MS IIS 2003

MS Internet Information Services 6.0

Christian Zahler

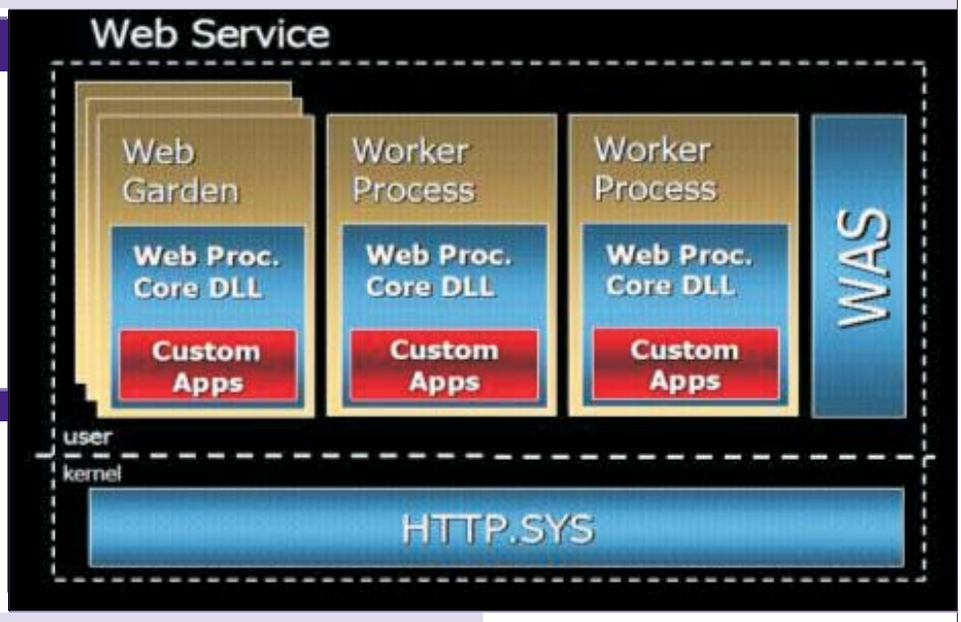
1 Installation der Microsoft Internet Information Services 6.0

Die Internet-Serverdienste sind in Windows 2003 Server bereits integriert; sie werden allerdings – anders als bisher - bei der Installation des Servers nicht mehr mitinstalliert.

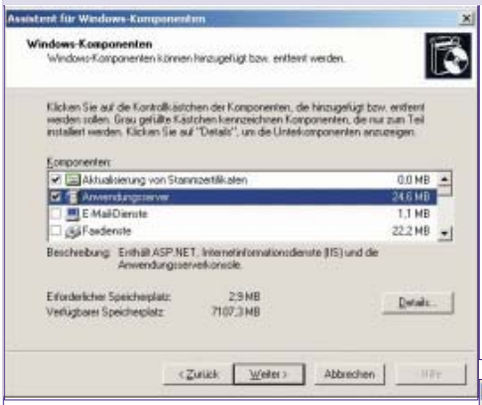
In der Systemsteuerung können unter ***„Software“*** – ***„Windows-Komponenten hinzufügen/entfernen“*** verschiedene Internet-Dienste installiert werden. Wählen Sie zunächst ***„Anwendungsserver“*** und klicken Sie für die genauere Konfiguration auf die Schaltfläche ***„Details“***.

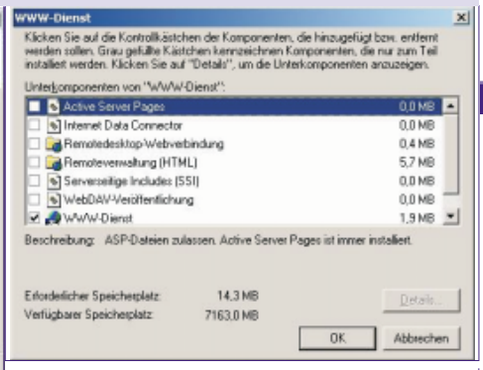
2 Architektur

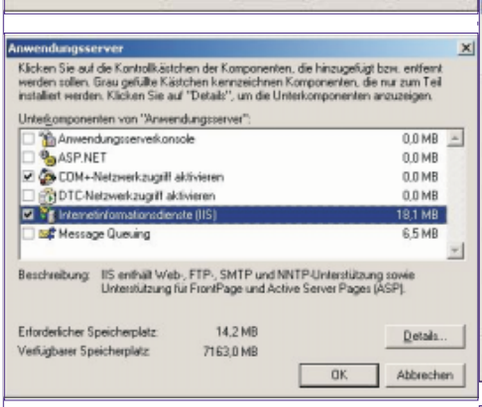
Alle Internet-Dienste werden von einem ausführbaren Dienst – `http.sys` – verwaltet, stellen aber – anders als früher – mehrere Dienste dar. Sämtliche Einstellungen der IIS-Dienste sind in der „Metabase“ gespeichert. Die Metabase kann basiert auf XML und kann direkt editiert werden. Die Metabase befindet sich im Verzeichnis %system%\inetsrv und hat den Dateinamen metabase.xml.

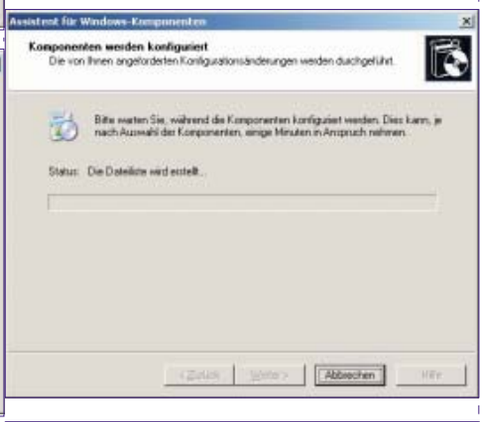


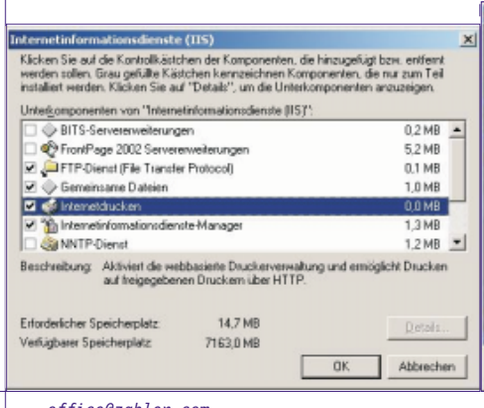
Installation des IIS

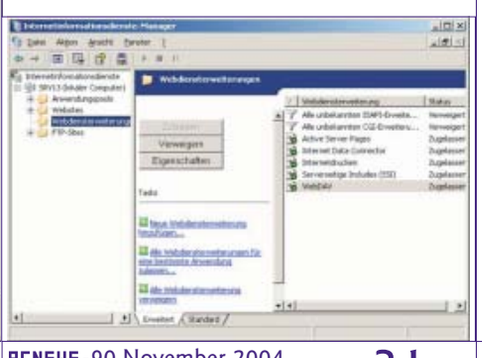












3 Administration

Wählen Sie ***Start*** – ***Programme*** – ***Verwaltung*** – ***Internetinformationsdienste-Manager***.

Es wird die **Microsoft Management Konsole** (`MMC.EXE`) aufgerufen. Die MMC ist ein allgemeines Werkzeug zur Verwaltung von Serverdiensten; sie ist in Windows 2000 ein zentrales Administrationstool.

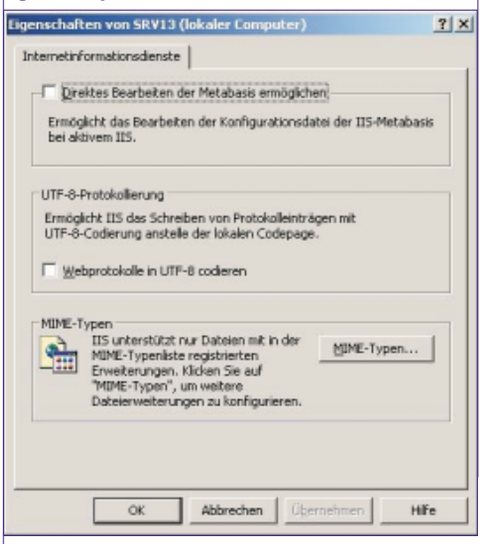
Man kann auch selbst eine Konsole definieren. Dazu ruft man `MMC.EXE` über ***Start*** – ***Ausführen*** auf und fügt ein sogenanntes **Snap-In** für verschiedene Administrationsaufgaben hinzu (Menü ***[Konsole]-[Snap-In hinzufügen/löschen]*** bzw. Strg M); die Einstellungen werden in Konfigurationsdateien gespeichert.

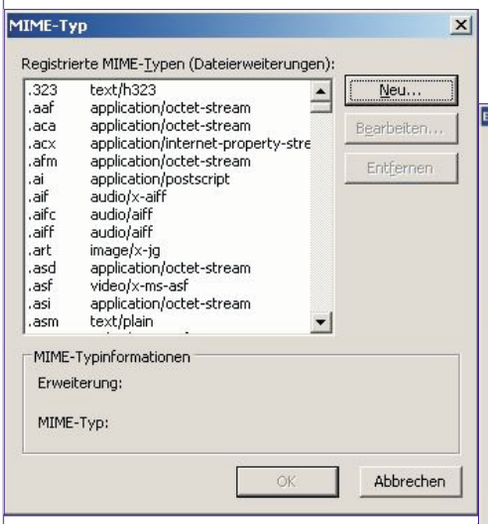
Ruft man den Internet-Dienstmanager auf, so wird bereits eine vorkonfigurierte Einstellung (Datei `IIS.MSC`) aufgerufen, die die Administration der Internet-Serverdienste stark vereinfacht.

Die Internet-Diensteverwaltung beruht auf der Datei `INETINFO.EXE`.

Allgemeine Diensteigenschaften:

Klicken Sie mit der rechten Maustaste auf das Symbol für Ihren Server (im Beispiel SRV13) und wählen Sie aus dem Kontextmenü ***„Eigenschaften“***.





4 Der WWW-Dienst im IIS

4.1 Standardwebsite

Besprechen Sie die einzelnen Karteikarten und deren Auswirkungen auf die Funktionalität der Website!

4.2 Verwalten mehrerer virtueller Websites

Der IIS ist in der Lage, mehrere Websites zu verwalten. Dazu gibt es folgende unterschiedliche Konfigurationsmöglichkeiten:

a) Unterschiedliche IP-Adressen

Jeder Website wird eine unterschiedliche IP-Adresse zugewiesen.

Vorteil: einfache Konfigurierbarkeit

Nachteil: oft ist die Anzahl vorhandener public IPs begrenzt; dieses Verfahren wird daher oft nur im Intranet-Bereich Verwendung finden können.

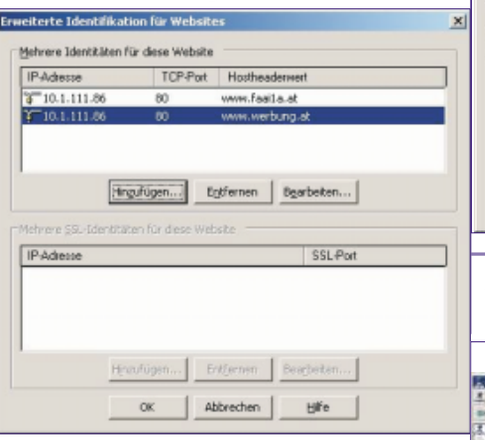
b) Gleiche IP-Adresse, unterschiedlicher TCP-Port

Die IP-Adresse wird für alle Websites einheitlich genommen, als Unterscheidungsmerkmal werden TCP-Ports aus dem frei verwendbaren Bereich ab Nr. 1024 genommen.

Nachteil: Um eine Website mit einem Nicht-Standard-TCP-Port zu erreichen, muss die Portnummer bekannt sein und in der Adresszeile des Browsers mit angegeben werden.

c) Host-Header-Name

Hier verwendet man ein Feld im HTTP-Header, in welchem ohnehin der nicht aufgelöste DNS-Name mitgesendet wird. Der IIS ist in der Lage, den DNS-Namen als Unterscheidungsmerkmal zu verwenden, sofern dies konfiguriert wurde. Voraussetzung ist die korrekte DNS-Konfiguration.



Es ist also denkbar, ein und dieselbe Webseite mit mehreren Domain-Namen aufzurufen.

