UniWeb | Installationsanleitung

16.02.2018

Inhalt

Installationsvoraussetzungen

Das UniWeb-Portal ist eine Online-Plattform auf Basis der Microsoft Silverlight-Technologie. Die komplette Umgebung wird als Webseite auf einem Microsoft IIS-Webserver bereitgestellt. Mindestvoraussetzung für die Installation ist der IIS 6.0, der mit Windows Server 2003 ausgeliefert wurde. Empfohlen wird die Verwendung von IIS 7.0 oder höher. Für die Installation von UniWeb wird außerdem das Microsoft .NET-Framework 4.6 vorausgesetzt.

Installationsablauf

1. Webserver (IIS) installieren.

Zuerst müssen, sofern noch nicht geschehen, die Webserver-Komponenten (IIS) installiert werden. Dazu öffnen Sie in der Systemsteuerung den Eintrag *Programme und Funktionen*. Hier wählen Sie auf der linken Seite den Menüpunkt *Windows-Funktionen aktivieren oder deaktivieren*. Auf einem Windows Client-Betriebssystem aktivieren Sie die Funktion *Internetinformationsdienste* in der Standard-Konfiguration. Auf einem Windows Server-Betriebssystem installieren Sie im Server-Manager die Rolle *Webserver (IIS)* in der Standard-Konfiguration.

2. ASP.NET 4.0 für den IIS registrieren

Die Installation der Webseite setzt das Microsoft .NET-Framework 4.6 voraus. Wenn der IIS nach dem .NET-Framework installiert wurde, dann muss ASP.NET 4.0 für den IIS extra registriert werden. Ansonsten wird beim Aufruf einer ASP.NET-Webseite folgende Fehlermeldung angezeigt:

HTTP-Fehler 500.19 - Internal Server Error
Auf die angeforderte Seite kann nicht zugegriffen werden, da die zugehörigen Konfigurationsdaten für die Seite ungültig sind.

Fehlercode: 0x80070021

Zur Registrierung muss einfach folgendes Kommando ausgeführt werden:

```
C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis -i
```

Dadurch wird ASP.NET 4 im IIS registriert. Vorhandene Anwendungen werden auf die ASP.NET 4-Version des Anwendungspools aktualisiert. Der Befehl aktualisiert sowohl den Handler für den klassischen als auch für den integrierten IIS-Modus und die Skriptzuordnungen in der IIS-Metabasis.

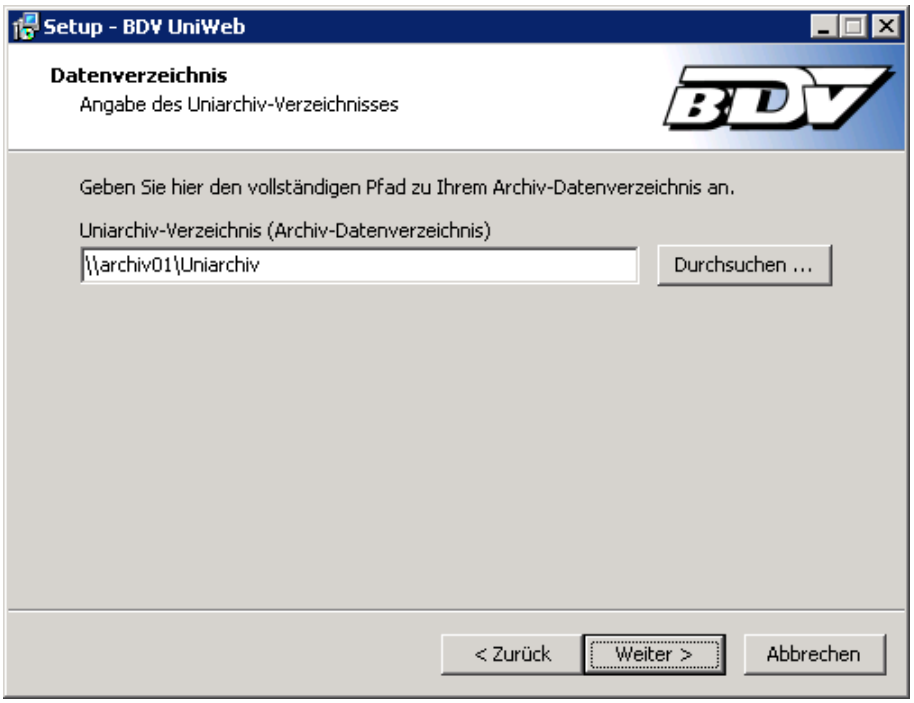
Mit dieser Option werden die beiden neuen Anwendungspools ASP.NET v4.0 und ASP.NET v4.0 Classic erstellt. Der Anwendungspool DefaultAppPool und die Classic .NETAppPool-Anwendungspools werden auf die .NET Framework 4-Version der CLR festgelegt.

3. Installation des Website-Contents

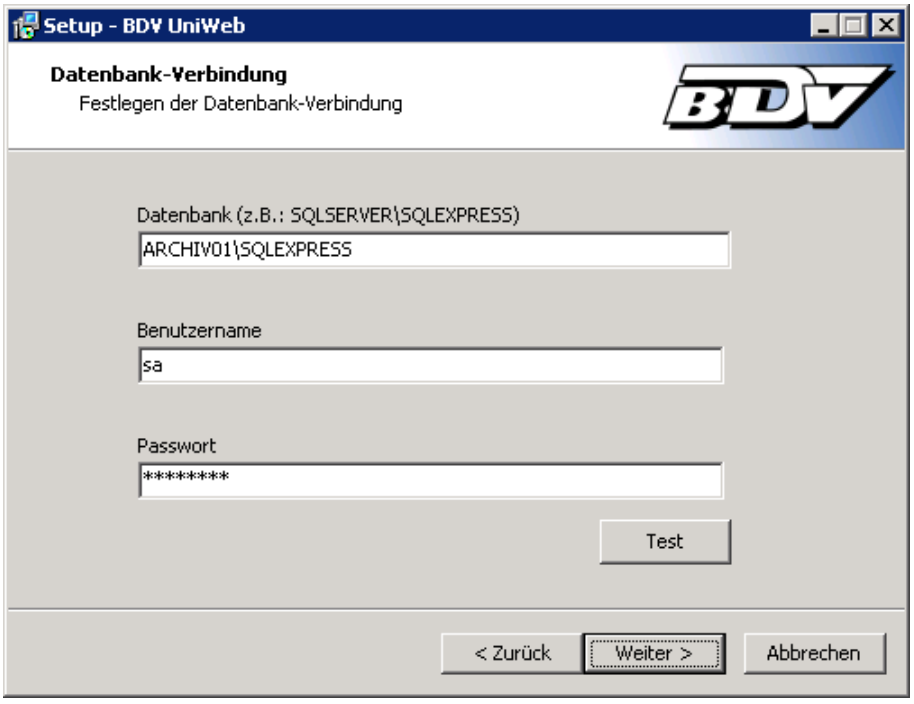
Für die Installation des Website-Contents rufen Sie das UniWeb-Setup auf.

Klicken Sie im Begrüßungs-Dialog auf <*Weiter*>, um den Installationsprozess zu beginnen.

An dieser Stelle muss der physikalische Pfad der Webseite angegeben werden. Klicken Sie anschließend auf <*Weiter*>, um die Installation fortzusetzen.



An dieser Stelle müssen Sie die Datenfreigabe Ihrer vorhandenen Uniarchiv/SBA-Installation auswählen. Klicken Sie anschließend auf <*Weiter*>.



