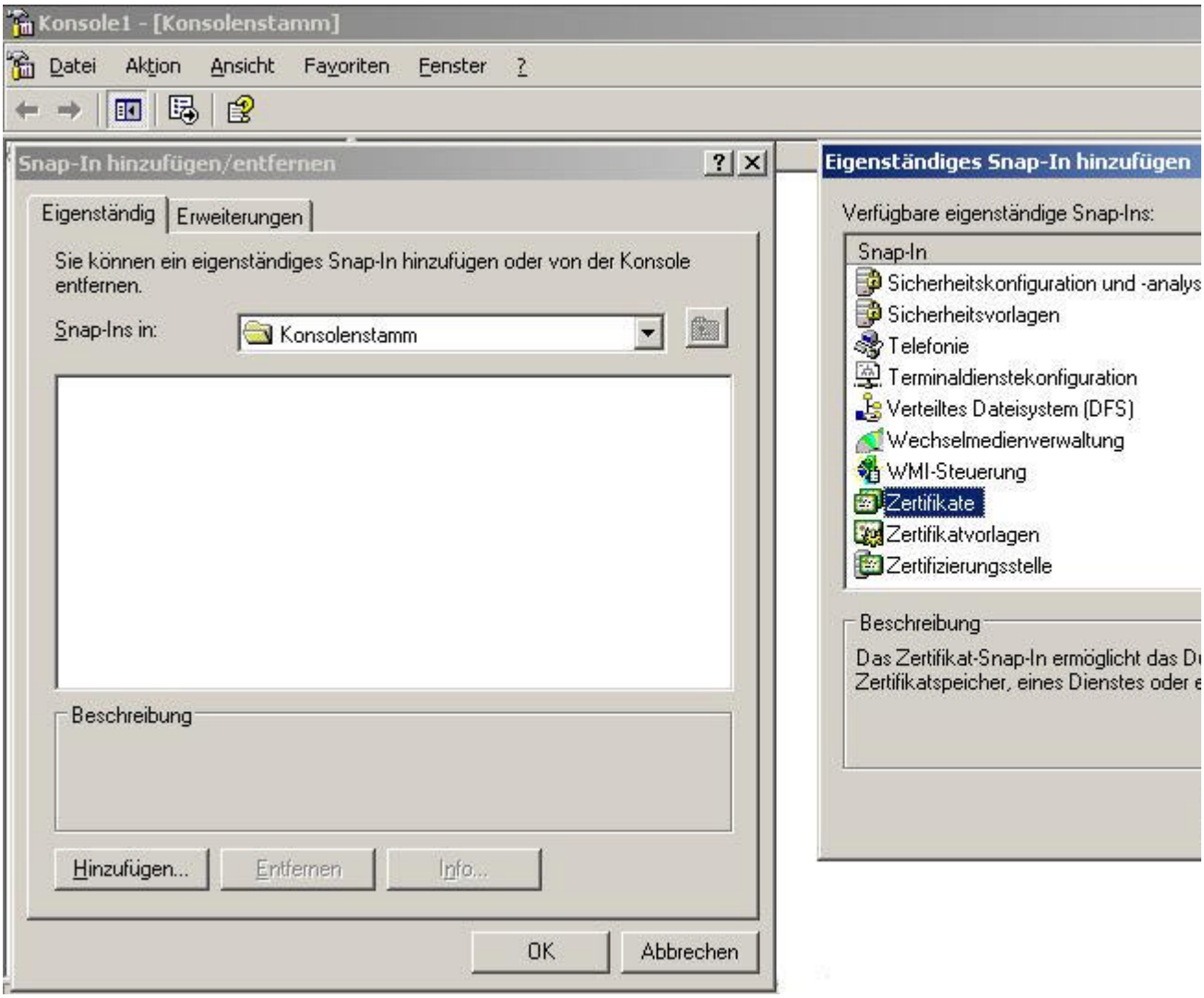
Es ist wichtig, dass sämtliche Computer, welche an einer sicheren Webserververöffentlichung beteiligt sind, Zugriff auf das Zertifizierungsstellenzertifikat der privaten CA haben. Bei der Verwendung einer Stammzertifizierungsstelle des Unternehmens und einer Mitgliedschaft aller Clients und Server in der Active Directory Domäne, wird das Stammzertifizierungsstellenzertifikat automatisch installiert. Bei Clients, welche nicht Mitglied der Domäne sind, müssen Sie das Zertifizierungsstellenzertifikat in den Zertifikatsspeicher der Vertrauenswürdigen Stammzertifizierungsstellen importieren.

Beispiel einer Ansicht auf **Vertrauenswürdige Stammzertifizierungsstellen** im Internet Explorer eines Windows XP Clients.