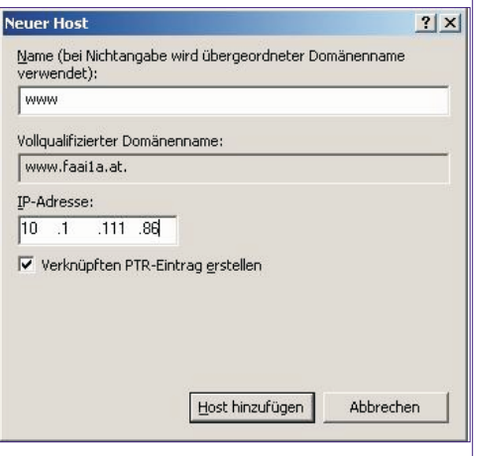
4.3 Einrichten einer Kunden-Website

4.3.1 Einrichten eines Basisverzeichnisses

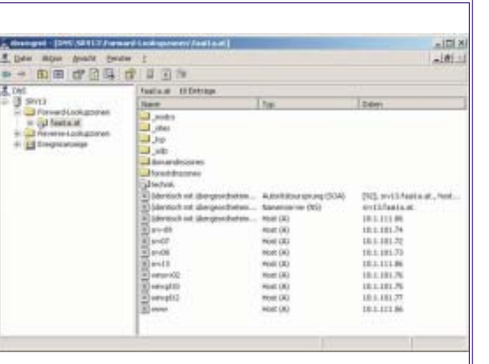
Richten Sie auf dem Webserver einen Ordner ein, in welchem die gesamte Website gespeichert werden soll.

4.3.2 Konfigurieren der DNS-Namensauflösung

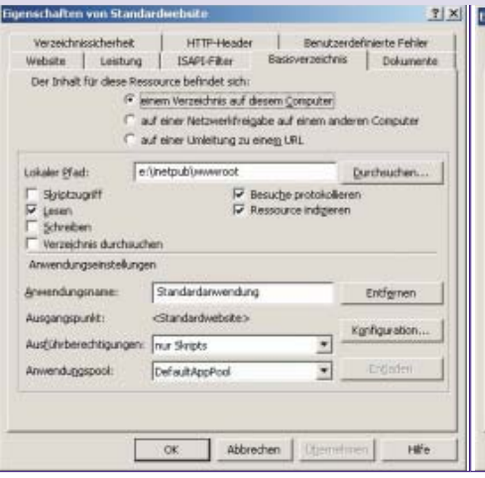
Richten Sie in der Forward-Lookup-Zone auf dem zuständigen DNS-Server einen A- oder CNAME-Eintrag für den von Ihnen gewünschten Namen ein.

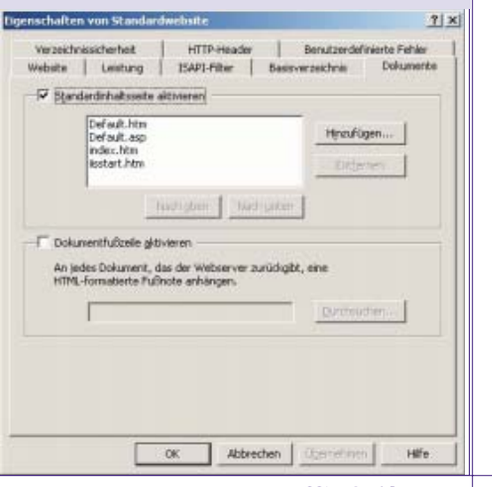


4.3.3 Anlegen eines virtuellen Webservers

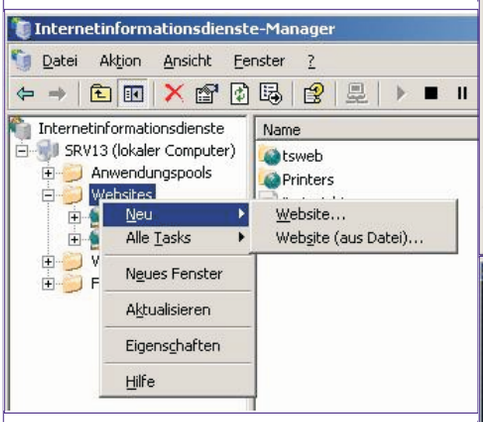


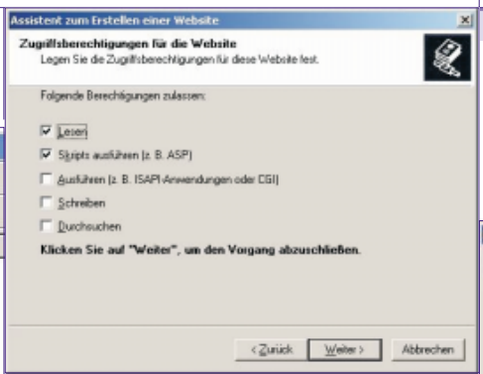
Standardwebsite Einstellungen

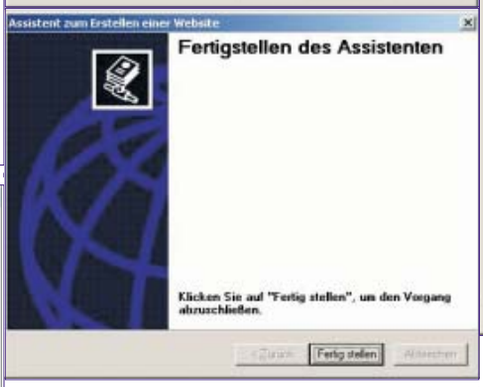




Zunächst legt man für den Kunden einen virtuellen Webserver (Website) an:

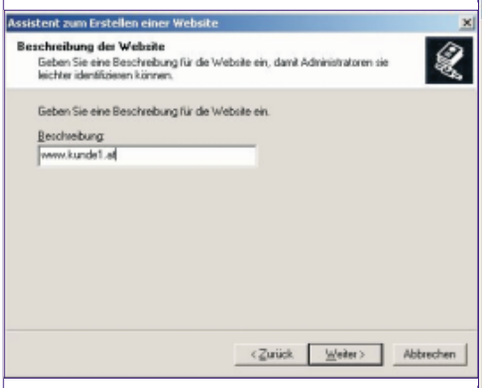


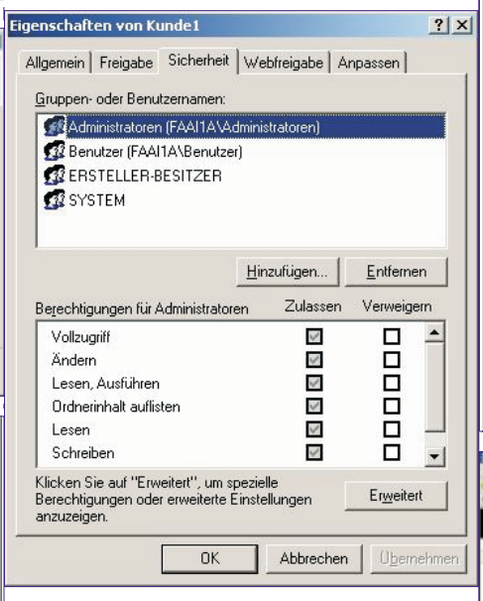


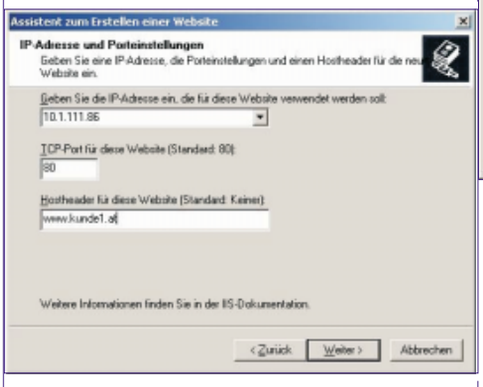


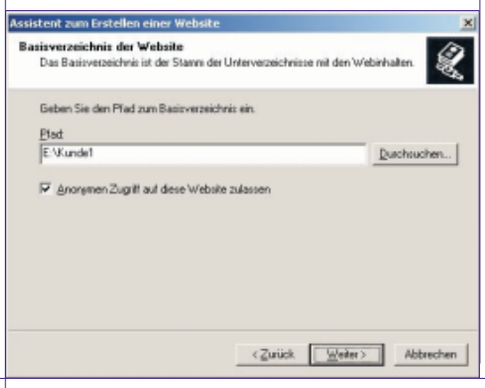
4.4 Absicherung einer Website

Die Rechtevergabe beruht auf NTFS-Berechtigungen, die etwa im Windows-Explorer für den gesamten Ordner gesetzt werden können.







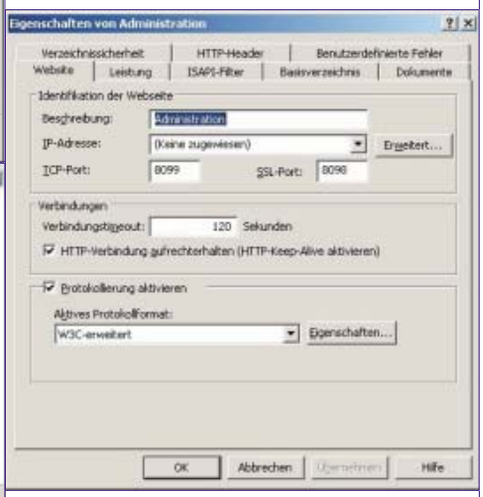


4.5 Verwaltungs-Website

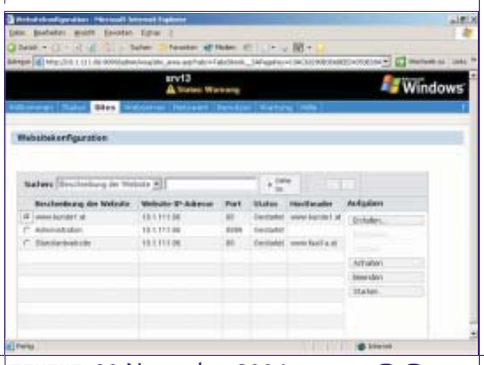
Die Verwaltungs-Website ist dreifach gesichert:

a) Verwendung eines nicht standardmäßigen TCP-Ports und

b) Verschlüsselte Übertragung mit SSL

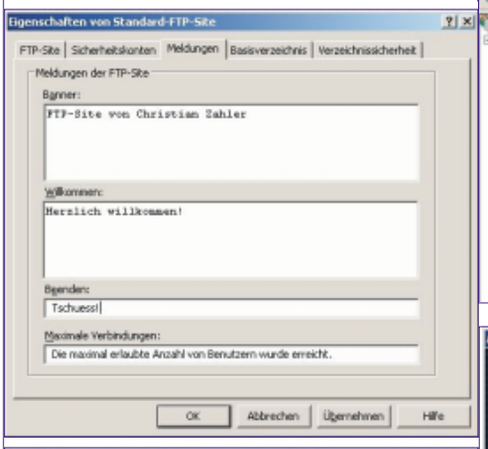


c) Die anonyme Anmeldung ist nicht möglich:



5 FTP-Server einrichten und testen

5.1 Standard-FTP-Site

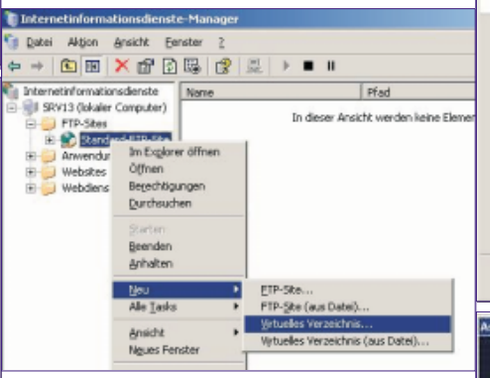


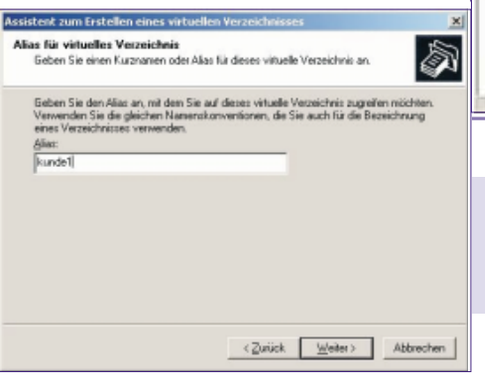
5.2 Einrichten und Konfigurieren eines FTP-Zugangs für die Wartung von Websites mit virtuellen Verzeichnissen

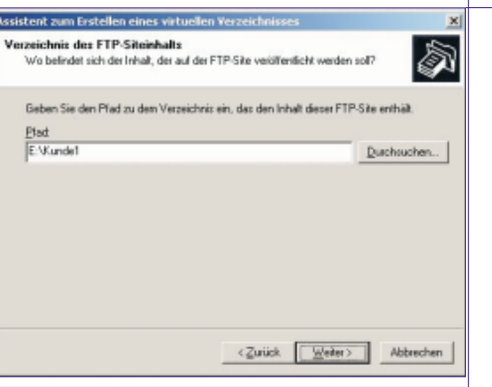
Der große Unterschied in der Konfiguration besteht darin, dass für FTP-Sites keine Host-Header zur Verfügung stehen. Es ist daher nur möglich, verschiedene IP-Adressen zu Grunde zu legen oder virtuelle Verzeichnisse zu nutzen.