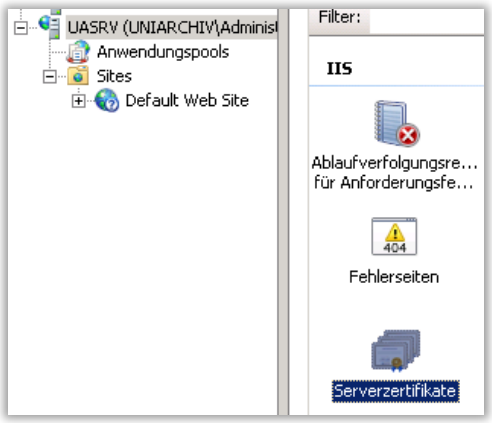
Wählen Sie hier die Datenbank-Instanz Ihrer vorhandenen Uniarchiv/SBA-Installation und die entsprechenden Anmeldeinformationen aus und drücken Sie anschließend auf <*Test*>. Nach einem erfolgreichen Verbindungstest können Sie im Installationsdialog auf <*Weiter*> klicken.

Wählen Sie hier die von Ihnen verwendete Finanzbuchhaltungs-Software aus. Ist Ihre Software nicht in der Liste vorhanden, dann wählen Sie *DATEV oder kompatibel*.

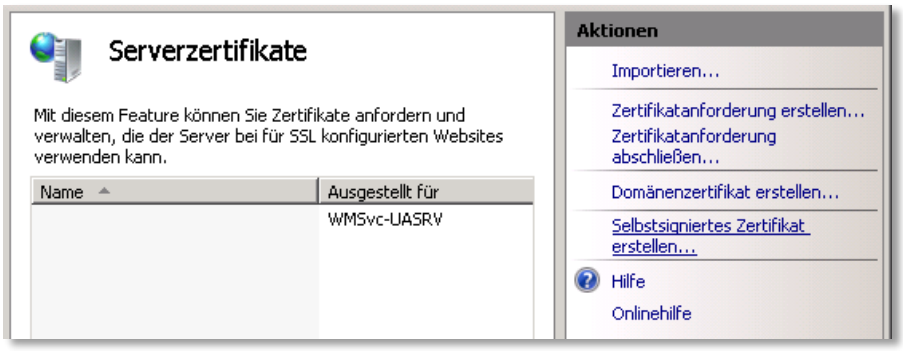
Vor dem eigentlichen Installationsprozess wird noch einmal eine Zusammenfassung der gewählten Einstellungen angezeigt. Klicken Sie auf <*Installieren*> um die eigentliche Installation zu starten.

4. Einrichten des Serverzertifikats für https im IIS

Die Webseite wird über https auf dem IIS bereitgestellt. Für das Bereitstellen einer https-Webseite wird ein Serverzertifikat benötigt. Öffnen Sie dazu im IIS-Manager den Bereich *Serverzertifikate*.



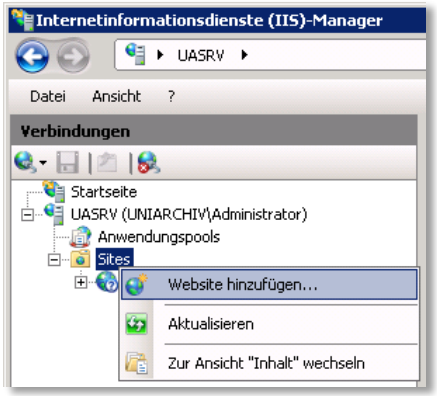
Es kann ein vertrauenswürdiges Zertifikat importiert oder ein selbstsigniertes Zertifikat erstellt werden.



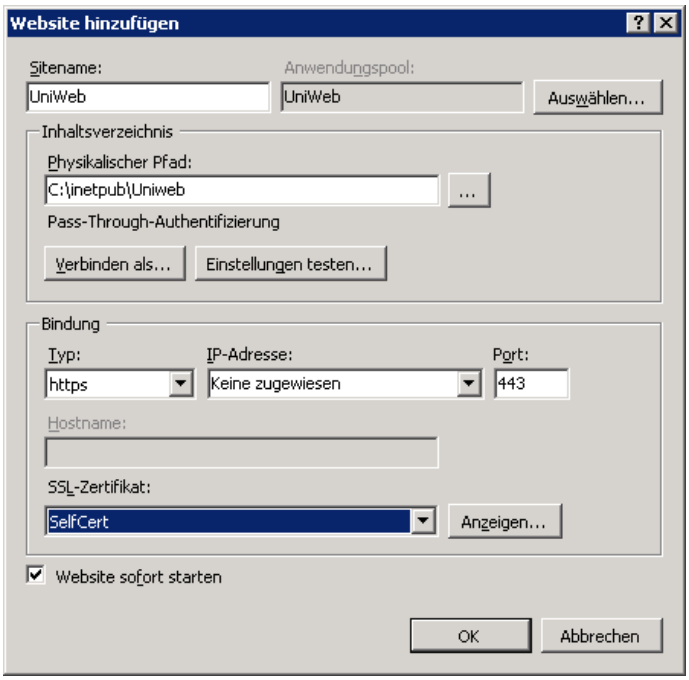
Bei einem selbstsignierten Zertifikat ist zu beachten, dass im Webbrowser eine Zertifikatswarnung ausgegeben wird, dass das verwendete Zertifikat nicht vertrauenswürdig ist.

5. Einrichtung der Webseite auf dem IIS

Zum Anlegen einer neuen Webseite im IIS-Manager klicken Sie mit der rechten Maustaste auf den Knoten *Sites* und wählen den Menüpunkt *Website hinzufügen...* aus.

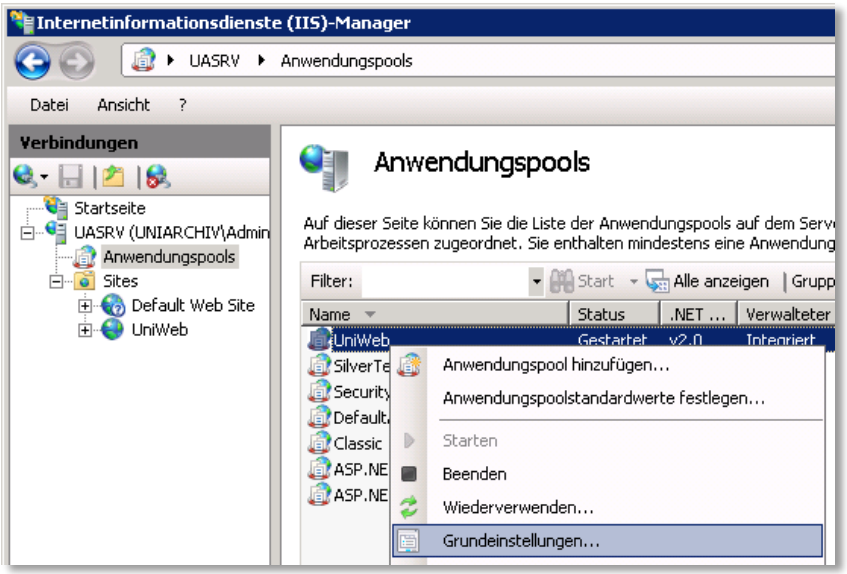


Für die neue Webseite muss der Sitename, der physikalische Pfad und die Bindung konfiguriert werden. Als Bindung wählen Sie den Typ https aus. Außerdem muss noch das zuvor generierte oder importierte SSL-Zertifikat ausgewählt werden.