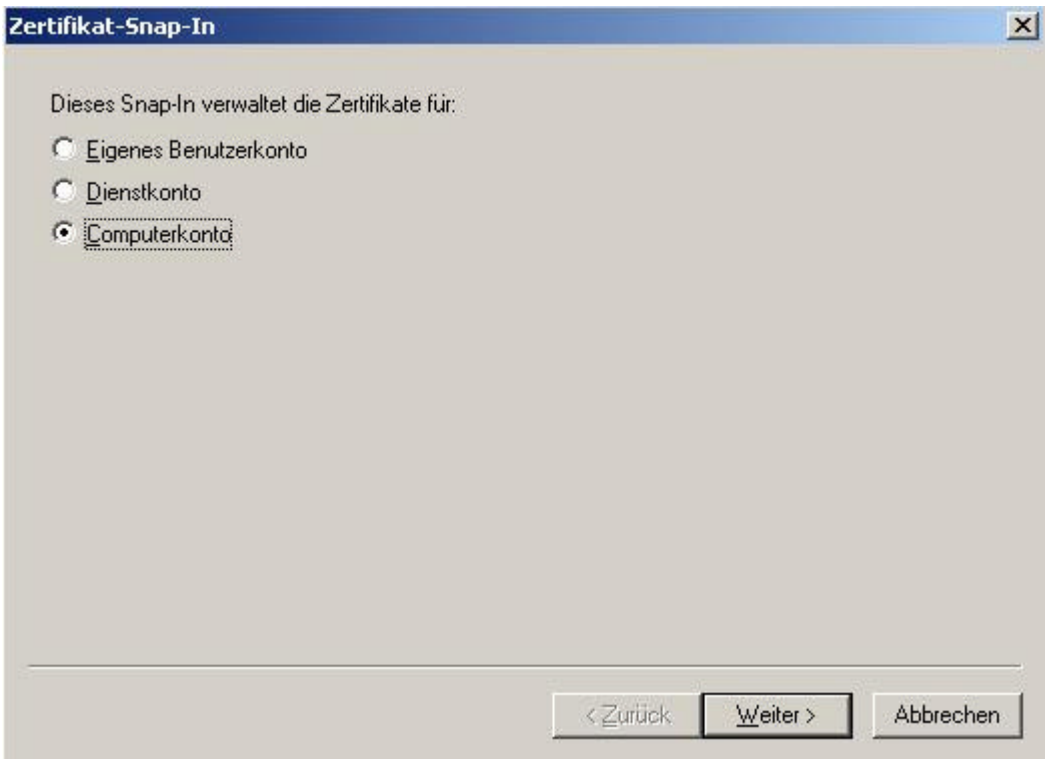


Zertifikats-Export und -Import

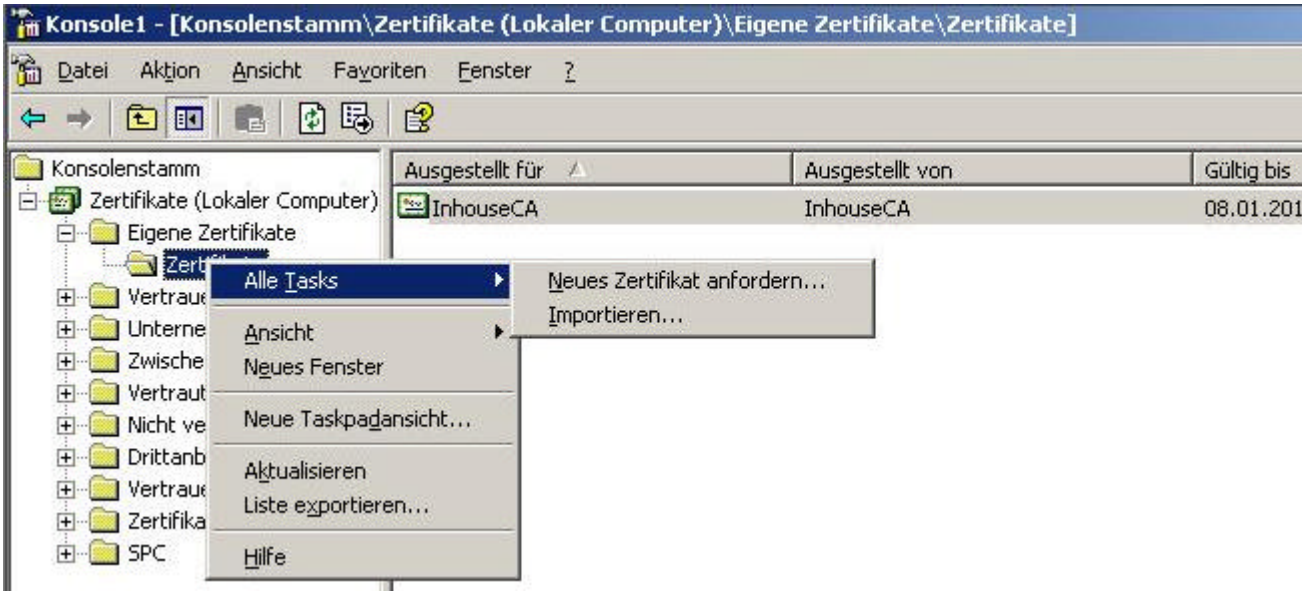
Sie können bereits im Zertifikatsspeicher vorhandene Zertifikate exportieren und importieren. Sie müssen dazu eine neue Zertifikats-Management-Konsole erstellen. Klicken Sie dazu auf **Start - Ausführen - MMC**. Klicken Sie dann auf **Datei** - **Snap-In hinzufügen/entfernen** und wählen in der Liste der verfügbaren Snap-Ins **Zertifikate** aus.