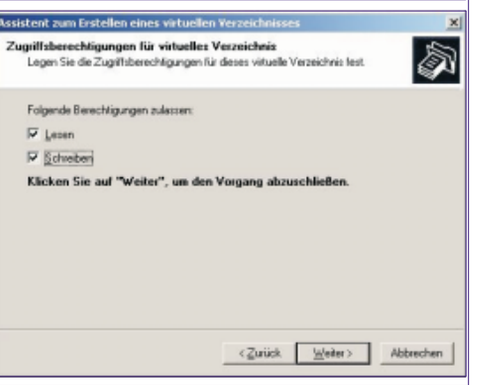
Oft werden FTP-Zugänge verwendet, um Websites remote zu warten und Inhalte auszutauschen. Dabei ist es jedoch empfehlenswert, keinen anonymen Zugriff zuzulassen.

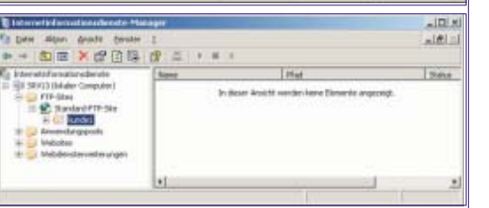
Hier ist es erforderlich, den anonymen Zugang für die **gesamte** FTP-Site zu deaktivieren!







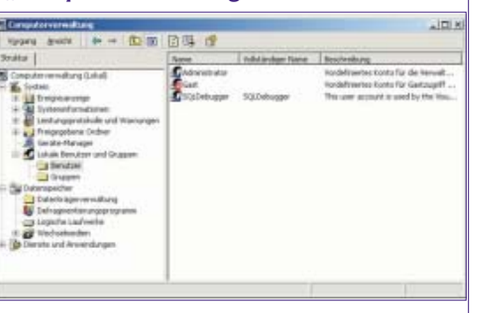




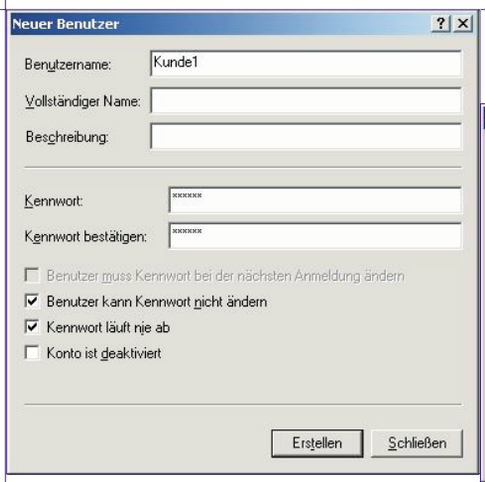
Konfigurieren eines lokalen Benutzerkontos

Besonders wichtig ist dieser Schritt, wenn der FTP-Server auf einem **Active Directory-Domänencontroller** installiert wird, da standardmäßig auf Domänencontrollern **keine lokale Anmeldung** möglich ist!

Start - ***Programme*** - ***Verwaltung*** – ***Snap-In „Computerverwaltung“*** auswählen

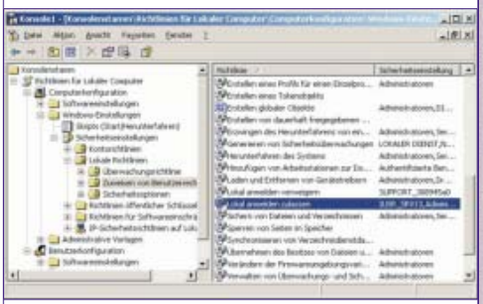


Für die Administration der Kunden-FTP-Site ist ein neues lokales Benutzerkonto anzulegen (Kontextmenü ***[Neuer Benutzer]***):

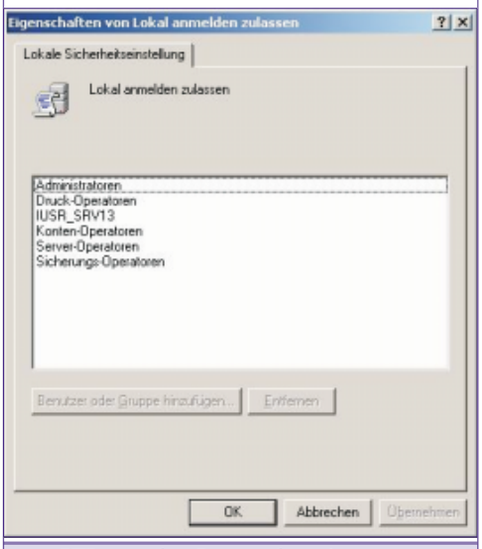


Nun muss sichergestellt werden, dass dieser Benutzer sich lokal am Webserver anmelden darf.

Dazu öffnet man das Snap-In ***„Lokale Sicherheitsrichtlinie“*** und wählt im Ordner ***„Lokale Richtlinien“*** die Kategorie ***„Zuweisen von Benutzerrechten“***:



Dort überprüft man, ob das neu angelegte Benutzerkonto die Berechtigung ***„Lokal anmelden“*** besitzt:



5.3 FTP von der Anwenderseite aus gesehen – FTP-Server testen

Mit FTP können Sie Dateien von Ihrem Rechner auf einen entfernten Server übertragen (**Upload**) oder von einem entfernten Server Dateien auf Ihren Rechner laden (**Download**).

Der FTP-Dienst ist auf verschiedene Art und Weise nutzbar:

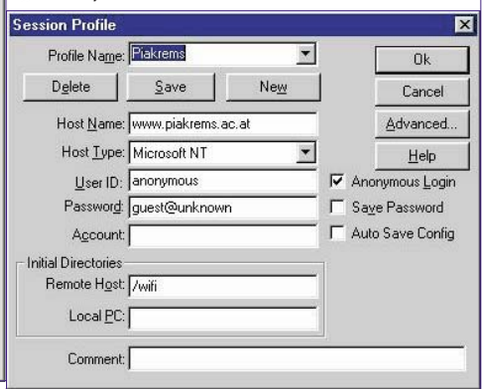
a) FTP-Programme (Beispiele):

- WS-FTP, FTPVoyager, CuteFTP

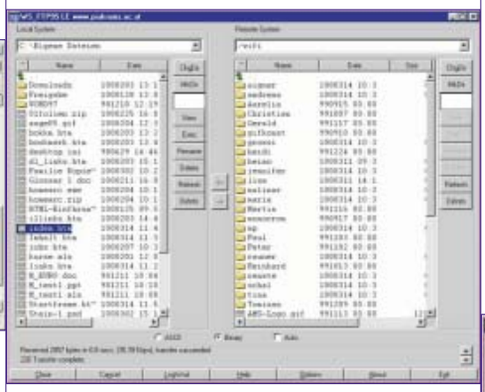
Es soll hier das Programm **WS-FTP95** kurz erläutert werden:

1. Starten Sie das Programm WS-FTP95

2. Legen Sie ein Profil mit folgenden Einträgen an (Klicken Sie auf die Schaltfläche ***„New“***):



3. Mit ***"OK"*** verbinden Sie sich zum PIAKREMS-FTP-Server: Links sehen Sie die Verzeichnis-/Laufwerksstruktur Ihres eigenen Rechners, rechts sehen Sie die Verzeichnisstruktur des FTP-Servers, mit dem Sie verbunden sind.



4. Mit den Pfeilen in der Mitte können Sie markierte Dateien von Ihrer Festplatte (links) auf den Server (rechts) kopieren oder umgekehrt!

b) Manuelle FTP-Sitzung:

Aufruf:

```
ftp Servername
```

FTP-Befehle:

```
! delete literal prompt send ? debug ls put
status append dir mdelete pwd trace ascii
disconnect mdir quit type bell get mget quote
user binary glob mkdir recv verbose bye hash
mls remotehelp cd help mput rename close lcd
open rmdir
```

`dir`	remote Verzeichnis auflisten
`cd, lcd`	Verzeichnis wechseln, remote / local
`pwd`	aktuelles Verzeichnis
`get, mget`	Datei/en von remote nach local kopieren
`put, mput`	Datei/en von local nach remote kopieren
`binary`	auf binären Transfer (Programme, Images, ...) umschalten
`prompt`	Bestätigung abschalten
`user`	als Benutzer einloggen
`open, close`	Verbindung öffnen / schließen
`?`	Hilfe anzeigen
`quit, bye`	Programm beenden

Beispiel für eine manuelle FTP-Sitzung (Benutzereingaben sind fett dargestellt):

```
C:\WIN98>ftp off97.noe.wifi.at
Verbindung mit off97.noe.wifi.at.
220 wifi2 Microsoft FTP Service (Version 3.0).
Benutzer (off97.noe.wifi.at:(none)): user401
331 Password required for user401.
Kennwort:****
230-Herzlich Willkommen am Wifi Ftp-Server !
230 User user401 logged in.
Ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
d--------- 1 owner group 0 Aug 19 1999 kids
d--------- 1 owner group 0 Feb 17 1998 kktn
---------- 1 owner group 0 Aug 18 1999 test.txt
---------- 1 owner group 0 Aug 19 1999 test3.txt
226 Transfer complete.
Ftp: 269 Bytes empfangen in 0.16Sekunden 1.68KB/Sek.
Ftp> get test.txt
200 PORT command successful.
150 Opening ASCII mode data connection.
226 Transfer complete.
Ftp> put xxx.htm
200 PORT command successful.
150 Opening ASCII mode data connection for xxx.htm.
226 Transfer complete.
Ftp: 1777 Bytes gesendet in 0.00Sek 1777000.00KB/Sek.
Ftp> pwd
257 "/" is current directory.
Ftp> quit
221 Auf Wiedersehen !
```

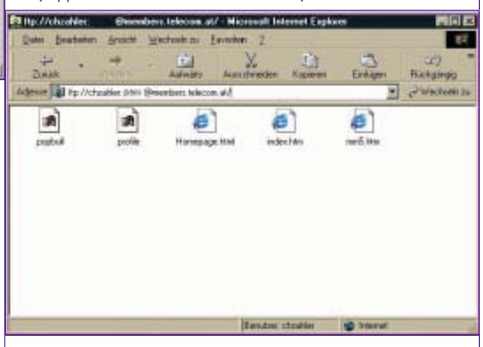
Wenn Sie als anonymer FTP-Nutzer arbeiten wollen, so geben Sie als Benutzername `anonymous` an, als Kennwort Ihre eigene `E-Mail-Adresse`. (Es ist kein Passwort nötig, allerdings verlangen die Regeln der Netiquette eine derartige – freiwillige! – Identifizierung.)

c) FTP über den Browser

Auch über Browser-Software ist eingeschränkter FTP-Betrieb möglich: Während Downloads problemlos möglich sind, können Uploads nicht durchgeführt werden!

Wichtig: Sollten Sie für den FTP-Server einen Benutzernamen und ein Kennwort eingeben müssen, dann wählen Sie bitte folgende Syntax für die Adresszeile des Browsers:

```
ftp://Benutzername:Kennwort@ftpserver.at
```



(Anmerkung: Das Passwort in der obigen Abbildung wurde abgedeckt bzw. verändert.)

6 Authentifizierung am IIS

Quelle: Windows 2000 Server-Hilfe

6.1 Anonyme Authentifizierung

Bei der anonymen Authentifizierung erhalten Benutzer Zugriff auf öffentliche Bereiche Ihrer Website oder FTP-Site, ohne dass sie einen Benutzernamen oder ein Kennwort eingeben müssen. Wenn ein Benutzer versucht, eine Verbindung zu Ihrer öffentlichen Website oder FTP-Site herzustellen, weist der Webserver dem Benutzer das Windows-Benutzerkonto `IUSR_Computername` zu, wobei Computername den Namen des Servers angibt, auf dem IIS ausgeführt wird.

Standardmäßig ist das Konto `IUSR_Computername` in der Windows-Benutzergruppe `Gäste` enthalten. Für diese Gruppe bestehen durch NTFS-Berechtigungen festgelegte Sicherheitsbegrenzungen. Durch diese Berechtigungen wird die Ebene des Zugriffs und die Art der Inhalte gekennzeichnet, die für öffentliche Benutzer verfügbar sind.

Befinden sich auf dem Server mehrere Sites oder sind für bestimmte Bereiche einer Site unterschiedliche Zugriffsrechte erforderlich, können Sie mehrere anonyme Konten, eines für jede Website bzw. FTP-Site, jedes Verzeichnis oder jede Datei einrichten. Indem Sie diesen Konten verschiedene Zugriffsberechtigungen erteilen oder indem Sie die Konten verschiedenen Windows-Benutzergruppen zuweisen, können Sie Benutzern den anonymen Zugriff auf verschiedene Bereiche der öffentlichen Web- und FTP-Inhalte ermöglichen.

IIS verwendet das Konto `IUSR_Computername` auf folgende Weise:

1. Das Konto `IUSR_Computername` wird zu der Gruppe Gäste auf dem Computer hinzugefügt.

2. Wird eine Anforderung empfangen, personalisiert IIS das Konto `IUSR_Computername`, bevor Code ausgeführt oder auf Dateien zugegriffen wird. IIS kann das Konto `IUSR_Computername` personalisieren, da der Benutzername und das Kennwort für dieses Konto bekannt sind.