6. Anwendungspool auf .NET 4 umstellen

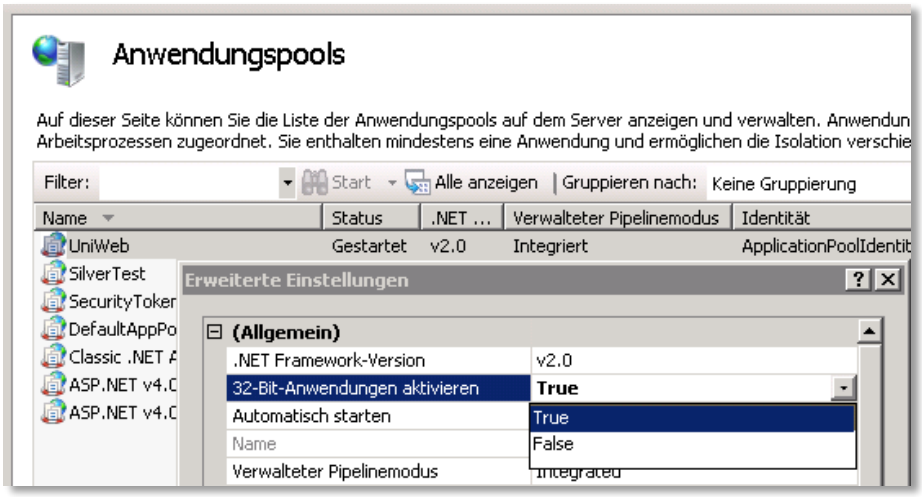
Im Internetinformationsdienste-Manager muss der Anwendungspool der ausgewählten Webseite noch auf .NET 4 umgestellt werden.



In den Grundeinstellungen des Anwendungspools muss dazu die .NET-Framework-Version auf v4.0.30319 oder höher eingestellt werden.

7. 32-Bit Anwendungen aktivieren

Im IIS-Manager müssen auf einem 64-Bit Betriebssystem 32-Bit Anwendungen für den verwendeten Anwendungspool explizit aktiviert werden. Diese Eigenschaft kann in den erweiterten Einstellungen des Anwendungspools umgestellt werden.



8. Dienstkonto des Anwendungspools umstellen

Im IIS-Manager muss das Dienstkonto des verwendeten Anwendungspools auf ein Windows-Benutzerkonto umgestellt werden, welches über Zugriffsrechte auf das Uniarchiv/SBA-Datenverzeichnis verfügt. Für das verwendete Dienstkonto muss zudem sichergestellt sein, dass deutsche Ländereinstellungen verwendet werden. Insbesondere muss als Dezimaltrennzeichen das Komma (,) eingestellt sein. Diese Zuordnung eines Dienstkontos wird über die Eigenschaft *Identität* in den erweiterten Einstellungen des Anwendungspools vorgenommen.

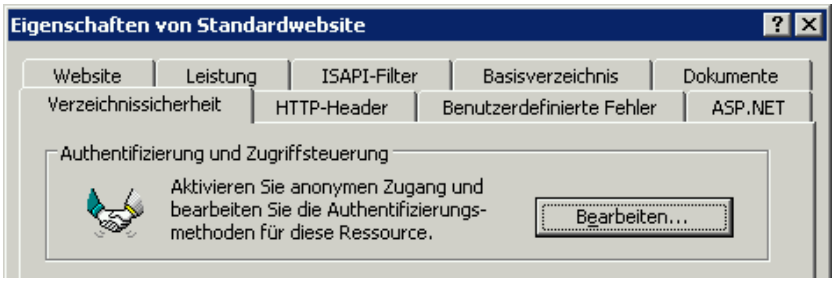
9. Aktivierung des Betriebssystem-Features „Windows Search“

Um in der Online-Hilfe von UniWeb die Suchfunktion nutzen zu können, muss das Betriebssystem-Feature „Windows Search“ aktiviert sein. Das UniWeb-Setup aktiviert dieses Feature automatisch auf einem Windows Server (ab Version 2008 R2). Dieses Feature kann in der Systemsteuerung oder im Server-Manager über die Funktion *Windows-Features hinzufügen* aktiviert werden. Wenn das Feature manuell installiert wurde, muss ggfs. das UniWeb-Setup noch einmal ausgeführt werden, damit die Suche in der Online-Hilfe von UniWeb ordnungsgemäß funktioniert.

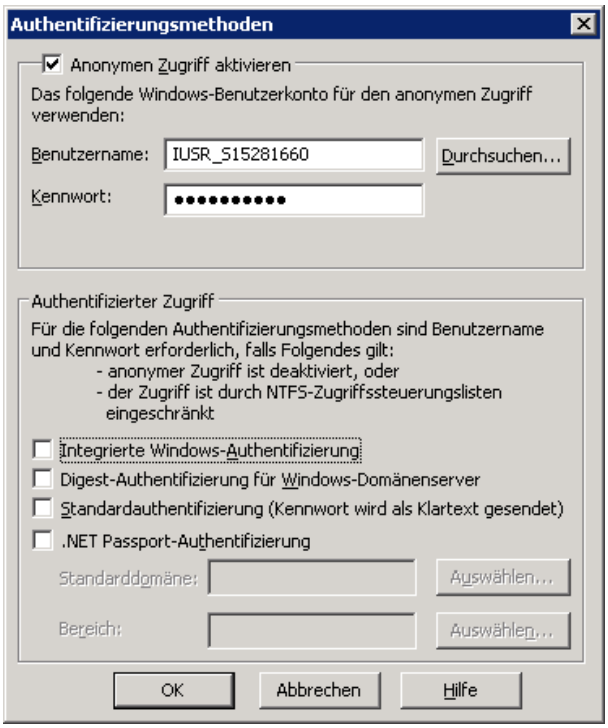
Weitere Hinweise

1. Windows-Authentifizierung im IIS 6 deaktivieren

Auf einem IIS 6.0 muss die integrierte Windows-Authentifizierung für die Webseite deaktiviert werden.



Dazu öffnet man den Eigenschaften-Dialog der Webseite und klickt im Reiter *Verzeichnissicherheit* im Bereich *Authentifizierung und Zugriffssteuerung* auf <*Bearbeiten...*>.

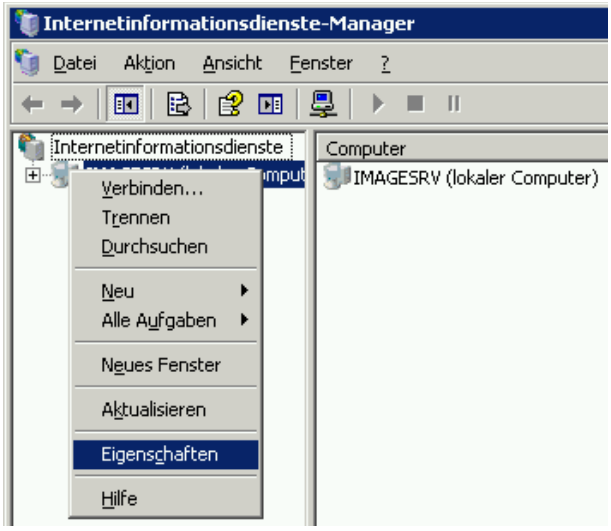


Im Bereich *Authentifizierter Zugriff* muss der Haken bei *Integrierte Windows-Authentifizierung* entfernt werden.

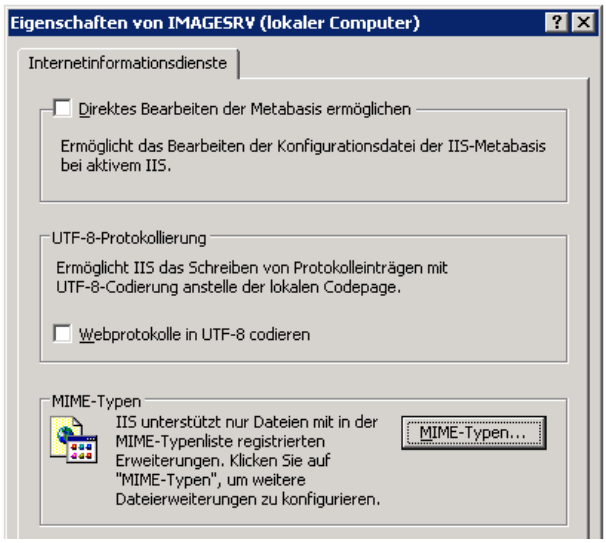
2. MIME-Typen im IIS 6 hinzufügen

Auf dem IIS 6.0 müssen folgende MIME-Typen hinzugefügt werden:

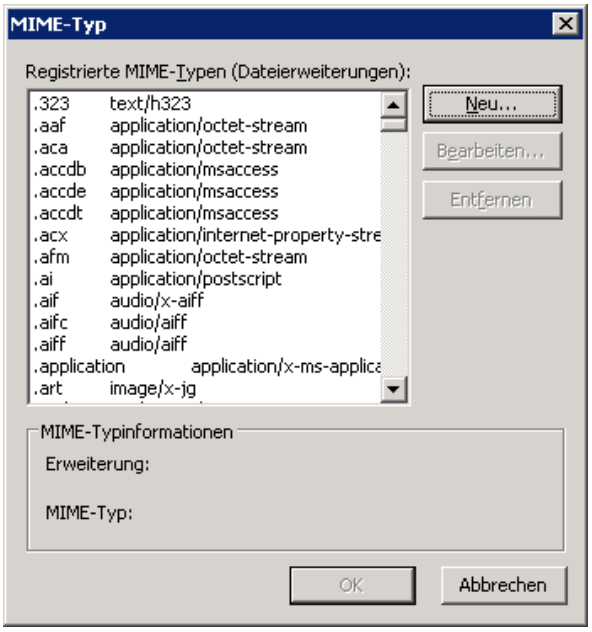
.xap application/x-silverlight-app
.xaml application/xaml+xml
.xbap application/x-ms-xbap
.uak application/octet-stream
.ann text/xml
.svg image/svg+xml



Öffnen Sie dazu den *Eigenschaften*-Dialog des Webservers im Internetinformationsdienste-Manager.



Im *Eigenschaften*-Dialog klicken Sie anschließend auf die Schaltfläche <*MIME-Typen...*>.



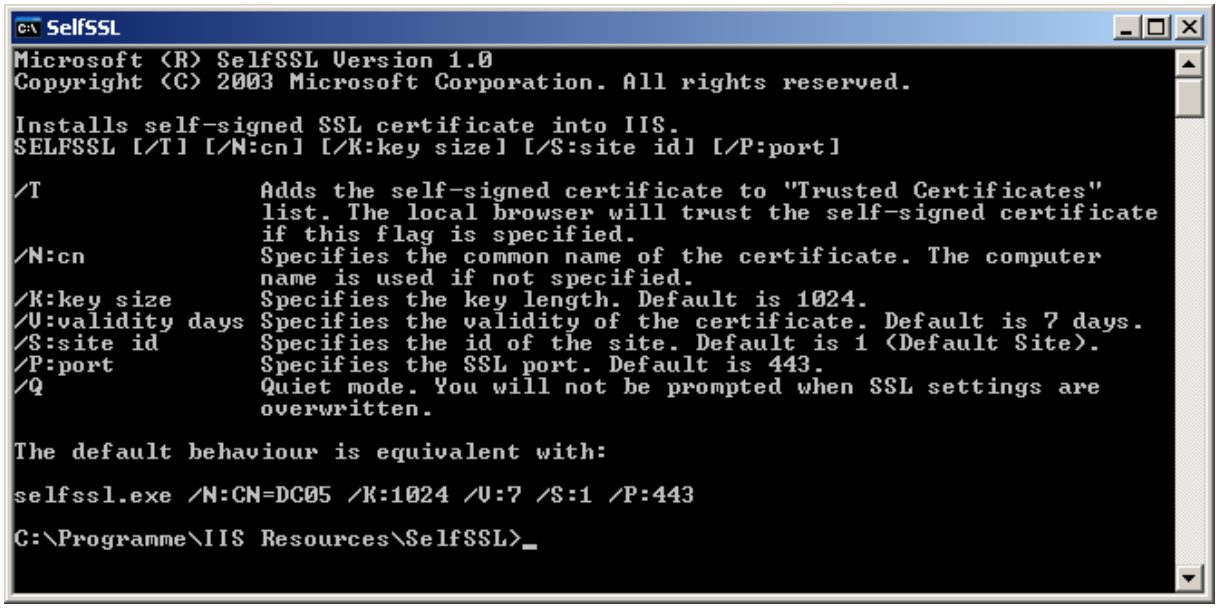
Über die Schaltfläche <*Neu...*> können Sie die oben genannten MIME-Typen hinzufügen.

3. Selbstsigniertes Zertifikat für den IIS 6 erzeugen und installieren

Mit einem IIS 6.0 ist es noch nicht möglich, über die grafische Benutzeroberfläche ein selbstsigniertes Zertifikat zu erzeugen. Um ein selbstsigniertes Zertifikat für den IIS 6.0 zu erzeugen und zu konfigurieren, benötigt man das *IIS Resource Kit*. Dieses kann man kostenlos von der Microsoft-Webseite herunterladen:

http://www.microsoft.com/en-us/download/details.aspx?id=17275

Zuerst muss das *IIS Resource Kit* installiert werden. Dazu startet man das Installationsprogramm *iis60rkt.exe* und wählt die Standardoptionen. Achten Sie bei einer benutzerdefinierten Installation darauf, dass die Komponente *SelfSSL* auswählt ist.



Nach der Installation kann das Programm SelfSSL.exe von der Eingabeaufforderung oder aus einer Batch-Datei heraus im Verzeichnis C:\Programme\IIS Resources\SelfSSL\ aufgerufen werden. Über die folgenden Parameter können die Eigenschaften des Zertifikats festgelegt werden:

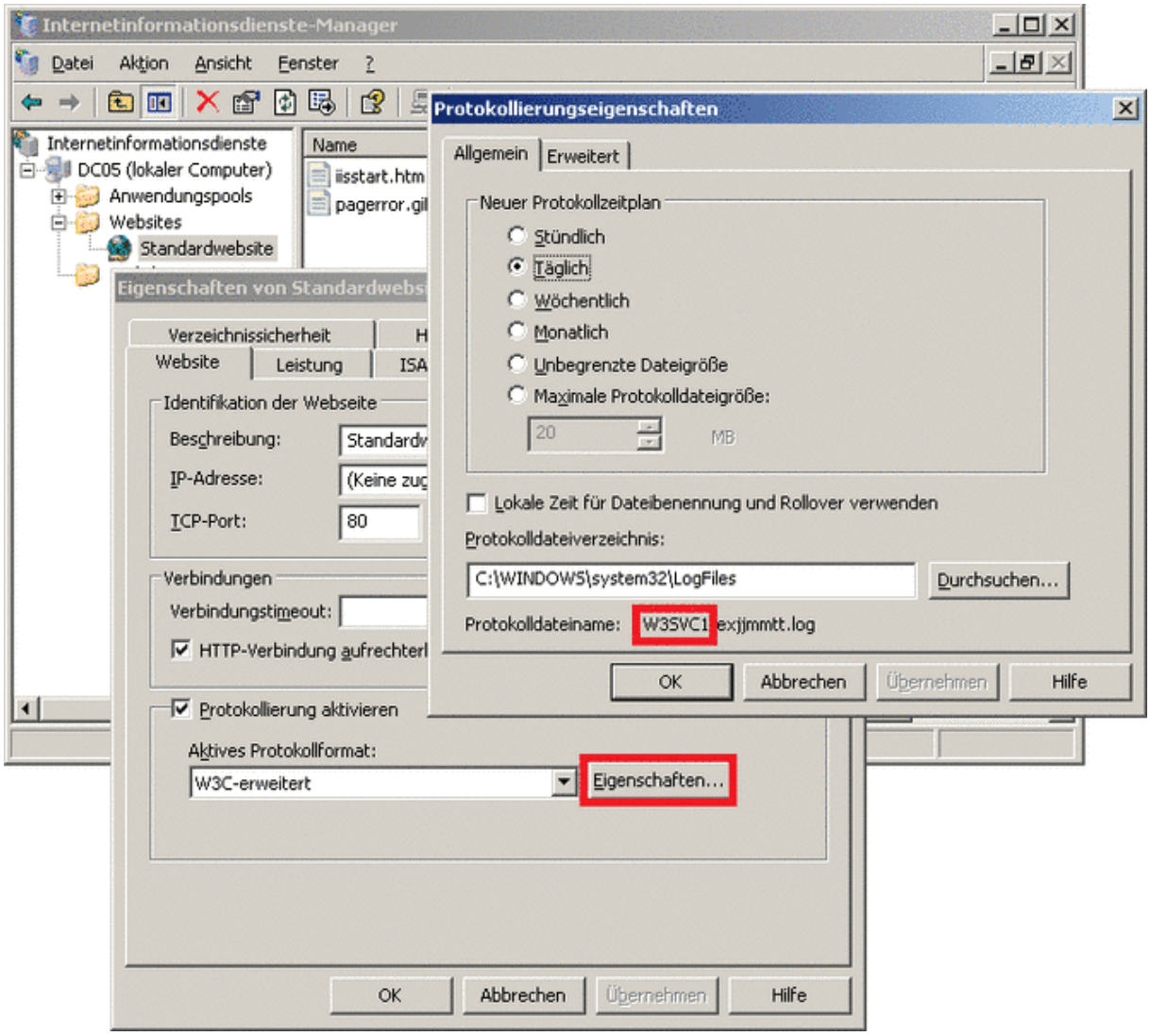
/T Mit dieser Option wird das selbst erzeugte Zertifikat zu den eigenen vertrauenswürdigen Zertifikaten hinzugefügt. Das bedeutet nicht, dass dem Zertifikat auch auf den Clients vertraut wird, die auf den IIS zugreifen. Dies kann man nur über ein kommerzielles Zertifikat erreichen oder aber, in dem man das selbst erzeugte Zertifikat den vertrauenswürdigen Zertifikaten auf den Clients hinzufügt, die auf den IIS-Server zugreifen.