Sie können ein Zertifikat-Snap-In für folgende Objekte verwalten:



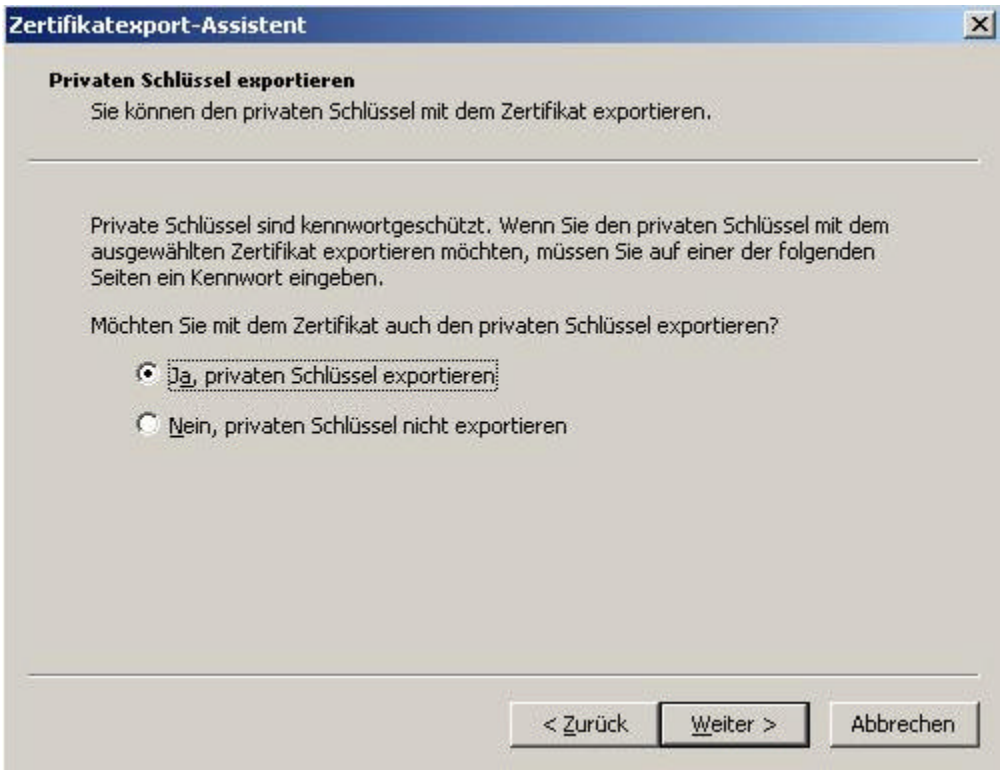
Nachdem Sie die Zertifikatskonsole erstellt haben, können sie ein **Neues Zertifikat anfordern** wenn sich Ihr Client in einer Windows 2000/2003 Domäne befindet und eine Zertifizierungsstelle installiert ist, sonst müssen Sie auf **Importieren** klicken um ein bereits ins Dateisystem exportiertes Zertifikat zu importieren.



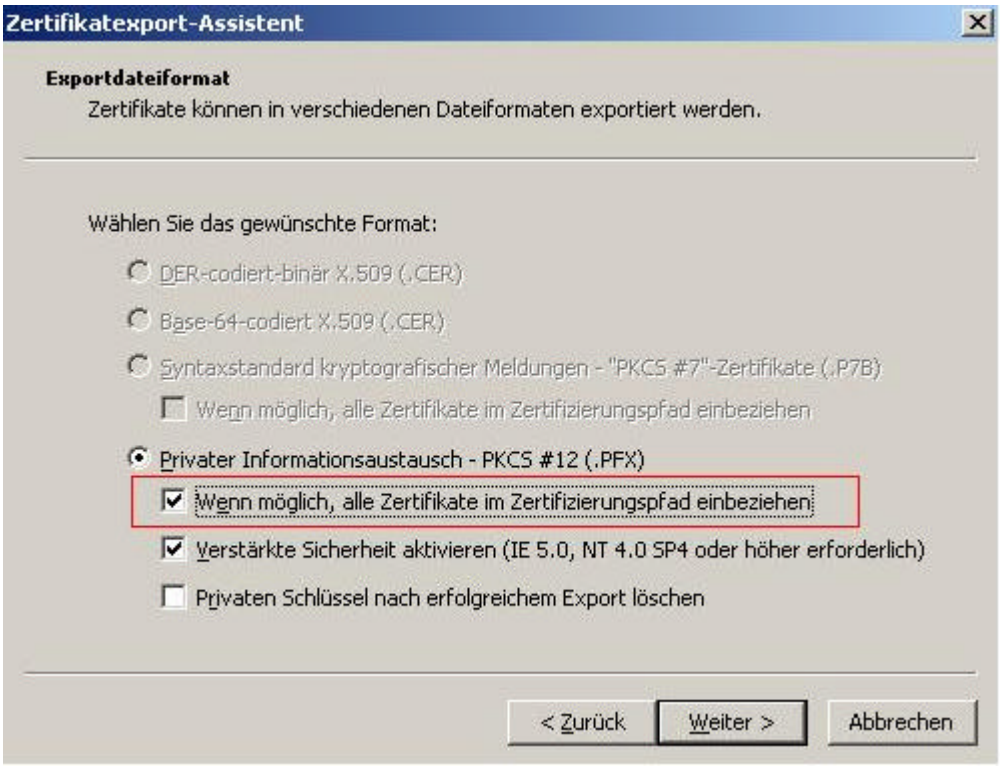
Durch einen Doppelklick auf das gewünschte Zertifikat gelangen Sie in dessen Eigenschaften. Sie können im Reiter Allgemein u. a. überprüfen, von welcher CA das Zertifikat ausgestellt wurde, wie lang das Zertifikat noch gültig ist und ob Sie einen privaten Schlüssel für dieses Zertifikat besitzen. Dieser Punkt ist sehr wichtig für die Verwendung von Zertifikaten in Webserververöffentlichungen.

