PEARSON Education

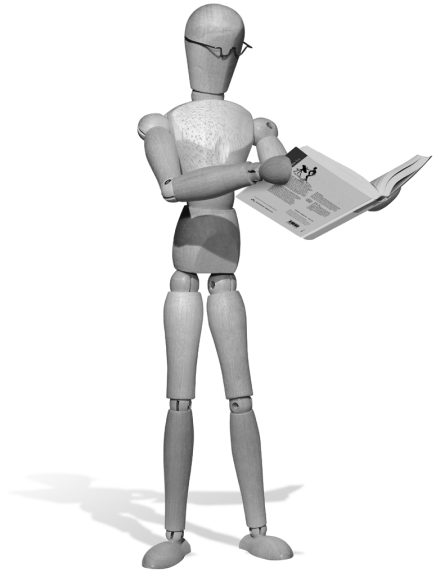
Kai Seidler, Kay Vogelgesang

ADDISON-WESLEY

open source library

Das XAMPP-Handbuch

Der offizielle Leitfaden zu Einsatz und Programmierung



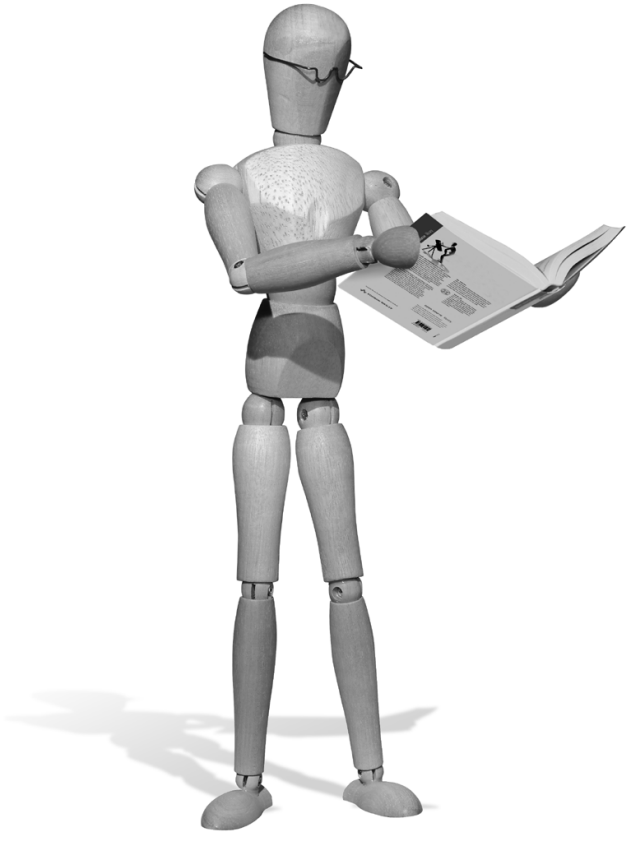
ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Teil II

Fortgeschrittene Benutzung von XAMPP



3 Apache

Seit der Version *XAMPP 1.5.1* mit *Apache HTTPD 2.2.0* ist die Konfiguration der `httpd.conf` in weitere Include-Dateien thematisch aufgeteilt. Zuvor war der Großteil der Konfiguration in der `httpd.conf` zu finden. Das hat sich seit der 2.2er-Version des Apache geändert.

Datei	Konfigurationsbereich	Verzeichnis
`httpd.conf`	Grundlegende Servereinstellung	`/opt/lampp/etc`
`httpd-autoindex.conf`	Index und Icons	`/opt/lampp/etc/extra`
`httpd-dav.conf`	WebDAV	`/opt/lampp/etc/extra`
`httpd-default.conf`	Standardeinstellungen	`/opt/lampp/etc/extra`
`httpd-info.conf`	Serverstatus und Info	`/opt/lampp/etc/extra`
`httpd-languages.conf`	Sprach-, Ländereinstellung	`/opt/lampp/etc/extra`
`httpd-manual.conf`	Apache-Manual-Konfiguration	`/opt/lampp/etc/extra`
`httpd-mpm.conf`	Server-Pool Management (MPM)	`/opt/lampp/etc/extra`
`httpd-multilang-errordoc.conf`	Mehrsprachige HTTP-Error-Dokumente definieren	`/opt/lampp/etc/extra`
`httpd-ssl.conf`	SSL/HTTPS-Konfiguration	`/opt/lampp/etc/extra`
`httpd-userdir.conf`	Standardisierte Benutzerpfade	`/opt/lampp/etc/extra`
`httpd-vhosts.conf`	Virtual Hosts einrichten	`/opt/lampp/etc/extra`
`httpd-xampp.conf`	XAMPP-spezifische Einstellungen	`/opt/lampp/etc/extra`