/N: Der sog. *common name* des Zertifikats. Dies ist in der Regel der vollqualifizierte Name des Servers oder der URL, über die die Webseite erreicht werden soll (z.B.: CN=www.domain.de). Hinweis: Das „CN=“ bei der Option „/N:“ muss unbedingt angegeben werden.

/K: Die Länge des Schlüssels, der zur Verschlüsselung des Datenverkehrs verwendet wird. Der Standardwert ist 1024. Kürzere Schlüssellängen sollten auf keinen Fall verwendet werden.

/V: Die Gültigkeitsdauer des Zertifikats in Tagen. Hier können beliebige Werte angegeben werden.

/S: Hier muss die ID der Webseite im IIS angegeben werden. Die Standardwebseite hat immer die ID 1. Sind mehrere Seiten auf dem IIS vorhanden, muss hier die korrekte ID eingegeben werden. Herausfinden kann man die ID beispielsweise, in dem man über die Eigenschaften der zu sichernden Webseite die Eigenschaften der Protokollierung anklickt und die Zahl hinter „W3SVC“ notiert:



/P: Die Portnummer, über die die Webseite auf dem IIS betrieben wird. Der Standardwert ist 443.

Ein Aufruf des Programms SelfSSL.exe könnte dann z.B. so aussehen:

```
selfssl.exe /T /N:CN=server1.domain.de /K:2048 /V:365 /S:1 /P:443
```

4. UniWeb mit dem IIS Express betreiben

Für Test- oder Demozwecke besteht auch die Möglichkeit UniWeb mit dem IIS Express zu betreiben. Der IIS Express ist ein auf die wichtigsten Funktionen beschränkter Webserver zum Entwickeln und Testen von Webanwendungen unter Windows. Im Produktiveinsatz sollte aber immer die Vollversion des IIS-Webservers verwendet werden.

Wenn Sie UniWeb mit dem IIS Express installieren wollen, dann rufen Sie das UniWeb-Setup über ein Batch-Skript mit dem Parameter /DEMO auf. Bitte beachten Sie die Einschränkung, dass der IIS Express nicht als Windows-Dienst, sondern nur als Konsolenanwendung gestartet werden kann. Mit dem Abmelden des Windows-Benutzers steht demzufolge auch UniWeb nicht mehr zur Verfügung.

Zum Starten des Webservers rufen Sie Anwendung *C:\Program Files (x86)\IIS Express\iisexpress.exe* auf. Das UniWeb-Setup legt außerdem eine Verknüpfung auf dem Desktop an, über die der IIS Express auch gestartet werden kann. Das Setup generiert außerdem eine Konfigurationsdatei für den IIS Express, sodass die UniWeb-Seite automatisch vom IIS Express bereitgestellt wird. Der Aufruf der UniWeb-Seite erfolgt, indem Sie in Ihrem Browser die Adresse https://localhost:44300 aufrufen. Wenn Sie die UniWeb-Seite auch für andere Rechner bereitstellen möchten, dann müssen Sie den IIS Express mit Administratorrechten starten. Die Einstellungen der Webseite werden benutzerbezogen in der Datei *applicationhost.config* konfiguriert. Diese Datei befindet sich im Dokumente-Ordner des aktuellen Windows-Benutzers im Unterverzeichnis IISExpress\config\.

Weitere Hinweise zum Konfigurieren von IIS Express finden Sie auf der Internetseite

http://learn.iis.net/page.aspx/860/iis-express/

5. Internet-Zugriff auf UniWeb

Folgende Einstellungen müssen im eigenen Netzwerk vorgenommen werden, damit der UniWeb-Server auch über das Internet erreichbar ist:

Portweiterleitung

Auf dem Internet-Router des eigenen Netzwerks muss eine Port-Weiterleitung zum internen UniWeb-Server eingerichtet werden. Dabei muss beachtet werden, dass die öffentliche Portnummer und die Portnummer der Webseite auf dem UniWeb-Server identisch sind. Der UniWeb-Server ist standardmäßig über HTTPS auf dem TCP-Port *443* erreichbar. Eine gültige Port-Weiterleitung auf dem Router sähe dann z.B. so aus:

Public Port:	*443*
Private Port:	*443*
Port Type:	*TCP*
Host IP-Adress:	*interne IP-Adresse des UniWeb-Servers z.B. 192.168.0.7*

Hostname / IP-Adresse

Der Internet-Router des eigenen Netzwerks muss entweder über eine feste IP-Adresse oder einen eindeutigen Hostnamen aus dem Internet erreichbar sein. Zusammen mit der Port-Weiterleitung ist der UniWeb-Server dadurch über eine feststehende Adresse erreichbar. Bei einem einfachen DSL-Anschluss besteht das Problem, dass man vom DSL-Anbieter bei jeder Einwahl eine andere öffentliche IP-Adresse zugewiesen bekommt.

Eine Möglichkeit wäre, die eigene Internetanbindung über einen höherwertigen DSL-Anschluss mit feststehender IP-Adresse zu realisieren. Dies ist im Allgemeinen aber auch mit höheren Kosten verbunden. Die Alternative dazu ist, die eigene öffentliche IP-Adresse über dynamisches DNS mit einem festen Host-Namen zu verknüpfen. Bei den meisten Anbietern dynamischer DNS-Dienste ist zumindest ein Eintrag in der Regel kostenlos. Viele aktuelle Internet-Router besitzen zudem bereits einen eingebauten Dynamic DNS (DDNS) Client, so dass man idealerweise einen DDNS-Anbieter wählt, der vom Router direkt unterstützt wird.