Im Reiter Details erhalten Sie weitere Informationen über das ausgestellte Zertifikat.

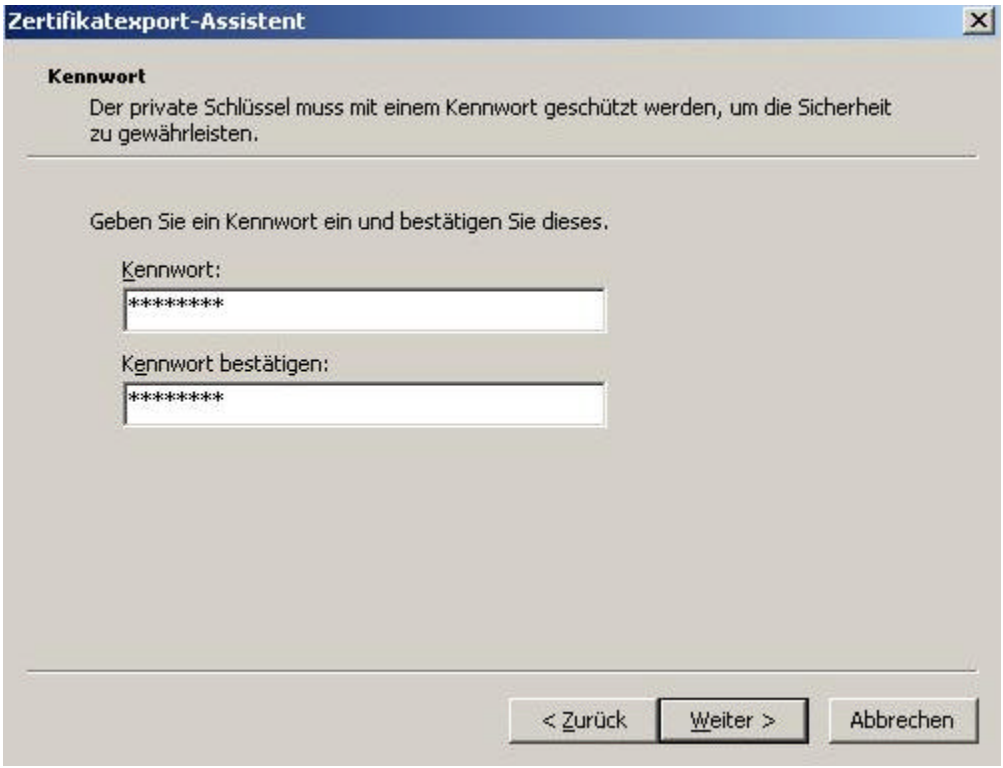
Ein in einem Zertifikatsspeicher enthaltenes Zertifikat kann mit Hilfe des **Zertifikatexport-Assistenten** in eine Datei exportiert werden. In unserem Beispiel der Webserververöffentlichung müssen Sie das Zertifikat mit dem privaten Schlüssel exportieren, da der ISA Server nur so verschlüsselte SSL Verbindungen entschlüsseln kann. Für diesen Artikel müssen Sie das IIS Webserverzertifikat des IIS exportieren, welcher für die sichere Webveröffentlichung verwendet werden soll.



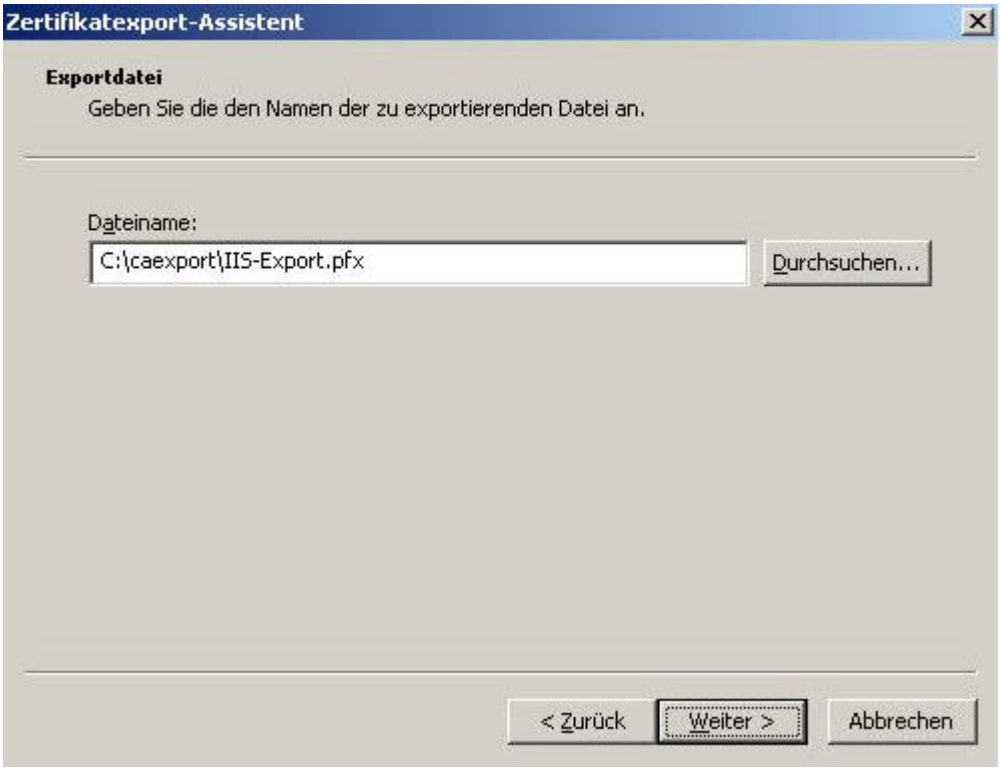
im Fenster **Exportdateiformat** setzen Sie den Haken bei **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen**. Damit werden alle Zertifikate in einem möglichen Certificate Chain eingeschlossen.