3. Bevor eine Seite an den Client zurückgegeben wird, überprüft IIS die NTFS-Datei- und Verzeichnisberechtigungen, um festzustellen, ob dem Konto `IUSR_Computername` der Zugriff auf die Datei möglich ist.

4. Ist der Zugriff möglich, wird die Authentifizierung abgeschlossen, und die Ressourcen sind für den Benutzer verfügbar.

5. Ist der Zugriff nicht möglich, versucht IIS, eine andere Authentifizierungsmethode zu verwenden. Wenn keine Authentifizierungsmethode ausgewählt ist, gibt IIS die Fehlermeldung *"HTTP 403 Access Denied"* an den Browser zurück.

Anmerkung

- Ist die anonyme Authentifizierung aktiviert, versucht IIS immer zuerst, diese Methode zu verwenden, auch wenn andere Methoden aktiviert sind.
- In einigen Fällen wird der Benutzer vom Browser zur Eingabe eines Benutzernamens und eines Kennwortes aufgefordert.

Sie können das Konto, das für die anonyme Authentifizierung verwendet wird, im Snap-In für Internet Informationsdienste entweder auf der Webserver-Dienstebene oder für einzelne virtuelle Verzeichnisse und Dateien ändern. Das anonyme Konto muss über das Benutzerrecht für die ***lokale Anmeldung*** verfügen. Verfügt das Konto nicht über die Berechtigung **Lokale Anmeldung**, kann IIS keine anonymen Anforderungen verarbeiten. Die IIS-Installation erteilt speziell dem Konto `IUSR_Computername` die Berechtigung Lokale Anmeldung. Die `IUSR_Computername`-Konten auf Domänencontrollern werden nicht standardmäßig Gastkonten zugewiesen und müssen für die lokale Anmeldung geändert werden, um anonyme Anmeldungen zu ermöglichen.

Anmerkung: Sie können die Anforderungen bezüglich des Rechts **"Lokale Anmeldung"** ändern, indem Sie ADSI *(Active Directory Service Interfaces)* verwenden.

Sie können die Sicherheitsrechte für das Konto `IUSR_Computername` auch in Windows ändern, indem Sie das MMC-Snap-In ***Gruppenrichtlinien-Manager*** verwenden. Verfügt das anonyme Benutzerkonto jedoch nicht über die Zugriffsberechtigung für eine bestimmte Datei oder Ressource, stellt der Webserver keine anonyme Verbindung für diese Ressource her.

Wichtig: Wenn Sie das Konto `IUSR_Computername` ändern, wirken sich die Änderungen auf jede anonyme HTTP-Anforderung aus, die von einem Webserver verarbeitet wird. Gehen Sie äußerst sorgfältig vor, wenn Sie Änderungen an diesem Konto vornehmen.

6.2 Standardauthentifizierung

Bei der Methode der Standardauthentifizierung handelt es sich um eine weit verbreitete, Industriestandards entsprechende Methode des Abfragens von Informationen über Benutzernamen und Kennwörtern. Der Prozess der Standardauthentifizierung verläuft folgendermaßen:

1. Im Webbrowser des Benutzers wird ein Dialogfeld angezeigt, in dem dieser den Benutzernamen und das Kennwort für das ihm zuvor zugewiesene Windows 2000-Konto eingeben kann.

2. Der Webbrowser versucht anschließend, mithilfe dieser Informationen eine Verbindung herzustellen. (Das Kennwort wird mit einer Base64-Codierung versehen, bevor es über das Netzwerk gesendet wird.)

3. Weist der Server die Informationen zurück, wird im Webbrowser wiederholt das Dialogfeld angezeigt, bis der Benutzer einen gültigen Benutzernamen und ein Kennwort eingibt oder das Dialogfeld schließt.

4. Hat der Webserver sichergestellt, dass der Benutzername und das Kennwort einem gültigen Windows-Benutzerkonto entsprechen, wird eine Verbindung hergestellt.

Der Vorteil der Standardauthentifizierung besteht darin, dass diese Teil der HTTP-Spezifikation ist und von den meisten Browsern unterstützt wird. Nachteilig wirkt sich jedoch aus, dass Webbrowser, die die Standardauthentifizierung verwenden, Kennwörter in unverschlüsselter Form übertragen. Indem ein Benutzer die Kommunikation in Ihrem Netzwerk überwacht, kann dieser auf einfache Weise die Kennwörter mit öffentlich zugänglichen Tools abfangen und entschlüsseln. Aus diesem Grund wird die Standardauthentifizierung nur dann empfohlen, wenn Sie davon ausgehen können, dass die Verbindung zwischen dem Benutzer und Ihrem Webserver sicher ist (z. B., wenn es sich um eine direkte Kabelverbindung oder eine Standleitung handelt).

Anmerkung: Die integrierte Windows-Authentifizierung hat Vorrang vor der Standardauthentifizierung. Der Browser wählt die integrierte Windows-Authentifizierung und versucht, die aktuellen Windows-Anmeldeinformationen zu verwenden, bevor der Benutzer zur Eingabe eines Benutzernamens und Kennwortes aufgefordert wird. Derzeit unterstützt nur Internet Explorer, Version 2.0 und höher, die integrierte Windows-Authentifizierung.

6.3 Digestauthentifizierung

Ein neues Feature von IIS 5.0, die Digestauthentifizierung, weist grundsätzlich dieselben Merkmale wie die Standardauthentifizierung auf. Hierbei werden jedoch die Anmeldeinformationen für die Authentifizierung auf andere Weise übertragen. Die Anmeldeinformationen für die Authentifizierung durchlaufen einen nicht umkehrbaren Prozess, der häufig als Hashing bezeichnet wird. Das Resultat dieses Prozesses wird als Hash oder Nachrichtendigest bezeichnet und kann nicht entschlüsselt werden. Das heißt, der ursprüngliche Text kann nicht aus dem Hash ermittelt werden.

Der Prozess der Digestauthentifizierung verläuft folgendermaßen:

1. Der Server sendet an den Browser bestimmte Informationen, die während des Authentifizierungsvorgangs verwendet werden.

2. Der Browser fügt diese und einige weitere Informationen zu dem Benutzernamen und dem Kennwort hinzu und führt für diese ein Hashing durch. Die zusätzlichen Informationen dienen dazu zu verhindern, dass ein Benutzer den Hashwert kopiert und erneut verwendet.

3. Der sich hieraus ergebende Hash wird zusammen mit den zusätzlichen Informationen unverschlüsselt über das Netzwerk an den Server gesendet.

4. Anschließend fügt der Server die zusätzlichen Informationen zur Kopie des Clientkennwortes als unformatierter Text hinzu, über die er verfügt, und führt ein Hashing für alle Informationen durch.

5. Der Server vergleicht dann den empfangenen Hashwert mit dem von ihm erstellten.

6. Der Zugriff wird nur erteilt, wenn beide Zahlen absolut identisch sind.

Die zusätzlichen Informationen werden dem Kennwort vor dem Hashing hinzugefügt, so dass niemand den Kennworthash abfangen und verwenden kann, um die Identität des Clients anzunehmen. Werte werden hinzugefügt, mit denen der Client, der Computer des Clients sowie der Bereich bzw. die Domäne, zu der der Client gehört, ermittelt werden können. Darüber hinaus wird einen Zeitstempel hinzugefügt, um zu verhindern, dass ein Client ein Kennwort verwendet, nachdem dieses gesperrt wurde.

Hierbei handelt es sich um einen eindeutigen Vorteil gegenüber der Standardauthentifizierung, bei der das Kennwort abgefangen und von einem Unbefugten verwendet werden kann. Die Digestauthentifizierung ist so strukturiert, dass sie bei Proxyservern und anderen Firewallanwendungen verwendet werden kann, und ist für WebDAV *(Web Dis-*

tributed Authoring and Versioning) verfügbar. Da es sich bei der Digestauthentifizierung um ein neues HTTP 1.1-Feature handelt, wird sie nicht von allen Browsern unterstützt. Sendet ein nicht konformer Browser eine Anforderung an einen Server, der die Digestauthentifizierung erfordert, weist der Server die Anforderung zurück und sendet eine Fehlermeldung an den Client. Die Digestauthentifizierung wird nur für Domänen mit einem Windows 2000-Domänencontroller unterstützt.

Wichtig: Die Digestauthentifizierung kann nur durchgeführt werden, wenn der Domänenserver, an den eine Anforderung gesendet wird, über eine unformatierte Textkopie des Kennwortes von dem Benutzer verfügt, der die Anforderung sendet. Da der Domänencontroller über unformatierte Textkopien von Kennwörtern verfügt, muss er vor Zugriffen von Unbefugten geschützt werden, die direkt oder über das Netzwerk erfolgen können. Weitere Informationen über das Sichern eines Domänencontrollers finden Sie im Microsoft Windows 2000 Server Resource Kit.

Anmerkung: Ein Hashwert besteht aus einer kleinen Menge binärer Daten, normalerweise aus höchstens 160 Bit. Dieser Wert ergibt sich aus der Verwendung eines Hashingalgorithmus. Alle Hashwerte weisen unabhängig vom verwendeten Algorithmus die folgenden Eigenschaften auf:

- **Hashlänge**: Die Länge des Hashwerts wird durch die Art des verwendeten Algorithmus bestimmt und ist nicht vom Umfang der Nachricht abhängig. Es ist unerheblich, ob die Nachricht mehrere Kilobyte oder Gigabyte umfasst. Die üblichsten Hashwertlängen sind 128 und 160 Bit.
- **Nichtermittelbarkeit**: Für zwei Nachrichten, die nicht identisch sind, ergeben sich stets voneinander abweichende Hashwerte, auch wenn die Nachrichten sich nur durch ein Bit unterscheiden. Mithilfe der heutzutage verfügbaren Technologie ist es nicht möglich, zwei Nachrichten zu ermitteln, für die sich derselbe Hashwert ergibt.
- **Wiederholbarkeit**: Jedes Mal, wenn das Hashing für eine Nachricht mit demselben Algorithmus durchgeführt wird, ergibt sich derselbe Hashwert.
- **Irreversibilität**: Kein Hashingalgorithmus ist umkehrbar. Anhand eines Hashwerts kann nicht die ursprüngliche Nachricht wiederhergestellt werden, auch wenn der Hashingalgorithmus bekannt ist. Keine der Eigenschaften der ursprünglichen Nachricht kann nur anhand des Hashwerts ermittelt werden.

6.4 Integrierte Windows-Authentifizierung

Bei der integrierten Windows-Authentifizierung (die zuvor als NTLM oder Authentifizierung mittels der Windows NT-Herausforderung/Rückmeldung bezeichnet wurde) handelt es sich um eine sichere Form der Authentifizierung, da der Benutzername und das Kennwort nicht über das Netzwerk gesendet werden. Wenn Sie die integrierte Windows-Authentifizierung aktivieren, weist der Browser des Benutzers nach, dass er über die richtigen Kennwortinformationen verfügt, indem verschlüsselte Informationen mit dem Webserver ausgetauscht werden, wobei auch ein Hashing durchgeführt wird.

Bei der integrierten Windows-Authentifizierung kann sowohl das Authentifizierungsprotokoll Kerberos v5, als auch das systemeigene Authentifizierungsprotokoll für Herausforderung/Rückmeldung verwendet werden. Sind die Verzeichnisdienste auf dem Server installiert und ist der Browser kompatibel mit dem Authentifizierungsprotokoll Kerberos v5, wird sowohl das Protokoll Kerberos v5 als auch das Protokoll für Herausforderung/Rückmeldung verwendet. Andernfalls wird nur das Protokoll für Herausforderung/Rückmeldung verwendet.

Beim Authentifizierungsprotokoll Kerberos v5 handelt es sich um ein Feature der Architektur von Windows 2000 Distributed Services. Damit die Authentifizierung mit Kerberos v5 erfolgen kann, müssen Client und Server über vertraute Verbindungen zu einem KDC *(Key Distribution Center)* verfügen und mit den Verzeichnisdiensten kompatibel sein. Weitere Informationen über das Protokoll finden Sie in der Windows-Dokumentation.

Der Prozess der integrierten Windows-Authentifizierung verläuft folgendermaßen:

1. Anders als bei der Standardauthentifizierung wird der Benutzer nicht zunächst zur Eingabe eines Benutzernamens und eines Kennwortes aufgefordert. Für die integrierte Windows-Authentifizierung werden die aktuellen Windows-Benutzerinformationen auf dem Clientcomputer verwendet.

2. **Anmerkung**: Internet Explorer, Version 4.0 und höher, kann so konfiguriert werden, dass der Benutzer zunächst zur Eingabe des Benutzernamens und des Kennwortes aufgefordert wird, falls dies erforderlich ist. Weitere Informationen finden Sie in der Internet Explorer-Dokumentation.