Firewall-Einstellungen

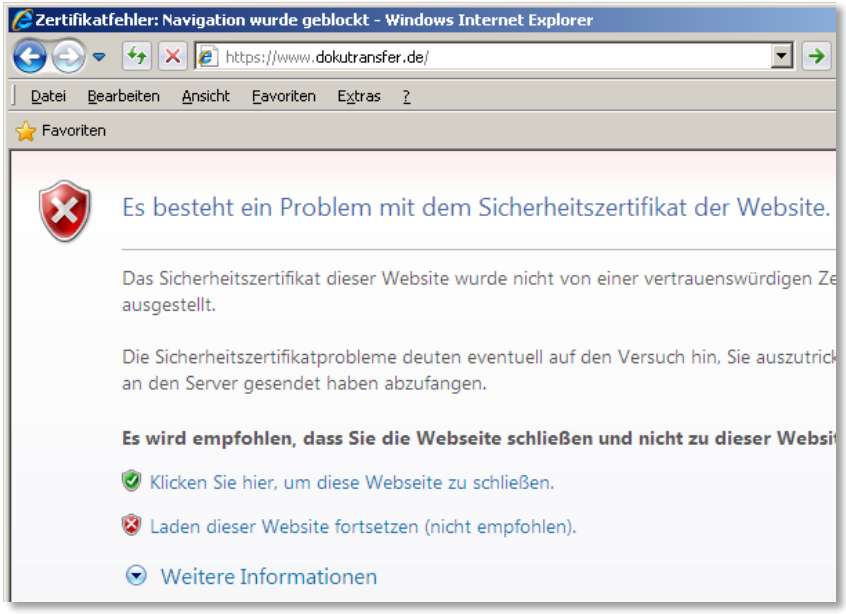
Für den UniWeb-Server müssen standardmäßig eingehende Verbindungen auf TCP-Port 443 zugelassen werden, vorausgesetzt der UniWeb-Server wurde nicht für die Verwendung eines anderen Ports konfiguriert. Dies gilt sowohl für die Windows-Firewall auf dem UniWeb-Server als auch für die Firewall des lokalen Netzwerks.

SSL-Zertifikat

Die Bereitstellung der UniWeb-Seite erfolgt über das verschlüsselte HTTPS-Protokoll und erfordert demzufolge ein gültiges SSL-Zertifikat für die Domain/URL, über welche die UniWeb-Seite vom Internet aus zu erreichen ist. Man kann für die Bereitstellung auch ein nicht vertrauenswürdiges selbstgeniertes Zertifikat verwenden. In diesem Fall wird aber bei jedem Aufruf der Seite im Browser eine Zertifikatswarnung angezeigt.

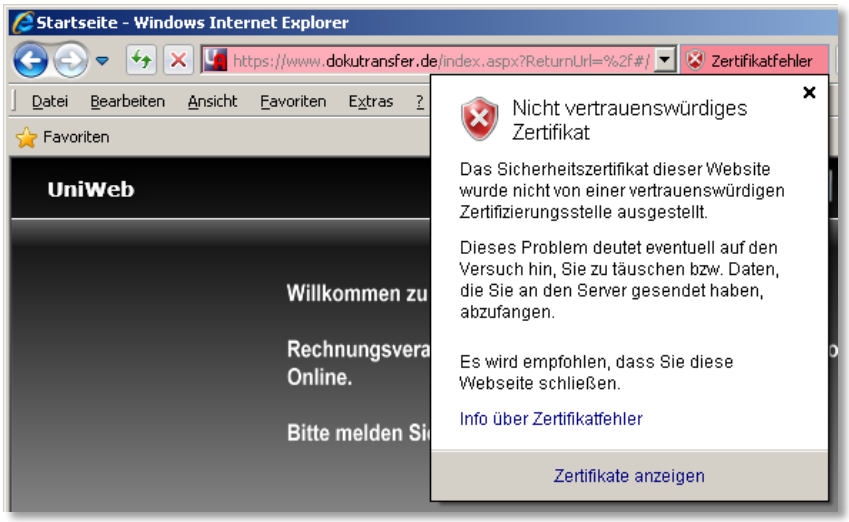
6. Abstellen der Zertifikatswarnung für UniWeb im Internet Explorer

Das UniWeb-Portal ist eine Online-Plattform auf Basis der Microsoft Silverlight-Technologie. Die komplette Umgebung wird als Webseite auf einem Microsoft IIS-Webserver über https bereitgestellt. Hierzu kann entweder ein vertrauenswürdiges Zertifikat oder ein selbstsigniertes Zertifikat verwendet werden. Bei einem selbstsignierten Zertifikat ist zu beachten, dass im Webbrowser eine Zertifikatswarnung ausgegeben wird, dass das verwendete SSL-Zertifikat nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde. An dieser Stelle muss man die zweite angebotene Option wählen und das Laden der Webseite fortsetzen.

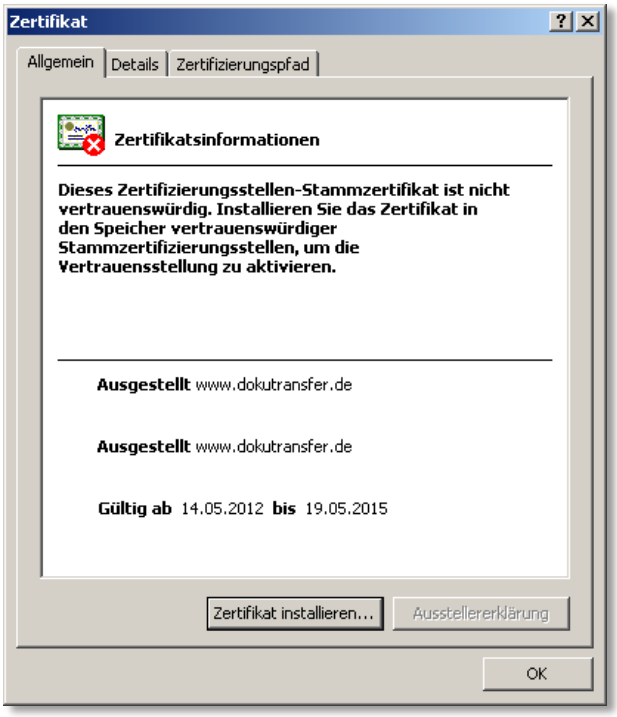


Nachdem die Seite vollständig geladen wurde, wird in der Adresszeile des Browsers ein Zertifikatsfehler angezeigt. Zum Anzeigen des Fehlers klicken Sie auf das Symbol *Zertifikatsfehler* und anschließend auf *Zertifikate anzeigen*.

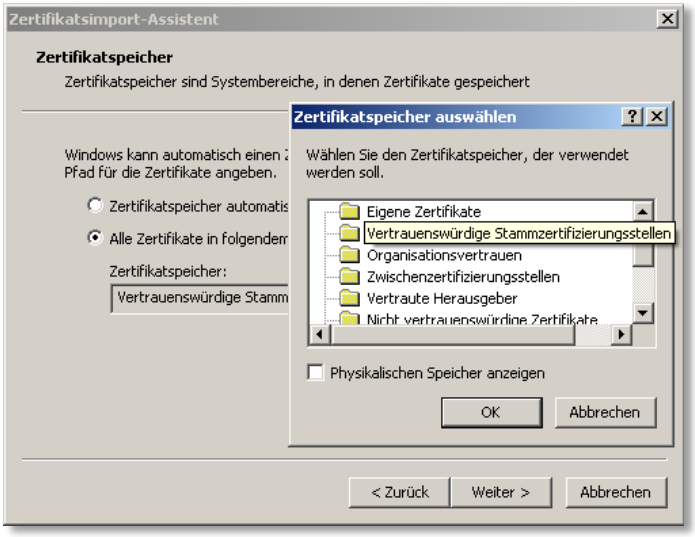
Installieren des Zertifikats



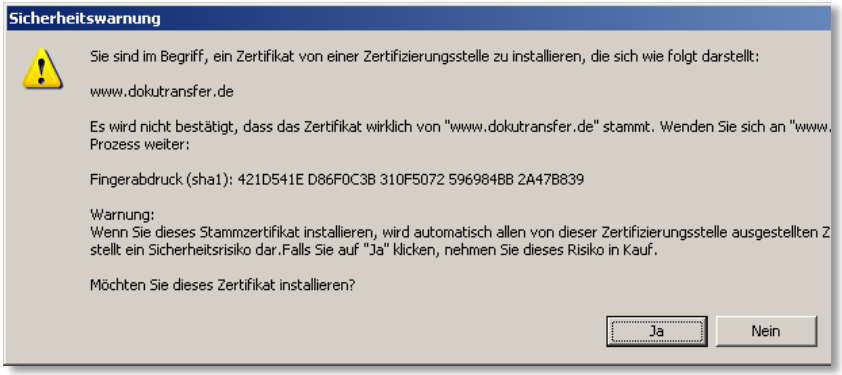
Im Dialog *Zertifikatsinformationen* klicken Sie anschließend auf *Zertifikat installieren...* .