Wenn Sie ein Zertifikat mit einem privaten Schlüssel exportieren, sollten Sie den privaten Schlüssel mit einem Kennwort schützen.

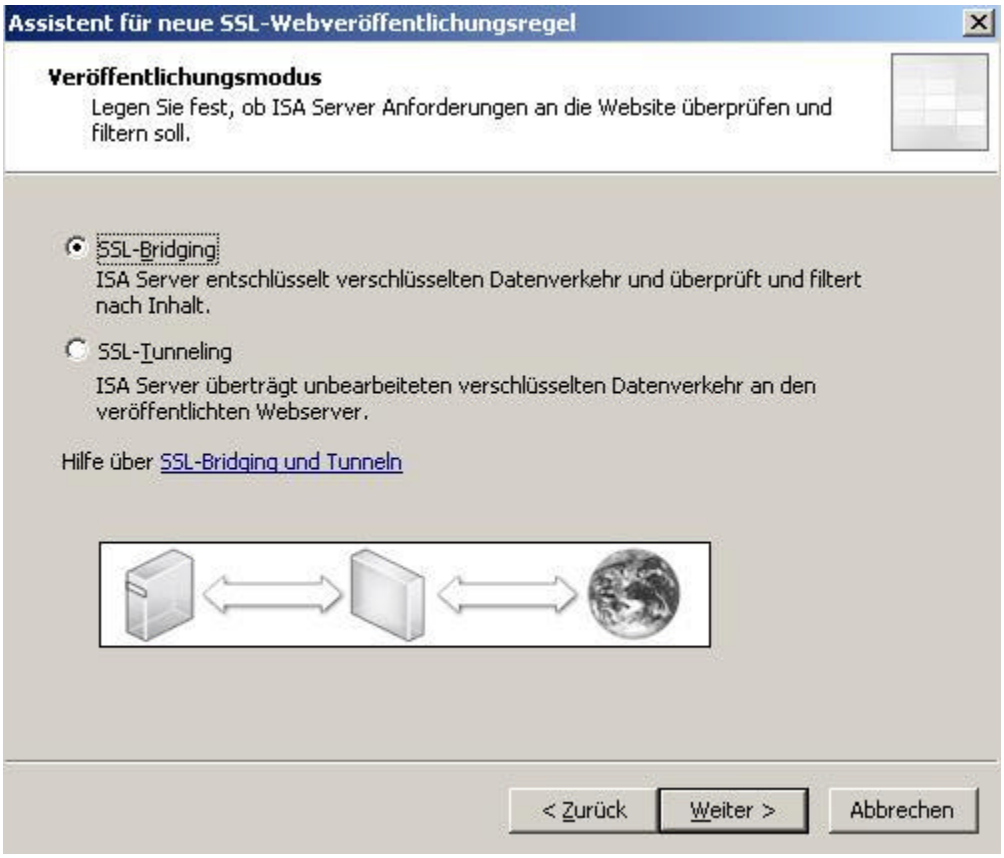


Geben Sie noch den Pfad zur Speicherung der Exportdatei an. Damit ist der Export des Zertifikats erfolgreich abgeschlossen.