Wenn der erste Versuch zur Identifizierung des Benutzers mittels Austausch von Authentifizierungsinformationen jedoch fehlschlägt, fordert der Browser den Benutzer auf, den Benutzernamen und das Kennwort eines Windows-Benutzerkontos einzugeben. Diese Angaben werden mit der integrierten Windows-Authentifizierung verarbeitet.

3. Der Benutzer wird so lange von Internet Explorer zur Angabe eines Benutzernamens und eines Kennwortes aufgefordert, bis ein gültiger Benutzername und ein gültiges Kennwort eingegeben oder das Dialogfeld geschlossen wird.

Obwohl die integrierte Windows-Authentifizierung sicher ist, weist sie zwei Einschränkungen auf.

1. Nur Microsoft Internet Explorer, Version 2.0 oder höher, unterstützt diese Authentifizierungsmethode.

2. Die integrierte Windows-Authentifizierung funktioniert nicht über HTTP-Proxyverbindungen.

Daher eignet sich die integrierte Windows-Authentifizierung am besten für eine Intranetumgebung, in der sich sowohl die Benutzercomputer als auch der Webservercomputer in derselben Domäne befinden und die Administratoren sicherstellen können, dass jeder Benutzer über Microsoft Internet Explorer, Version 2.0 oder höher, verfügt.

6.5 Zertifikatauthentifizierung

Sie können auch die SSL-Sicherheitsfeatures *(Secure Sockets Layer)* des Webservers für zwei Arten der Authentifizierung verwenden. Sie können ein Serverzertifikat verwenden, um Benutzern die Authentifizierung Ihrer Website zu ermöglichen, bevor sie persönliche Informationen, wie beispielsweise eine Kreditkartennummer, übertragen. Sie können außerdem Clientzertifikate zur Authentifizierung von Benutzern verwenden, die Informationen von Ihrer Website anfordern. SSL führt die Authentifizierung durch, indem der Inhalt einer verschlüsselten digitalen Identifizierung überprüft wird, die vom Webbrowser des Benutzers während des Anmeldevorgangs übergeben wird. (Benutzer erhalten Clientzertifikate von einer Organisation, die von beiden Seiten anerkannt wird.) Die Serverzertifikate enthalten in der Regel Informationen über Ihre Firma und die Organisation, die das Zertifikat ausgegeben hat. Die Clientzertifikate enthalten in der Regel Informationen, die den jeweiligen Benutzer und die Organisation identifizieren, die das Zertifikat ausgegeben hat.

Zuordnung von Clientzertifikaten

Sie können Clientzertifikate Windows-Benutzerkonten auf dem Webserver zuordnen. Nachdem Sie eine Zertifikatzuordnung erstellt und aktiviert haben, ordnet der Webserver einen Benutzer automatisch dem entsprechenden Windows-Benutzerkonto zu, sobald sich dieser Benutzer mit einem Clientzertifikat anmeldet. Auf diese Weise kann die Authentifizierung von Benutzern, die sich mit Clientzertifikaten anmelden, automatisch erfolgen, ohne dass hierzu die Verwendung der Standardauthentifizierung, der Digestauthentifizierung oder der integrierten Windows-Authentifizierung erforderlich ist. Sie können einem Windows-Benutzerkonto ein oder mehrere Clientzertifikate zuordnen. Wenn sich beispielsweise die Websites mehrerer verschiedener Abteilungen oder Unternehmen auf dem Server befinden, könnten Sie alle Clientzertifikate jeder Abteilung oder Firma der jeweiligen Website zuordnen. Auf diese Weise wäre nur den Clients einer Site der Zugriff auf diese möglich.

6.6 FTP-Authentifizierung

Anonyme FTP-Authentifizierung

Sie können den FTP-Server so konfigurieren, dass er den anonymen Zugriff auf FTP-Ressourcen zulässt. Ist die anonyme Authentifizierung aktiviert, versucht IIS immer zuerst, diese Methode zu verwenden, auch wenn die Standardauthentifizierung aktiviert ist. Wenn Sie die anonyme Authentifizierung für eine Ressource auswählen, werden alle Anforderungen für diese Ressource angenommen, ohne dass der Benutzer zur Eingabe eines Benutzernamens oder Kennwortes aufgefordert wird. Dies ist möglich, da IIS automatisch ein Windows-Benutzerkonto mit der Bezeichnung IUSR_Computername erstellt, wobei Computername den Namen des Servers angibt, auf dem IIS ausgeführt wird. Diese Art der Authentifizierung weist große Ähnlichkeit mit der webbasierten anonymen Authentifizierung auf.

FTP-Standardauthentifizierung

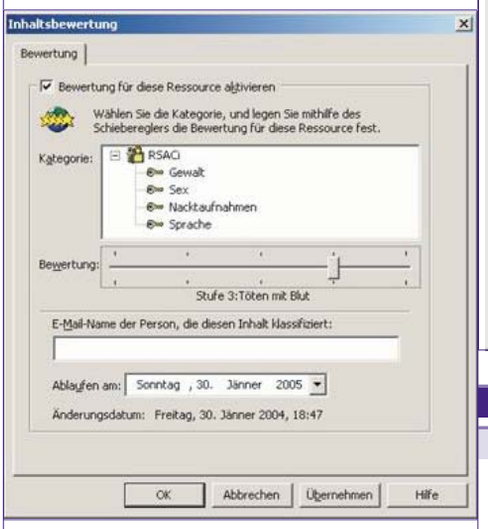
Zum Herstellen einer FTP-Verbindung zum Webserver mithilfe der Standardauthentifizierung müssen sich die Benutzer mit einem Benutzernamen und einen Kennwort anmelden, die zusammen einem gültigen Windows-Konto entsprechen. Wenn der FTP-Server die Identität eines Benutzers nicht über-

prüfen kann, gibt er eine Fehlermeldung zurück. Die FTP-Authentifizierung ist nicht besonders sicher, da die Benutzer das Kennwort und den Benutzernamen in unverschlüsselter Form über das Netzwerk übermitteln.

7 Schutz von Kindern und Jugendlichen durch RSACi-Filter und PICS-Labels

Quellen:

- www.w3.org/PICS
- www.rsac.org oder www.icra.org



RSACi = *Recreational Software Advisory Council for the Internet*

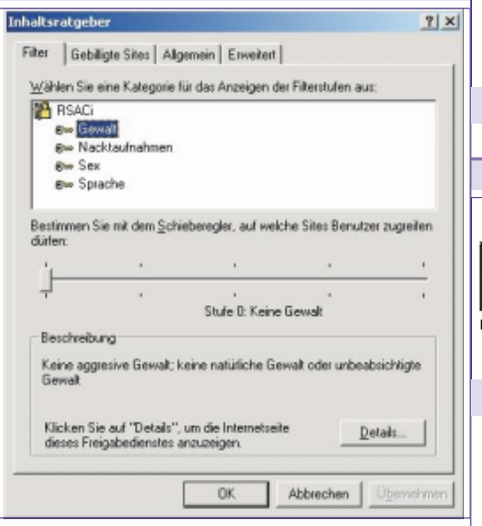
Das RSACi-System ist ein Filtersystem für jugendgefährdende Inhalte im Web, das von der ICRA *(Internet Content Rating Association)* verwaltet wird. Ziel dieses Systems ist die Gewährleistung der „Redefreiheit“ im Internet einerseits, der Schutz von Kindern und Jugendlichen vor gefährlichen oder anstößigen Inhalten andererseits.

Das RSACi-System ist im Internet Explorer integriert. Eltern können – gesichert durch ein Supervisor-Kennwort – den Level bestimmen, der angezeigt werden soll.

Für jeden RSACi-Label gibt es vier Sicherheitsstufen (siehe **Tabelle**):

Beispiel, wie man einen PICS-Label korrekt in ein HTML-Dokument einbettet:

```
<head>
<META http-equiv="PICS-Label"
content='(PICS-1.1 "http://www.gcf.org/v2.5"
labels on "1994.11.05T08:15-0500" until
"1995.12.31T23:59-0000" for
"http://w3.org/PICS/Overview.html" ratings
(suds 0.5 density 0 color/hue 1))'>
</head>
```



8 SSL und HTTPS

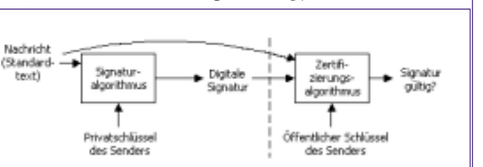
8.1 Grundlagen der Kryptographie

Die Sicherheit der Datenübertragung über das Internet lässt sich deutlich erhöhen, wenn die Dateien nicht im Klartext übertragen werden, sondern durch Verschlüsselungsalgorithmen unlesbar gemacht werden.

(Quelle: Microsoft Hilfe)

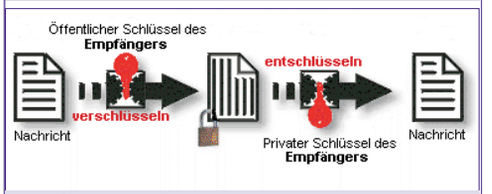
Man unterscheidet zwei Gruppen von Verschlüsselungsverfahren:

- **Symmetrische Verfahren**: Hier wird derselbe Schlüssel zur Ver- und Entschlüsselung verwendet.
- **Asymmetrische Verfahren:** Hier werden zwei verschiedene Schlüssel verwendet, ein „öffentlicher Schlüssel“ *(public key)* und ein „privater Schlüssel“ *(private key)*.



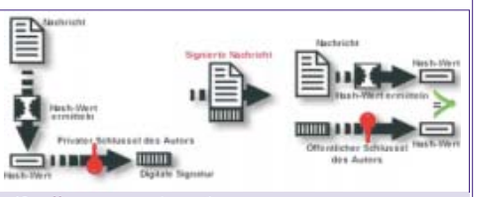
(Quelle: Microsoft Hilfe)

8.2 Verschlüsselung von E-Mails



(Quelle: www.a-sign.at)

Von einer Nachricht wird ein Hash-Wert ermittelt und mit dem Privaten Schlüssel des Autors verschlüsselt. Die Nachricht wird mit dieser Signatur übermittelt, der Empfänger kann mit dem Öffentlichen Schlüssel des Autors den Hash-Wert entschlüsseln. Der Empfänger generiert selbst den Hash-Wert der Nachricht und vergleicht diesen mit dem übermittelten Hash-Wert des Autors. Stimmen diese überein, ist die Nachricht vom Autor und unverändert.



(Quelle: www.a-sign.at)

8.3 Funktionsweise der Verschlüsselung

Die Verschlüsselung ist der Vorgang des "Zerstückelns" von Informationen, indem eine mathematische Funktion so angewendet wird, dass es äußerst schwierig für jeden anderen als den beabsichtigten Empfänger ist, die ursprünglichen Informationen wiederzugewinnen. Zentral bei diesem Vorgang ist ein eindeutiger mathematischer Wert, der Schlüssel genannt und von der Funktion dazu verwendet wird, die Informationen auf eindeutige und komplexe Weise zu zerstückeln.

Der Webserver verwendet im Wesentlichen denselben Verschlüsselungsvorgang, um Kommunikationsverbindungen zu Benutzern zu sichern. Nach dem Herstellen einer sicheren Verbindung wird ein bestimmter Sitzungsschlüssel vom Webserver wie vom Webbrowser des Benutzers verwendet, um die Informationen zu verschlüsseln und zu entschlüsseln. Wenn zum Beispiel ein authentifizierter Benutzer versucht, eine Datei von einer Website zu downloaden, die einen sicheren Channel erfordert, dann verwendet der Webserver einen Sitzungsschlüssel, um die Datei und die entsprechenden HTTP-Header zu verschlüsseln. Nach Empfang der verschlüsselten Datei verwendet dann der Webbrowser eine Kopie desselben

	Gewalt	Nacktheit	Sex	Sprache
Level 4	Vergewaltigungen oder willkürliche, brutale Gewaltakte	provozierende Nacktaufnahmen, von vorn fotografiert	Sexualverbrechen oder brutale, deutliche sexuelle Vorgänge	Rohe, vulgäre Sprache, freizügige sexuelle Anspielungen
Level 3	Aggressive Gewalt oder Töten von Menschen	Vollständige Nacktheit, von vorn fotografiert	Sexuelle Vorgänge	Deftige, vulgäre oder hasserfüllte Sprechweise; obszöne Kraftausdrücke
Level 2	Zerstörung realistischer Objekte	Teilweise Nacktheit	Sexuelle Berührungen im bekleideten Zustand	Kraftausdrücke; nicht sexuell bezogene anatomische Anspielungen
Level 1	Verletzen von Menschen	Aufreizende Bekleidung	Leidenschaftliche Küsse	Schwache Kraftausdrücke, milde Ausdrücke für Körperfunktionen
Level 0	Keine der obigen oder im Zusammenhang mit Sport	Keine der obigen	Keine der obigen oder “unschuldige” Küsse; Romantik	Keine der obigen

Sitzungsschlüssels, um die Datei wiederherzustellen.