Im darauffolgenden Assistenten müssen Sie den Zertifikatspeicher manuell auswählen. Wählen Sie als Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* aus.



Vor der Installation des Zertifikats wird noch eine Sicherheitswarnung angezeigt. Diese muss mit *Ja* bestätigt werden.



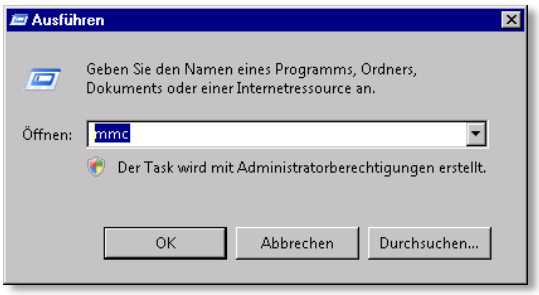
Wenn das Zertifikat erfolgreich installiert wurde, wird eine entsprechende Meldung ausgegeben. Gegebenenfalls muss der Internet Explorer anschließend neu gestartet werden, damit in der Adressleiste kein Zertifikatsfehler mehr angezeigt wird.

Wenn Sie die Webseite nach dem Neustart des Internet Explorers erneut aufrufen, sollte kein Zertifikatsfehler mehr angezeigt werden. Stattdessen kann nun ein Sicherheitsbericht über das verwendete Zertifikat zur SSL-Verschlüsselung abgerufen werden.

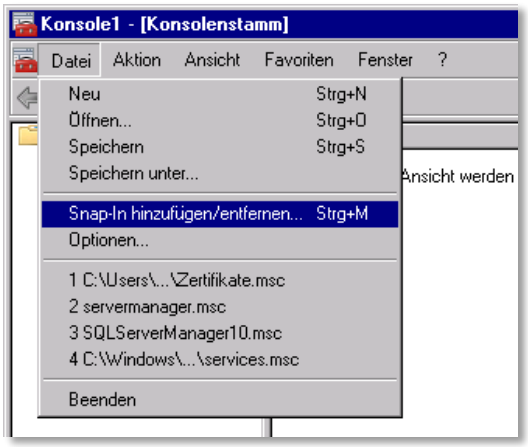
Zertifikat für alle Benutzer bereitstellen

Das im vorangegangenen Schritt beschriebene Verfahren installiert das Zertifikat im Zertifikatspeicher des aktuellen Benutzers. Um das Zertifikat allen Benutzern des Computers zur Verfügung zu stellen, muss man das installierte Zertifikat aus dem Zertifikatspeicher des aktuellen Benutzers in den Zertifikatspeicher des lokalen Computers kopieren.

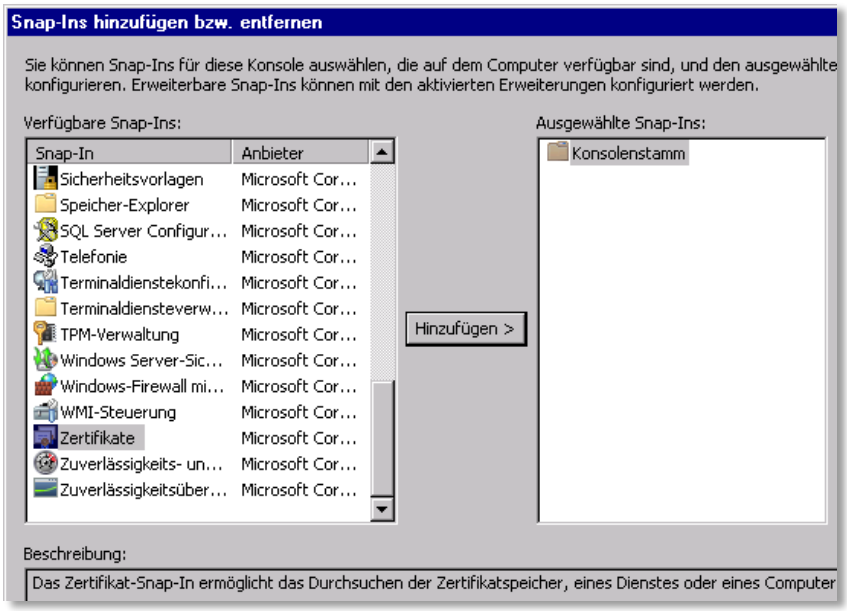
Dazu gehen Sie folgendermaßen vor:



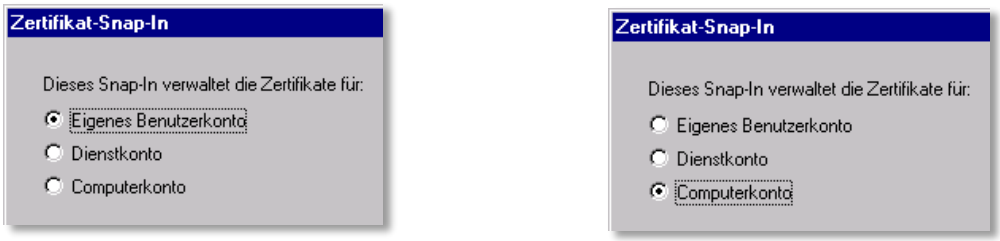
Öffnen Sie die Windows Management-Konsole indem Sie z.B. aus dem Windows-Startmenü *Ausführen* aufrufen, *mmc* eingeben und mit *Enter* bestätigen.



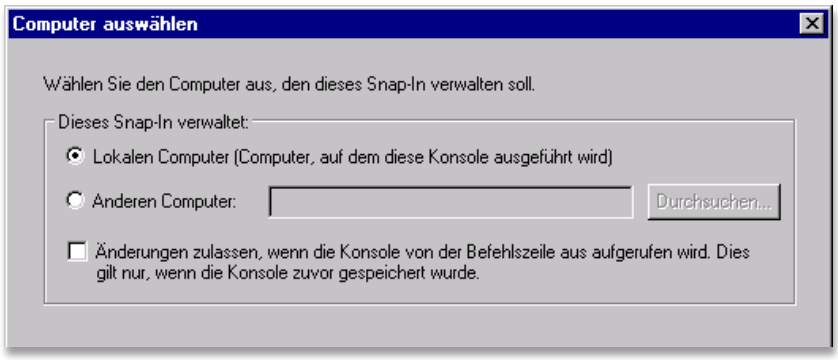
In der Management-Konsole wählen Sie aus dem Menü *Datei* den Eintrag *Snap-In hinzufügen / entfernen...* aus.



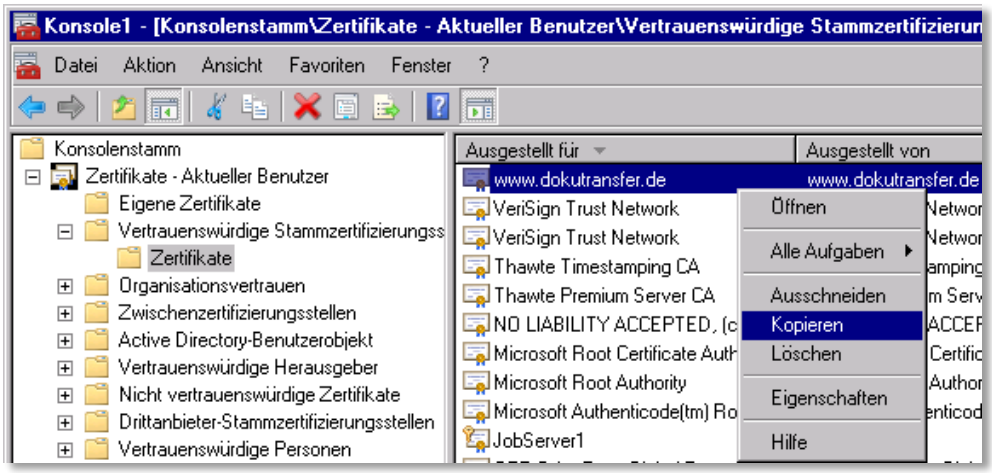
Wählen Sie bei den verfügbaren Snap-Ins *Zertifikate* aus und klicken Sie auf *Hinzufügen*.