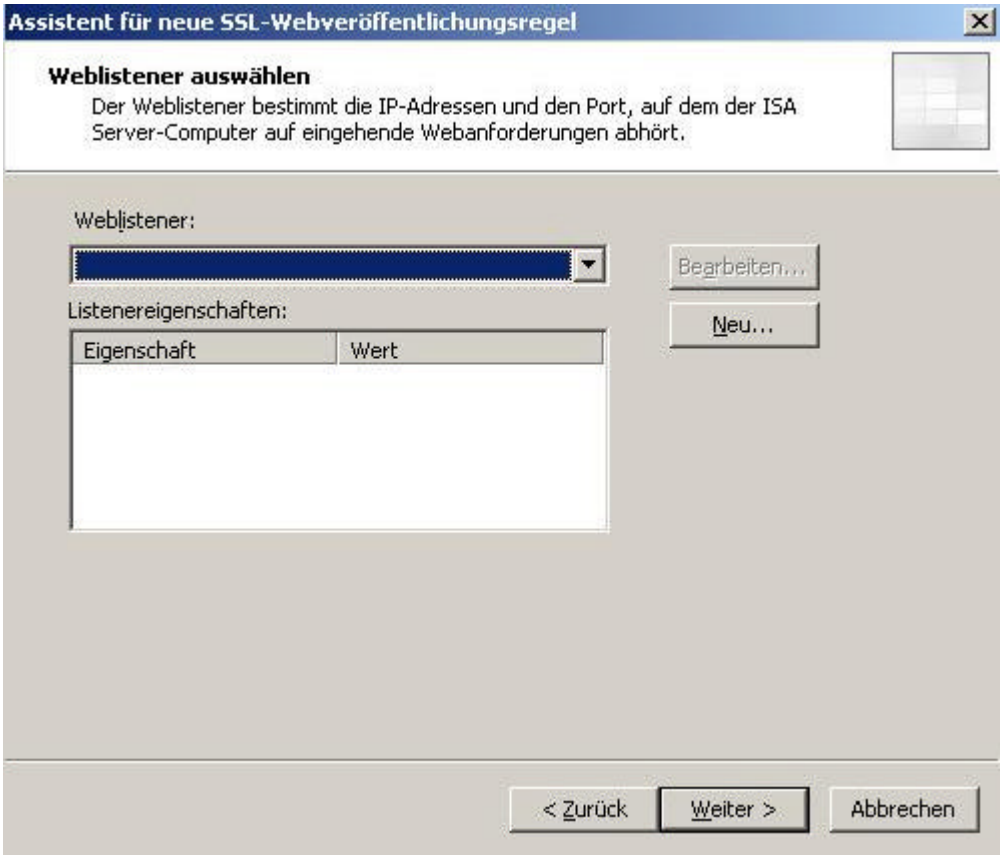


Verwenden von Zertifikaten in Webserververöffentlichungen

Bei der Verwendung einer Webserververöffentlichung können Sie zwischen **SSL-Bridging** und **SSL-Tunneling** auswählen. Für das Beispiel in diesem Artikel wählen Sie SSL-Bridging.



Der Wizard besteht aus weiteren Schritten, auf deren Erläuterung in diesem Artikel, wie bereits am Anfang erwähnt, jedoch verzichtet wurde. Der folgende Screenshot zeigt die Konfiguration des Weblistener für die SSL-Webveröffentlichungsregel.

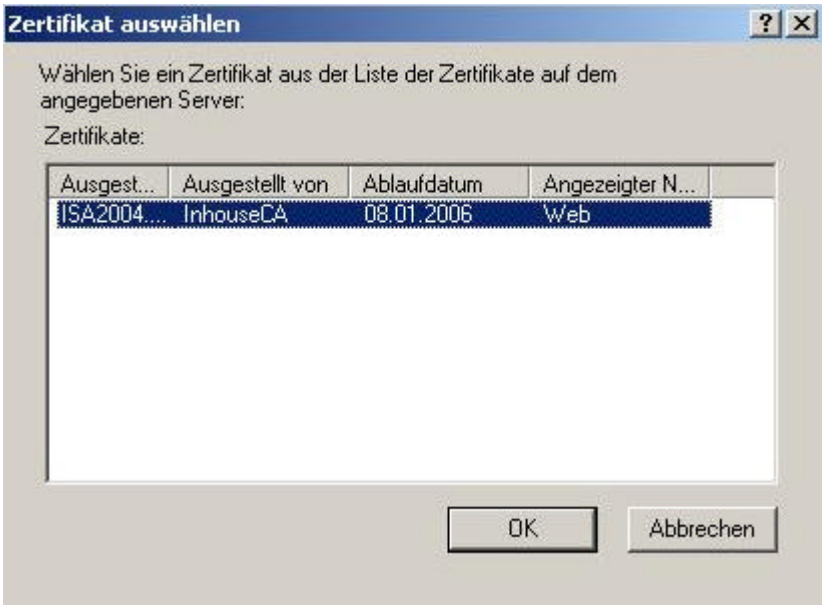


Wählen Sie bei der Portspezifizierung **SSL aktivieren** aus. Dazu müssen Sie jetzt auf