Tabelle 3.1: Apache-Konfigurationsdateien im XAMPP für Linux ab Version 1.5.1

Sie können diese Tabelle für *XAMPP für Windows* einfach gedanklich übertragen. Dabei ist der Linux-Pfad

```
/opt/lampp/etc/extra
```

gleich dem Windows-Pfad

```
<xampp>\apache\conf\extra
```

Hinweis

Die Inhalte vieler der hier vorgestellten »inkludierten« Konfigurationsdateien handeln von sehr spezifischen Einstellungen. Aus diesem Grund ist das Einlesen dieser Dateien in der `httpd.conf` oftmals auskommentiert.

3.1 Virtual Hosts

Ein physikalischer Rechner kann mehrere Virtual Hosts mit eigener Domain beherbergen. Sie kennen das sicherlich. Denn die meisten einschlägigen und preiswerten Hosting-Pakete bekannter Provider beruhen auf diesem Prinzip. Ein Server (d.h. Rechner) verwaltet viele Kunden, alle mit mindestens einer, wenn nicht sogar mehreren Domains. Alle Kunden besitzen für ihre Dokumente auf dem (einen) Server einen separaten Speicherplatz mit eigenem Login (meistens per FTP). Dort legt der Kunde die Webdokumente für den Auftritt seiner Domain ab. Doch wieso kann der Apache bei einer Anfrage eine Domain ihrem Stammverzeichnis richtig zuordnen, wenn er mehrere Domains verwaltet? Natürlich durch die Virtual Hosts. Bei den hier vorgestellten Virtual Hosts handelt es sich einzig um *HTTP*-Hosts für den Apache. Ein FTP-Server wie ProFTPD kann für sein Protokoll eigene Virtual Hosts bereitstellen, die nur beim FTP-Transfer wirken, nicht aber bei einer HTTP-Anfrage.

Prinzipiell unterscheidet der Apache-Webserver IP-basierte Virtual Hosts (*IP-based virtual hosts*) von namensbasierten Virtual Hosts (*name-based virtual hosts*). Beim IP-basierten Virtual Host besitzt jede Website ihre eigene IP-Adresse. Ein namensbasierter Virtual Host besitzt dagegen keine dedizierte, eigene IP-Adresse, sondern teilt sich eine IP-Adresse mit anderen Websites. D. h., mehrere Websites benutzen dieselbe IP-Adresse. Die Aufschlüsselung zu den verschiedenen Websites erledigt der Apache dann eigenständig. Der Trick: Ab HTTP/1.1 sendet der Client (meist der Browser) den Namen der gesuchten Website in dem HTTP-Host-Header mit.

Als Beispiel stellt dieses Kapitel die Einrichtung eines IP-basierten Virtual Hosts und die zweier namensbasierter Virtual Hosts für jeweils eine Website vor.

3.1.1 Namensauflösung

Die Auflösung des Domainnamens zu der IP-Adresse (*resolving*) wird häufig mit dem *Domain Name System* (DNS) in Verbindung gebracht. Tatsächlich stellen die öffentlichen DNS-Server das Rückrat der Auflösungsarbeit im Internet dar.

Die Übersetzung des Namens in die IP-Adresse kann für den Hausgebrauch, z.B. im privaten Intranet, auch über die `hosts`-Datei realisiert werden. Die Hosts finden Sie unter:

- Linux: `/etc/hosts`
- Windows NT/XP/2000: `C:\WINDOWS\system32\drivers\etc\hosts`
- Windows 95/98: `C:\WINDOWS\hosts`

Um dieses Beispiel nicht unnötig kompliziert zu machen, arbeiten wir hier mit der `hosts`-Datei. Für die Umsetzung der Auflösung über einen DNS-Server lesen Sie bitte Kapitel 25, »Der BIND-Nameserver«.