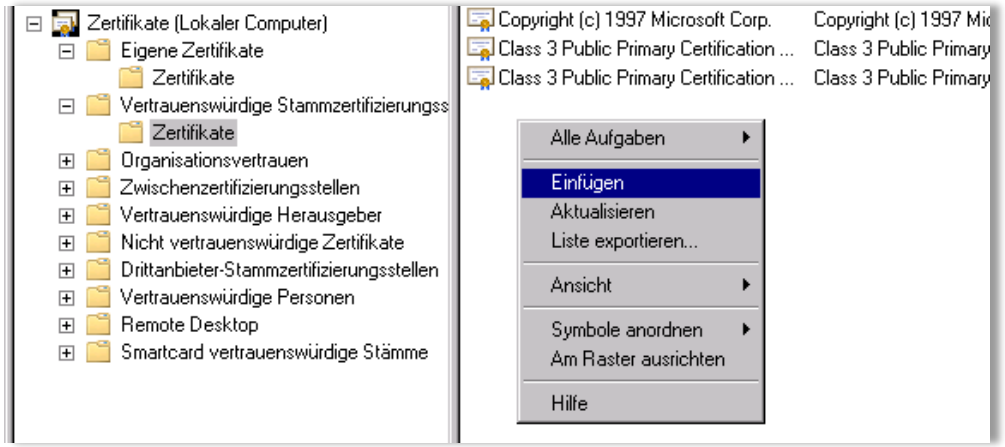
Im anschließenden Dialogfenster wählen Sie *Eigenes Benutzerkonto* aus und bestätigen ihre Auswahl. Fügen Sie anschließend noch einmal das Snap-In *Zertifikate* hinzu und wählen diesmal *Computerkonto* aus.



Im anschließenden Dialog wählen Sie *Lokaler Computer* aus und bestätigen Ihre Auswahl.



Navigieren Sie nun in den Zertifikaten des aktuellen Benutzers zum Ordner *Zertifikate* der vertrauenswürdigen Stammzertifizierungsstellen. Hier sollten Sie das zuvor über den Browser hinzugefügte Zertifikat wiederfinden. Markieren Sie das Zertifikat und wählen aus dem Kontextmenü *Kopieren* aus.



Navigieren Sie nun in den Zertifikaten des lokalen Computers zum Ordner Zertifikate der vertrauenswürdigen Stammzertifizierungsstellen. Hier können Sie das zuvor kopierte Zertifikat über das Kontextmenü wieder einfügen. Anschließend können Sie die Management-Konsole wieder schließen.

7. Hinweise zu Antiviren-Programmen

Da Virenscanner sehr tief ins System eingreifen, kann es bei anderen Anwendungen zu Problemen kommen, wenn sie gescannt werden. Zumeist kommen diese Probleme beim Echtzeitscan zum Tragen. Um Komplikationen zu verhindern, erlauben die meisten Virenscanner das Führen einer Ausschlussliste, in der definiert werden kann, welche Daten nicht vom Echtzeitscanner überwacht werden sollen.

Deshalb müssen für eine UniWeb-Installation das lokale Uniarchiv-Verzeichnis für temporäre Dateien, die Uniarchiv-Datenfreigabe und die TEMP-Verzeichnisse des Betriebssystems von der Echtzeitüberprüfung der installierten Antiviren-Programme ausgeschlossen werden.

Ebenso sollten etwaige Indizierungsdienste, insbesondere der Windows-Indizierungsdienst, diese Verzeichnisse ausschließen.

Glossar

Portweiterleitung

Eine Portweiterleitung ist die Weiterleitung einer Verbindung, die über ein Rechnernetz auf einem bestimmten Port eingeht, zu einem anderen Computer.

Ein Router, der beispielsweise mit einem privaten lokalen Netz und dem Internet verbunden ist, wartet dabei an einem bestimmten Port auf Datenpakete. Wenn Pakete an diesem Port eintreffen, werden sie an einen bestimmten Computer und gegebenenfalls einen anderen Port im internen Netzwerk weitergeleitet. Alle Datenpakete von diesem Computer und Port werden, wenn sie zu einer eingehenden Verbindung gehören, per NAT so verändert, dass es im externen Netz den Anschein hat, der Router würde die Pakete versenden.

Durch eine Portweiterleitung wird es Rechnern innerhalb eines LAN, welche von einem externen Netz nicht direkt erreichbar sind, somit möglich, auch außerhalb dieses Netzes, insbesondere auch im Internet als Server zu fungieren, da diese somit über einen festgelegten Port eindeutig ansprechbar gemacht werden. Für alle Rechner im externen Netz sieht es anschließend so aus, als ob der Router den Serverdienst anbietet.

Dynamisches DNS

Das Domain Name System (DNS) ist ein auf mehrere Server im Netzwerk verteilter Dienst und dient der Namensauflösung von Hostnamen in IP-Adressen. Dynamisches DNS (DDNS) ist ein System zur Aktualisierung von DNS-Einträgen in Echtzeit. Ständig wechselnde Einträge sind im DNS in der Regel nicht vorgesehen. Es gibt aber spezielle Anbieter, die diesen Service (in gewissen Umfang auch kostenlos) anbieten.

Um einen dynamischen DNS-Eintrag bei einem solchen Anbieter zu aktualisieren, wird üblicherweise eine spezielle Client-Software verwendet, die sich automatisch bei einem Wechsel der öffentlichen IP-Adresse mit einem Nameserver des DDNS-Anbieters verbindet und die neue IP-Adresse des Rechners übermittelt. Viele aktuelle DSL-Router haben einen derartigen Client bereits integriert.

HTTPS / SSL

HTTPS steht für Hypertext Transfer Protocol Secure. Dieses Kommunikationsprotokoll wird im Internet benutzt, um Daten abhörsicher zu übertragen. Das HTTPS-Protokoll wird zur Verschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver und Browser im World Wide Web verwendet.

Die Authentifizierung dient dazu, dass sich jede Seite der Identität des Verbindungspartners vergewissern kann. Die Verschlüsselung der Daten geschieht mittels SSL (Secure Sockets Layer). Unter Verwendung des SSL-Handshake-Protokolls findet zunächst eine geschützte Identifikation und Authentifizierung der Kommunikationspartner statt.

Der Standard-Port für HTTPS-Verbindungen ist 443. Weiterhin ist ein Digitales Zertifikat für SSL notwendig. Ein digitales Zertifikat wird im Allgemeinen von einer selbst wiederum zertifizierten Zertifizierungsstelle ausgestellt und identifiziert den Server und die Domain eindeutig. Bei der Beantragung werden zu diesem Zweck z.B. die Adressdaten und die Firmierung des Antragstellers geprüft.

Für weitergehende Fragen stehen wir Ihnen gerne zur Verfügung.

Mail: uniarchiv@bdv.com

Hotline: 02301 / 9109120

Ihr BDV Team

BDV Branchen-Daten-
Verarbeitung GmbH
Ziegelstraße 1
59439 Holzwickede

Fon 02301 / 9109120
Fax 02301 / 8640

uniarchiv@bdv.com
www.bdv.com