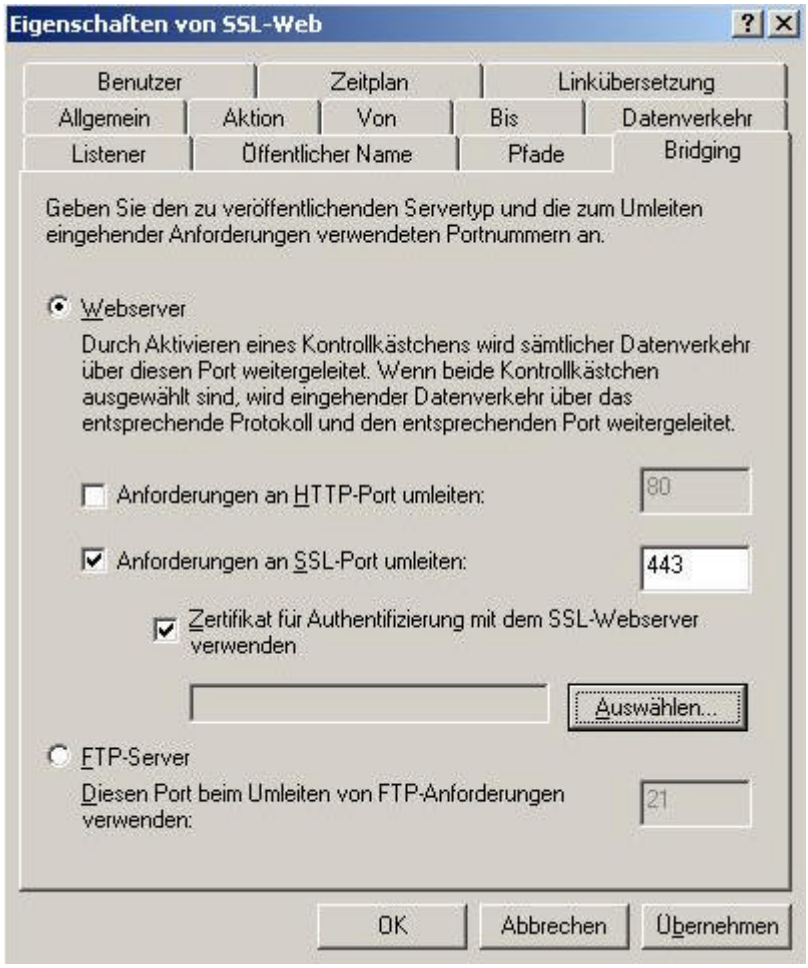
Auswählen klicken um das SSL-Zertifikat auszuwählen, welches für das SSL-Bridging verwendet werden soll.

In diesem Beispiel ist kein entsprechendes Zertifikat mit einem privaten Schlüssel im Zertifikatsspeicher des lokalen Computerkontos vorhanden, so dass folgende Fehlermeldung erscheint:

Nachdem Sie, wie weiter oben beschrieben, das entsprechende Zertifikat angefordert oder importiert haben, erhalten Sie beim klicken auf die Schaltfläche **Auswählen** folgendes Auswahlfenster:



Für das SSL-Bridging müssen Sie im Reiter **Bridging** den Haken bei **Zertifikat für Authentifizierung mit dem SSL-Webserver verwenden** aktivieren. Klicken Sie dann auf **Auswählen**.



In diesem Beispiel ist wieder kein entsprechendes Zertifikat mit einem privaten Schlüssel im Zertifikatsspeicher vorhanden, so dass folgende Fehlermeldung erscheint:

Warum erscheint schon wieder diese Meldung, obwohl wir schon ein entsprechendes Zertifikat in den Zertifikatsspeicher des lokalen Computers auf dem ISA importiert haben? Hintergrund ist, dass hier ein **Benutzerzertifikat** für den **Firewall-Dienst** angefordert werden muss.

Das Vorgehen ist etwas trickreich:

Fordern Sie am ISA Server per Internet Explorer ein **Benutzerzertifikat** bei der privaten Zertifizierungsstelle an.
Danach starten Sie den Internet Explorer und navigieren zu **EXTRAS - INTERNETOPTIONEN - INHALTE - ZERTIFIKATE** - wählen dort das so eben erstellte Zertifikat aus und exportieren dieses.
Stellen Sie beim Export sicher, dass Sie den privaten Schlüssel exportieren, und **wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen**.
Öffnen Sie dann auf dem ISA Server eine MMC (Start - Ausführen - MMC), fügen das Zertifikats-SnapIn hinzu und wählen dort den Dienst Microsoft Firewall Dienst aus
Sie können jetzt das im Internet Explorer exportierte Zertifikat importieren. Stellen Sie beim Import sicher, dass Sie den privaten Schlüssel exportieren, und **wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen**.
Danach ist das Zertifikat in Reiter **Bridging** der Webserververöffentlichungsregel auswählbar.

Fehlermeldung "500 Internal Server Error"

Eine sehr häufige Fehlermeldung, gerade bei der Veröffentlichung von Outlook WebAccess oder RPC over HTTPS ist die Fehlermeldung "500 Internal Server Error - The target principal name is incorrect. Was bedeutet diese Fehlermeldung?

Diese Fehlermeldung kann immer dann auftreten, wenn Sie bei einer Webserververöffentlichung SSL Briging verwenden. Bei SSL Tunneling tritt das Problem nicht auf!

Wo ist der Unterschied?

Beim SSL Tunneling existiert eine SSL Verbindung von Client zu Server durch den ISA Server. ISA Server leitet hier nur SSL Anfragen weiter, ohne den Inhalt der Daten lesen zu können.
Beim SSL Bridging wird ein SSL-Objekt von einem Client angefordert. Die Anforderung wird von ISA Server entschlüsselt, anschließend erneut verschlüsselt und an den Webserver weitergeleitet. Vom Webserver wird das verschlüsselte Objekt an ISA Server zurückgesendet. Das Objekt wird von ISA Server entschlüsselt, erneut verschlüsselt und an den Client gesendet. Mit anderen Worten: SSL-Anforderungen werden als SSL-Anforderungen weitergeleitet.