Diese Verschlüsselungsmethode ist zwar sicher, enthält jedoch einen Nachteil: Während des Erstellens einer sicheren Verbindung wird eine Kopie des Sitzungsschlüssels möglicherweise über ein unsicheres Netzwerk übermittelt. Das bedeutet, dass ein unbefugter Benutzer, der beabsichtigt, die Verbindung auszuspionieren, nur den Sitzungsschlüssel abfangen und stehlen muss. Um sich gegen diese Möglichkeit abzusichern, implementiert der Webserver jedoch noch eine weitere Methode der Verschlüsselung.

8.4 Verschlüsselung über einen öffentlichen Schlüssel

Das Sicherheitsfeature *Secure Sockets Layer* (SSL) eines Webservers verwendet eine Technik, die als Verschlüsselung über einen öffentlichen Schlüssel bekannt ist und den Sitzungsschlüssel vor dem Abfangen während der Übertragung schützt. Diese Verschlüsselungsmethode verwendet zwei zusätzliche Schlüssel, einen privaten und einen öffentlichen Schlüssel, und funktioniert auf folgende Weise:

- Der Webbrowser des Benutzers stellt eine sichere Kommunikationsverbindung `https://` mit dem Webserver her.
- Der Webbrowser des Benutzers und der Server treten in "Verhandlungen" ein, um festzustellen, welcher Verschlüsselungsgrad für eine sichere Kommunikation verwendet werden soll.
- Der Webserver sendet seinen öffentlichen Schlüssel an den Browser.
- Der Webbrowser verschlüsselt die Informationen, die beim Generieren eines Sitzungsschlüssels verwendet werden, mit dem öffentlichen Schlüssel des Servers, und sendet diese an den Server.
- Mit dem privaten Schlüssel entschlüsselt der Server die Nachricht, generiert einen Sitzungsschlüssel, verschlüsselt diesen mit dem öffentlichen Schlüssel und sendet ihn an den Browser.
- Der Webserver und der Browser verwenden beide den Sitzungsschlüssel, um die übertragenen Daten zu verschlüsseln und zu entschlüsseln.

Beachten Sie, dass der private Schlüssel insofern eine wichtige Rolle ausübt, da er sicherstellt, dass eine Kommunikationsverbindung sicher bleibt. Sie sollten daher große Vorsicht walten lassen, um den privaten Schlüssel vor Verlust oder Diebstahl zu schützen. Sie können Ihr Zertifikat sichern, indem Sie dieses auf Diskette kopieren und an einem sicheren Ort aufbewahren. Wenn Sie den Verdacht haben, dass die Sicherheit Ihres privaten Schlüssels gefährdet ist, benachrichtigen Sie Ihre Zertifizierungsstelle, erstellen Sie über den Zertifikats-Assistenten eine neue Zertifikatanforderung, und beschaffen Sie sich ein neues Serverzertifikat.

Die Stärke des Sitzungsschlüssels

Die Stärke eines Sitzungsschlüssels ist proportional zur Anzahl der binären Bits, aus denen die Sitzungsschlüsseldatei besteht. Das bedeutet, dass Sitzungsschlüssel mit einer größeren Anzahl von Bits ein höheres Maß an Sicherheit bieten und beträchtlich schwerer von Außenstehenden zu dekodieren sind.

Wenn ein Benutzer versucht, einen sicheren Kommunikationschannel mit einem Webserver herzustellen, muss der Browser des Benutzers den stärkstmöglichen Grad an Verschlüsselung oder Stärke des Sitzungsschlüssels aushandeln, die zur Sicherung der Kommunikation über diesen Channel verwendet werden kann. Das bedeutet, dass der Webserver und der Benutzerbrowser mit kompatiblen Funktionen zur Verschlüsselung und Entschlüsselung des Sitzungsschlüssels ausgestattet sein müssen. Wenn Sie zum Beispiel Ihren Webserver so konfigurieren, dass ein Sitzungsschlüssel mit einer minimalen Verschlüsselungsstärke von 40 Bit verlangt wird, dann muss ein Benutzer, der eine Verbindung sicher zu machen versucht, einen Webbrowser verwenden, der in der Lage ist, Informationen mit einem 40 Bit langen Sitzungsschlüssel zu verarbeiten.

8.5 SSL

Secure Sockets Layer 3.0 ist ein Industriestandard-Protokoll, das die Authentifizierung von Rechnern und das Verschlüsseln von Daten für die Übertragung im Internet unterstützt. Es bietet ein sicheres Verfahren für das Einrichten eines verschlüsselten Kommunikationskanals.

IIS 5.0 unterstützt neben SSL 3.0 auch SSL 2.0. einer der Hauptunterschiede ist, dass die neuere Version die Möglichkeit von Client-Zertifikaten anbietet. Außerdem wird auch PCT 1.0 *(Private Communication Technology)* unterstützt.

SSL ist ein offenes, nicht proprietäres Protokoll und arbeitet auf der Basis von TCP/IP. Da es sich zwischen Transport und Anwendungen schiebt, müssen die existierenden Anwendungsprotokolle nicht geändert werden. SSL besteht dazu aus zwei Hauptkomponenten:

- SSL *Record Protocol*
- SSL *Handshake Protocol*

Das *Record Protocol* sitzt direkt oberhalb von TCP und kapselt die Daten ein, die aus den Anwendungen kommen und weitertransportiert werden sollen. Das *Handshake Protocol* koordiniert den Algorithmus.

Standardmäßig verwendet SSL allerdings nicht den Port 80 (TCP), sondern den Port 443.

8.6 Vorgehensweise

Die folgende Auflistung beschreibt die Vorgehensweise, wie eine gesicherte SSL-Sitzung zwischen Client und Server hergestellt werden kann:

- Der Client stellt eine Anfrage an den Server in der Form `https://...`
- Der Server erkennt die Anforderung einer gesicherten Ressource und sendet eine Kopie seines Zertifikats und seines öffentlichen Schlüssels an den Client.
- Im Folgenden wird der Grad der Verschlüsselung bestimmt, im Standardfall 40 oder 128 Bit.
- Der Client erzeugt einen so genannten Sitzungsschlüssel, der mit dem öffentlichen Schlüssel des Servers verschlüsselt und an den Server geschickt wird.
- Der Server entschlüsselt den Sitzungsschlüssel mit seinem privaten Schlüssel und richtet einen gesicherten Kommunikationskanal ein.
- Für die Verschlüsselung der zu übermittelnden Daten wird nun der Sitzungsschlüssel verwendet.

Viele Browser, unter anderem auch der Internet Explorer, zeigen bei Übertragungen dieser Art ein symbolisches Vorhängeschloss in den jeweiligen Statuszeilen und informieren auch per Dialogfenster, wann z.B. ein gesicherter Bereich wieder verlassen wird.

Genauere Beschreibung des Aufbaus einer SSLv3-Verbindung (mit Client- und Server-Authentifizierung):

Im ersten Schritt sendet der Client einen challenge string sowie weitere Informationen wie etwa den geplanten Schlüsselaustausch-Algorithmus (z.B. DES), den geplanten Hash-Algorithmus (MD5) usw. Der Server antwortet mit seinem Server-Zertifikat, der Bestätigung, daß die vorgeschlagenen Algorithmen unterstützt werden, und einem random connection identifier. Der Client überprüft das Server-Zertifikat und generiert einen *master session key*, der mit dem Öffentlichen Server-Schlüssel verschlüsselt und an den Server geschickt wird. Dieser *master session key* kontrolliert die Generierung der zwei bei SSL verwendeten symmetrischen Schlüsselpaare, und zwar des *client-read key* (identisch mit dem *server-write key*) und des *client-write key* (identisch mit dem *server-read key*). Der Client verschlüsselt den random connection identifier mit dem *server-write key*. Der Server entschlüsselt den *master session key* und generiert damit das entsprechende Server-Schlüsselpaar. Danach schickt er den mit dem *server-write key* verschlüsselten *challenge string* an den Client zurück. Der Server verlangt nun vom Client die Übermittlung eines Client-Zertifikates und schickt ihm eine neue, mit dem *server-write key* verschlüsselte *challenge phrase*. Der Client entschlüsselt die *challenge phrase* mit dem *client-read key* und bildet eine Antwortphrase, die aus dem Hash-Wert der *challenge phrase* und dem Server-Zertifikat besteht. Diese Antwortphrase wird gemeinsam mit dem Client-Zertifikat mit dem Privaten Schlüssel des Clients digital signiert und dem Server übermittelt. Der Server überprüft zunächst das Client-Zertifikat und anschließend die Antwortphrase durch Bilden der entsprechenden Hash-Werte. Abschließend übermittelt der Server dem Client einen eindeutigen, mit dem *server-write key* verschlüsselten *session identifier*, der in der verbleibenden Session verwendet wird. (Quelle: `www.a-sign.at`)

8.7 SGC

Ein 128-Bit-Sitzungsschlüssel kann aufgrund von Einschränkungen durch die amerikanische Regierung normalerweise nur in den USA verwendet werden und wurde in den Exportversionen nicht zur Verfügung gestellt.

Durch die Erweiterung von SSL um *Server Gated Cryptography* (SGC) wird der Einsatz dieser Technologie auch im Ausland möglich. Vor allem Banken und die Versicherungswirtschaft profitieren von dieser Entwicklung und können ihren Kunden beim Kontakt über das Internet damit fast hundertprozentige Sicherheit bieten.

SGC ist zwar in Windows 2000 bereits integriert. Für den endgültigen Einsatz ist aber ein spezielles SGC-Zertifikat erforderlich.

Auch dafür sind die oben erwähnten Zertifizierungsstellen zuständig.

8.8 RSA

Die Verschlüsselung selbst findet mit dem RSA-Algorithmus statt. RSA ist ein 1977 von **ivest**, **Shamir** und **Adleman** vorgestellter Algorithmus. Heute kümmert sich die RSA Date Security (www.rsa.com) um dieses Verschlüsselungsverfahren.

Microsoft Zertifikatsdienste Erstellen einer https-Site

Bei der Installation des Zertifikatsservers wird ein "Notar" installiert, der selbst Zertifikate ausstellen kann. Ein solcher "Notar" (Zertifizierungsinstanz, englisch *Certificate Agency*, CA) benötigt selbst nur ein sogenanntes Basiszertifikat. Solche Zertifikate gelten als "absolut vertrauenswürdig" und werden durch keine weitere Instanz bestätigt. Basiszertifikate haben international natürlich nur dann Gewicht, wenn die Organisation einen hohen Bekanntheitsgrad bzw. ein hohes Vertrauen des Publikums genießt.

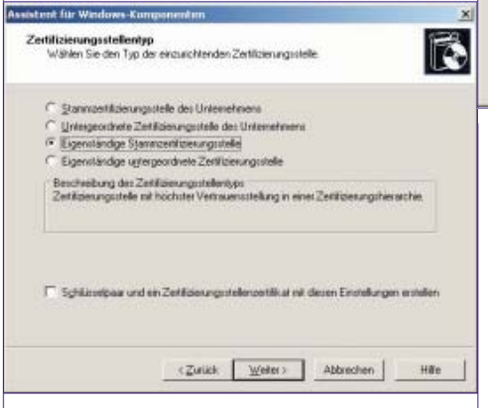
Der MS *Certificate Server* erzeugt Zertifikate im X.509-Format.

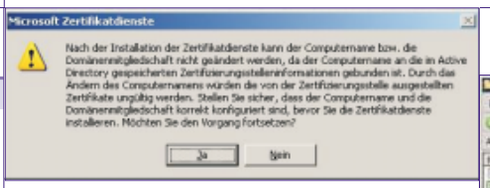
Möchte man eine Seite international gültig zertifizieren lassen, so gibt es dazu anerkannte Zertifizierungsinstitute:

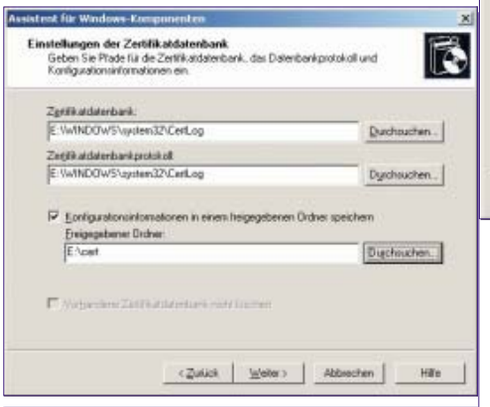
- http://www.verisign.com

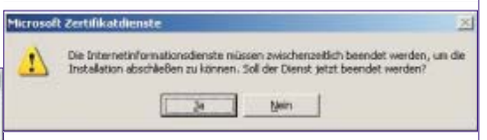
Der MS *Certificate Server* ist im Lieferumfang von **MS Windows 2003 Server** enthalten, wird aber standardmäßig nicht mitinstalliert. Er muss nachinstalliert werden, am einfachsten in der Systemsteuerung unter ***„Software"*** – Karteikarte ***„Windows-Komponenten hinzufügen/entfernen"***.