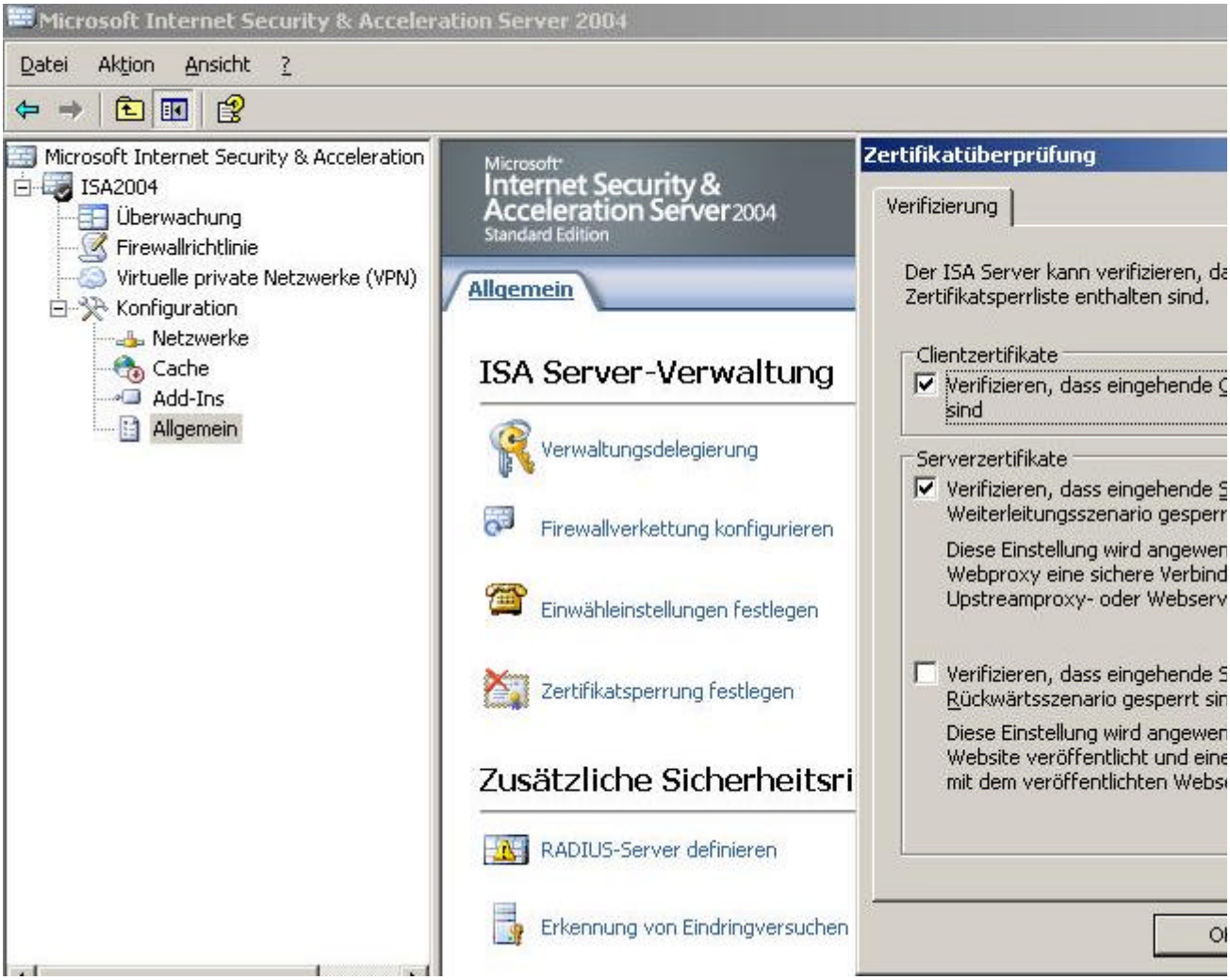
Die Fehlermeldung "500 Internal Server Error" tritt auf, wenn es keine Übereinstimmung zwischen dem FQDN der Anfrage und dem CN des Website Zertifikats gibt. Die Lösung für dieses Problem ist die Konfiguration der Webveröffentlichungsregel zur Verwendung des

FQDN der internen Webseite und der Verwendung einer Split DNS Konfiguration oder einer HOSTS Datei. Für einfachere Installationen oder etwas unbedarftere Administratoren ist die Konfiguration einer HOSTS Datei pragmatischer. Der ISA Server kann dann den Namen zu der internen IP-Adresse auflösen und nicht auf die öffentliche IP-Adresse des Server. Die HOSTS Datei enthält dann die IP-Adresse des internen Webservers und den öffentlichen Namen.

Für mehr Informationen über diese Fehlermeldung lesen Sie folgenden Artikel.

Umgang des ISA Server mit Zertifikaten

Sie können in der ISA Server 2004 Management Konsole unterhalb von **Konfiguration** - **Allgemein** - Eigenschaften für die **Zertifikatsperrung festlegen.**
Mit Hilfe dieser Funktion kann der ISA Server verifizieren, dass eingehende Zertifikate nicht in einer Zertifikatsperrliste (CRL) enthalten sind.



Wo können noch Zertifikate verwendet werden

- Standort zu Standort Verbindungen mit L2TP/IPSEC
- Standort zu Standort Verbindungen mit IPSEC
- EAP / Smartcard Authentifizierung

- SSL-Zertifikatsauthentifizierung in einem Weblistener

Für mehr Informationen über digitale Zertifikate lesen Sie folgenden Artikel.

Stand: Sonntag, 09. Januar 2005/MG. http://www.it-training-grote.de