Hier ist die verwendete Windows 2003-Server-CD gemeint, die zur Systeminstallation verwendet wurde.(Es folgt noch ein Dialog, der zut Fertigstellung auffordert.)







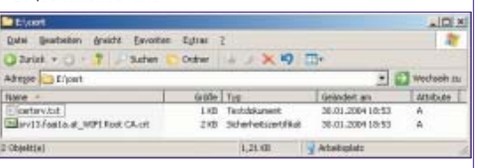


Ab jetzt ist es möglich, Schlüsselpaare zu erstellen, die vom eben installierten Zertifikatsserver "signiert" werden können.

Damit eine Zertifizierungsstelle ordnungsgemäß funktioniert, muss sie selbst ein **zertifikat** besitzen. Die oberste Zertifizierungsstelle stellt sich das Zertifikat selbst aus (**signiertes Zertifikat**). Das Eigenzertifikat wird im angegebenen Freigabeordner (hier: `C:\cert`) abgelegt:

Überprüfen der Schlüsselkonfiguration:

`E:\Dokumente und Einstellungen\Administrator>certutil -dump`



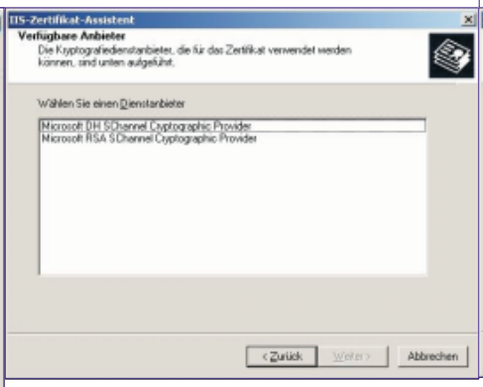

```
Einstellungen\Administrator>certutil -dump
Eintrag 0: ( okal)
 Name:  WIFI Root CA
 Organisationseinheit:
 Organisation:
 Stadt:
 Bundesland/Kanton:
  and/Region:
 Konfiguration:  srv13.faai1a.at\WIFI Root CA
 Exchange- ertifikat:
 Signaturzertifikat:  srv13.faai1a.at WIFI Root CA.crt
 Beschreibung:
 Server:  srv13.faai1a.at
 Stelle:  WIFI Root CA
 Sicherer Name:  WIFI Root CA
 Kurzname:  WIFI Root CA
 Sicherer Kurzname:  WIFI Root CA
 Flags:  15
CertUtil: -dump-Befehl wurde erfolgreich
ausgeführt.
```

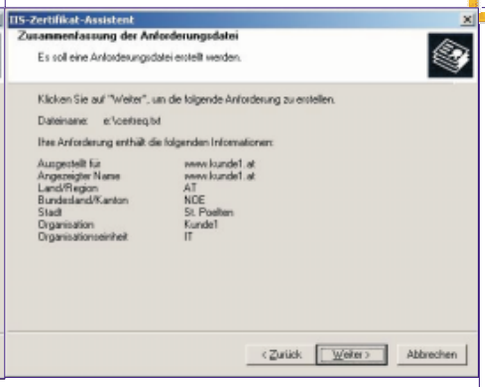
Erstellen eines „Serverzertifikats" (zertifizierten Schlüsselpaares) für die Website:

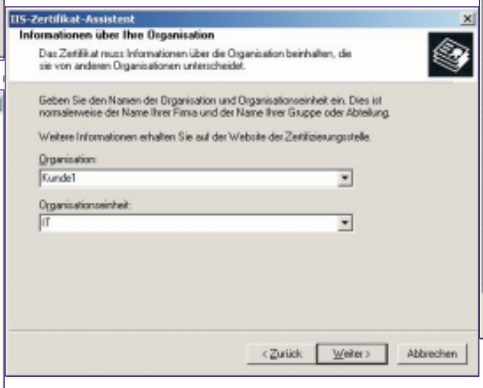
Der nächste Schritt ist die Erstellung eines eigenen Schlüsselpaares. Der Schlüssel muss natürlich von einer Zertifizierungsinstitution bestätigt werden. Wir könnten die Anforderung entweder an Verisign schicken oder von unserem eigenen Zertifizierungsserver bestätigen lassen.

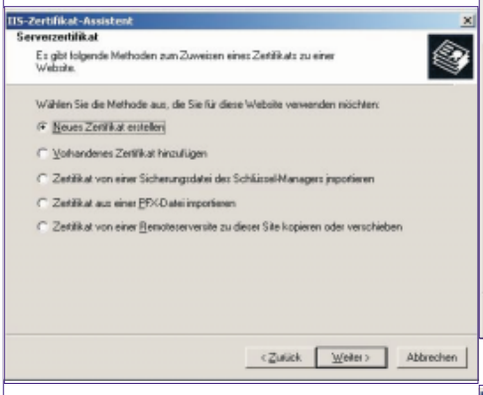
In Windows 2003 gibt es einen Assistenten zur Schlüsselerstellung, der über das Kontextmenü ***[Eigenschaften]*** der abzusichernden Website erreichbar ist.

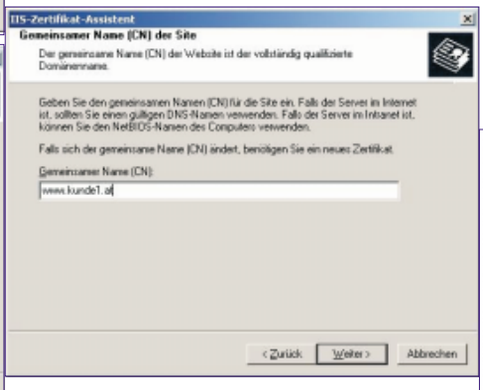
Klicken Sie auf die Schaltfläche ***„Serverzertifikat"***. (Screenfolge nächste Seite)





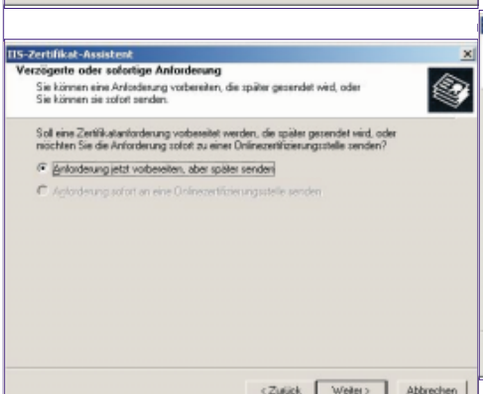


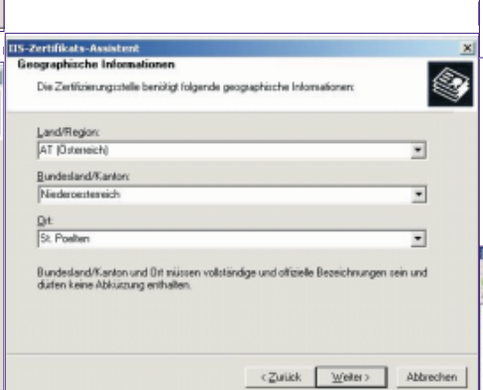




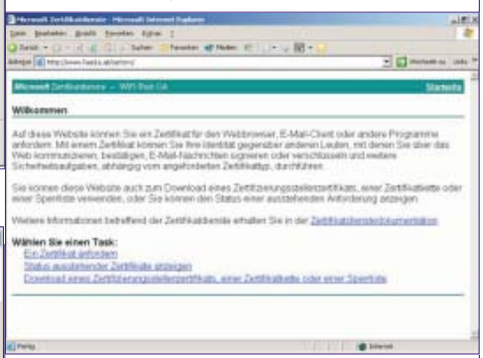
Wir haben nun folgende Situation: Es wurde ein Schlüsselpaar erstellt, das bereit zur Bestätigung der Zertifizierungsinstanz ist. Gleichzeitig wurde der Schlüssel in einer Zertifizierungsanforderungsdatei gespeichert, in unserem Fall `e:\certreq.txt`.

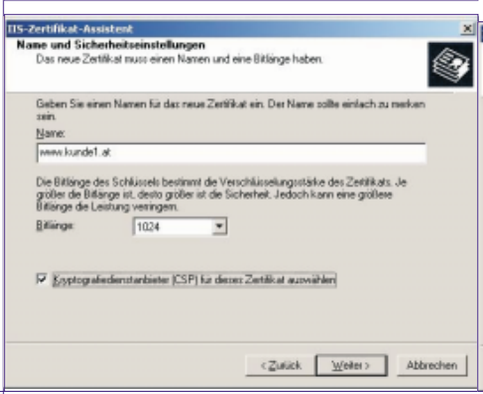
Diese Datei sieht folgendermaßen aus:

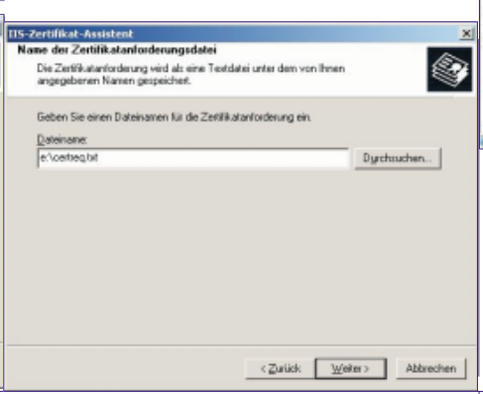




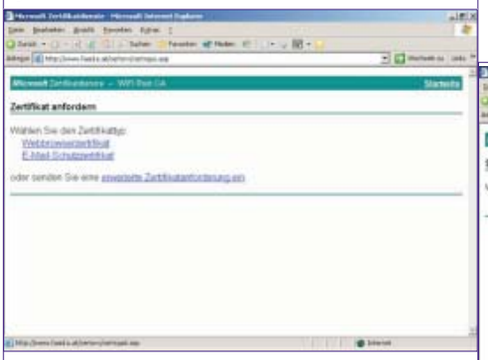
Als nächster Schritt wird die Anforderung an der Zertifikatsserver geschickt (wir verwenden den unseren eigenen), der eine Bestätigung (digitale Signatur) durchführen soll. Dafür gibt es vorinstallierte Hilfsprogramme, aufrufbar unter *http://Servername/certsrv*:



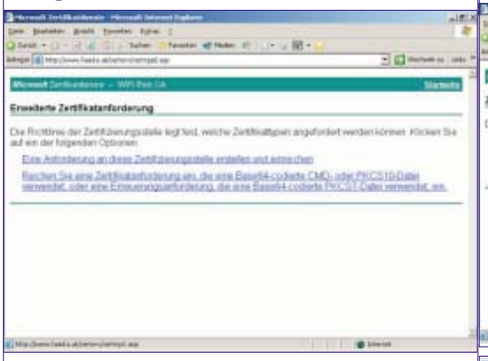




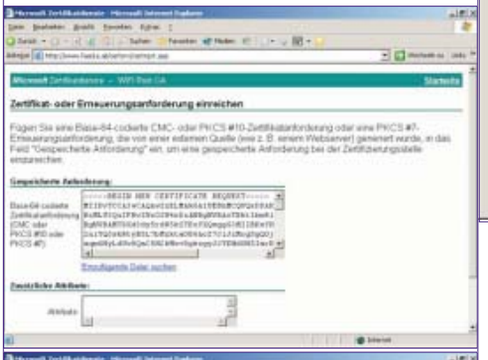
Klicken Sie zunächst auf ***„Ein Zertifikat anfordern“***.

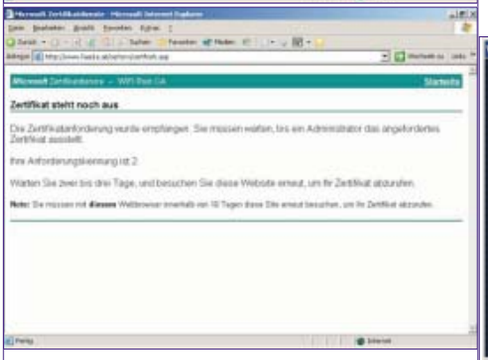


Nun auf ***„erweiterte Zertifikatsanforderung“***:

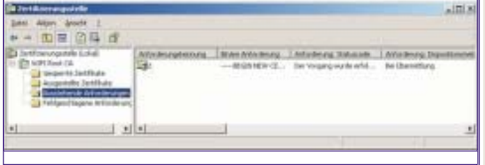


Klicken Sie auf ***„Reichen Sie eine Zertifikatsanforderung ein, die eine Base64-codierte Datei verwendet“*** und fügen Sie die Datei `CERTREQ.TXT` ein.

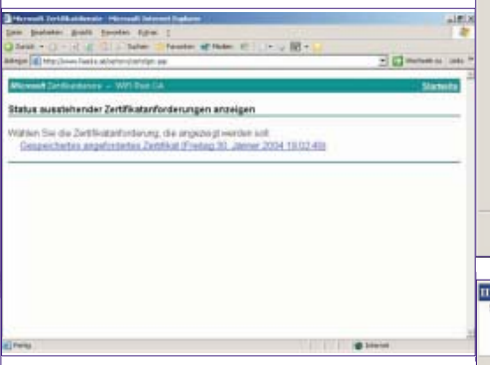


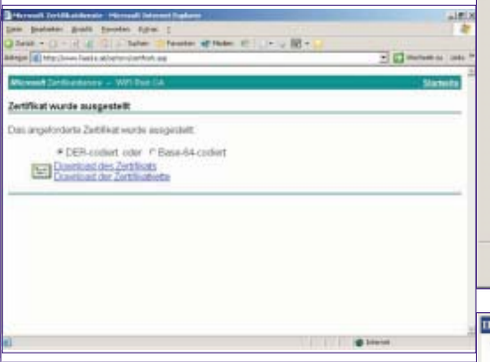


Nun muss die Zertifizierungsstelle die Anforderung bearbeiten. Im MMC-Snap-In ***„Zertifizierungsstelle“*** muss die ausstehende Anforderung erledigt werden:

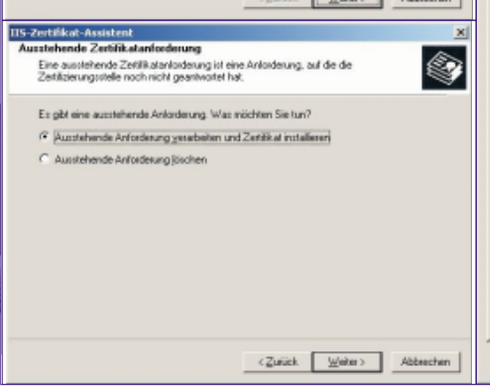


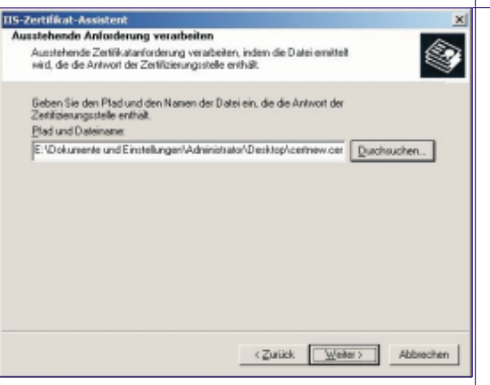
Besuchen Sie nochmals die Seite `http://Servername/certsrv` und klicken Sie nun auf ***„Status ausstehender Zertifikate anzeigen“***:

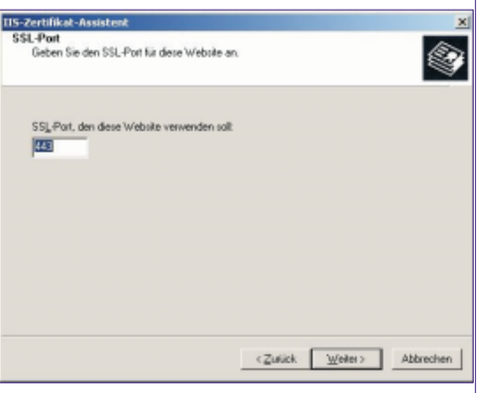


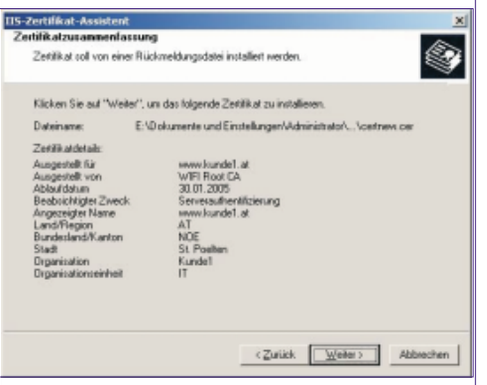


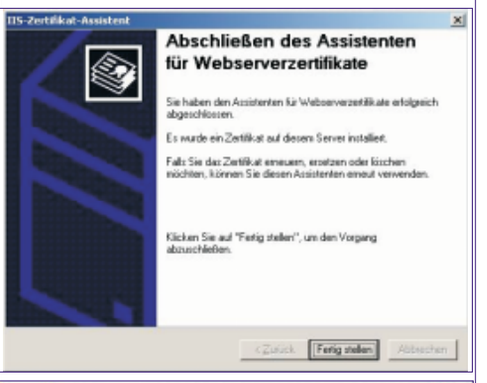
Nun geht es wieder zurück zu den Eigenschaften der Website: Wir rufen wieder die Karteikarte ***„Verzeichnissicherheit“*** auf und wählen zum zweiten Mal die Schaltfläche ***„Serverzertifikat“***.

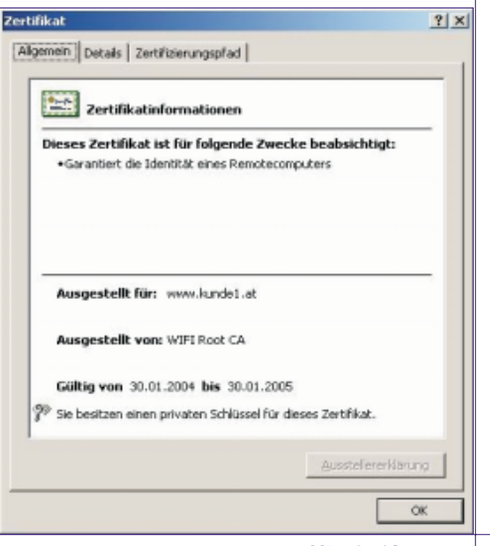


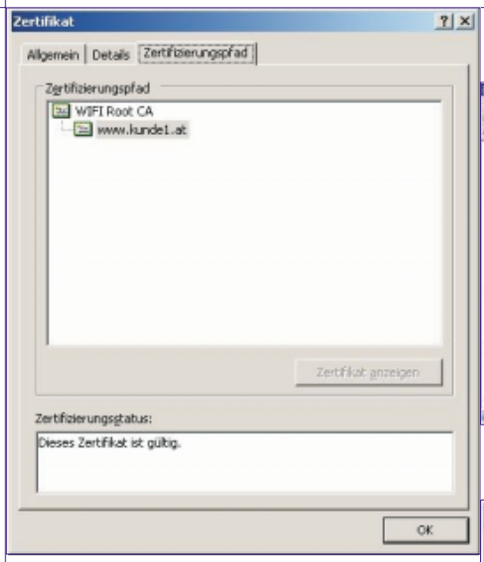




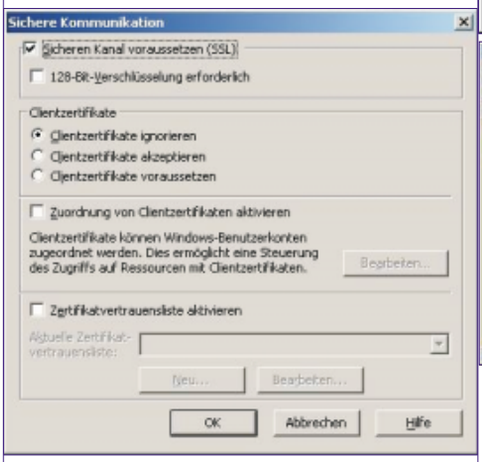




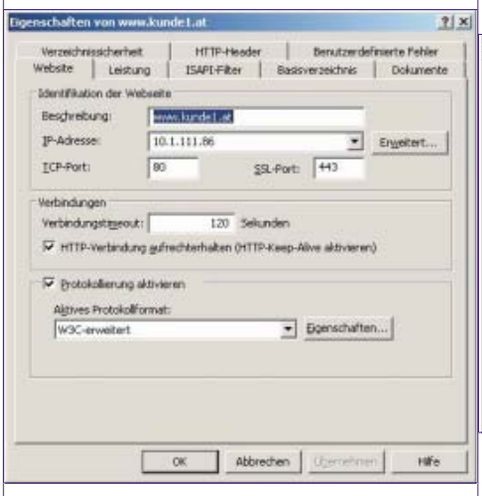




Klicken Sie nun in der Karteikarte ***"Verzeichnissicherheit"*** im Abschnitt ***"Sichere Kommunikation"*** auf die Schaltfläche ***"Bearbeiten..."*** und aktivieren Sie ***„Sicheren Kanal voraussetzen"***:



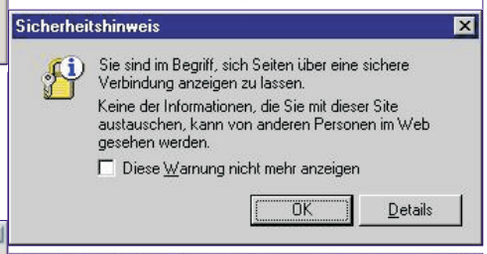
Überprüfen Sie noch einmal die TCP-Portnummer für die SSL-Kommunikation; üblicherweise wird 443 verwendet:



Tests

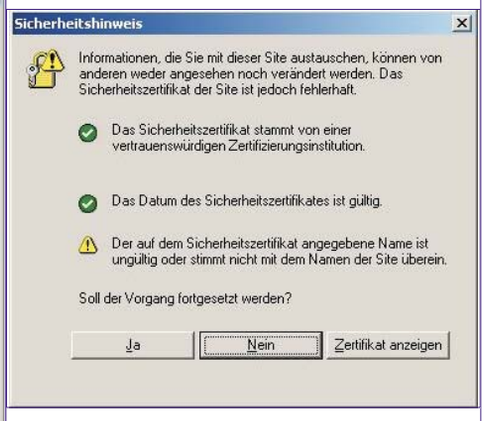
Eingabe von `http://.../ssltest.htm` schlägt fehl.

Erst durch das Protokoll `https://...` ist eine Anzeige der Datei möglich.



Weitere Versuche

Die Meldung `"Der auf dem Sicherheitszertifikat angegebene Name stimmt nicht mit dem Namen der Site überein"` weist darauf hin, dass die Angaben bei "Allgemeiner Name" nicht mit Namen bei DNS-Suchvorgang übereinstimmen.



Wiederholungsfragen

1. Welche Rolle spielen Berechtigungen bei der Einrichtung eines FTP- und WWW-Zugangs zu einem Webspace unter Win2003?
   - Auf NTFS-Ebene?
   - Auf Ebene des Internetdienstmanagers?
   - Welche Benutzer spielen dabei eine Rolle?
2. Welche Verzeichnisbegriffe gibt es beim IIS? erläutern Sie den grundlegenden Unterschied:
   - Basisverzeichnis
   - Physikalisches Verzeichnis
   - Virtuelles Verzeichnis

   Wie erstellt man virtuelle Verzeichnisse? Wie können Sie erreichen, dass virtuelle Verzeichnisse für den FTP-Benutzer "anklickbar" sind?
3. Welche Verwaltungsmöglichkeiten bietet der Internet-Dienstmanager (Win 2003) bezüglich WWW und FTP? Erläutern Sie dies an ausgewählten Registerkarten:
   - Basisverzeichnis
   - FTP-Site
   - Web-Site
   - Dokumente
4. Erläutern Sie in groben Schritten den Ablauf einer FTP-Sitzung mit

   Dem FTP-Client im Eingabefenster
   - FTP-Clients (WS-FTP, CuteFTP, LeechFTP,...)
   - dem MS Internet Explorer 6.x (bzw. 5.x)
5. Was bedeutet die Abkürzung RFC und welchen Stellenwert haben RFCs am Internet? Können Sie einen RFC namentlich nennen?
6. Was bewirken folgende administrative Handlungen?
   - Anhalten einer FTP-Site?
   - Beenden einer FTP-Site?
   - Beenden des IIS-Administrationsdienstes?
7. Nennen Sie einige Techniken im Umgang im IP-Adressen, die aus einem begrenzten Adressvorrat das Maximum herausholen und erläutern Sie diese kurz:
   - Subnetmask
   - DHCP-Server
8. Erklären Sie Absicht und Sinn von PICS-Labels (RSACi-FIltern)!
9. Was ist ein PKCS? Erläutern Sie asymmetrische Kryptographie-Verfahren an Hand von PGP und SSL!
10. Welche Schritte sind nötig, um eine Website mit SSL abzusichern?
11. Erläutern Sie die Begriffe "Server-Zertifikat" und "Basis-Zertifikat"!
12. Welche Eigenschaften hat der *MS Certificate Server*? Was ist nicht mehr möglich, wenn man diesen Server-Dienst installiert?
13. Welche drei Verfahren gibt es, um mehrere Webauftritte auf einem physischen IIS laufen zu lassen? (verschiedene IP; gleiche IP, verschiedener TCP-Anschluss; gleiche IP und TCP, verschiedener Hostheadername)
14. Wie erreichen Sie die Administrations-Website? Wodurch ist diese Site geschützt?
15. Was versteht man unter "MIME-Typen"? Erklären Sie die Anwendung der MIME-Typen beim E-Mail-Versand!