Ändern Sie Ihre `hosts`-Datei, indem Sie die folgenden Zeilen am Ende hinzufügen:

```
127.0.0.1       localhost1
127.0.0.2       localhost2 localhost3
```

Das war es. Und keine Angst, Ihr System funktioniert immer noch tadellos. Wir haben ja nur der *loopback*-Adresse drei Namen zugefügt: *localhost1*, *localhost2* und *localhost3*. Es sind zwar keine schönen Namen, aber sehr funktionale. Apropos: Das Funktionieren der neuen Namen können Sie mit *ping* gleich auf Ihrer Shell bzw. Eingabeaufforderung testen:

```
ping localhost1
ping localhost2
ping localhost3
```

3.1.2 httpd-vhosts.conf mit Virtual Hosts

Wie eingangs bereits erwähnt, wurden Teile der zuvor zentralen `httpd.conf` seit dem *Apache 2.2* in einzelne Konfigurationsdateien im Unterordner `extras` ausgelagert. Die für die Einstellung von Virtual Hosts vorgesehene Konfigurationsdatei heißt `httpd-vhosts.conf`.

- Linux: `/opt/lampp/etc/etxra/httpd-vhosts.conf`
- Windows: `<xampp>\apache\conf\extra\httpd-vhosts.conf`

Prüfen Sie unbedingt, ob in der `httpd.conf` die Datei `httpd-vhosts.conf` über die `Include`-Anweisung geladen wird, also ob dort die folgende Zeile steht und nicht auskommentiert ist:

```
Include conf/extra/httpd-vhosts.conf
```

Zu Beginn arbeiten Sie mit der Direktive *NameVirtualHost*. Mit dieser Anweisung definieren Sie, dass es sich bei der Adresse 127.0.0.2 um eine »Sammel-IP-Adresse« für namensbasierte Virtual Hosts handelt, also um Virtual Hosts, die sich anhand ihres Namens und nicht anhand ihrer IP-Adresse unterscheiden.

Danach folgen die VirtualHost-Container für *localhost1*, *localhost2* und *localhost3*. Die Anweisung *ServerName* im zweiten und dritten Container kennzeichnet dann den entsprechenden Domainnamen. Das Dokumentenverzeichnis wird schließlich über *DocumentRoot* definiert.

Für dieses Beispiel haben wir ein neues Verzeichnis namens `/opt/lampp/vhosts` bzw. `<xampp>\vhosts` mit den folgenden Unterverzeichnissen erstellt.

Unter Linux:

```
/opt/lampp/vhosts/localhost1/htdocs
/opt/lampp/vhosts/localhost1/logs
/opt/lampp/vhosts/localhost2/htdocs
/opt/lampp/vhosts/localhost2/logs
/opt/lampp/vhosts/localhost3/htdocs
/opt/lampp/vhosts/localhost3/logs
```

Unter Windows:

```
C:\Programme\XAMPP\vhosts\localhost1\htdocs
C:\Programme\XAMPP\vhosts\localhost1\logs
C:\Programme\XAMPP\vhosts\localhost2\htdocs
C:\Programme\XAMPP\vhosts\localhost2\logs
C:\Programme\XAMPP\vhosts\localhost3\htdocs
C:\Programme\XAMPP\vhosts\localhost3\logs
```

Wobei in den Unterverzeichnissen `htdocs` jeweils eine unterscheidbare Startseite (z.B. `index.html`) für die drei Virtual Hosts liegt.

	localhost1	**localhost2**	**localhost3**
IP-Adresse	`127.0.0.1`	`127.0.0.2`	`127.0.0.2`
DocumentRoot	`localhost1/htdocs/`	`localhost2/htdocs/`	`localhost3/htdocs/`
Log-Dateien	`localhost1/logs/`	`localhost2/logs/`	`localhost3/logs/`

Tabelle 3.2: Ordnerstruktur unter /opt/lampp/vhosts/ bzw. <xampp>\vhosts

Hinweis

Liebe Linux-Benutzer: Übersetzen Sie bitte das folgende Beispiel für Windows in das Linux-Verzeichnissystem. Liegt der XAMPP unter `C:\Programme\xampp`, heißt das für Sie also `/opt/lampp`.

Und liebe Windows-Benutzer: Für den Apache existiert unter Windows immer nur das Slashzeichen (/) zum Auszeichnen der Pfadstrukturen, also `C:/Programme/xampp` usw.

Tragen Sie diese Zeilen in die `httpd-vhosts.conf` ein:

Listing 3.1: Ein IP-basierter Virtual Host für localhost1 und zwei namensbasierte Virtual Hosts für localhost2 und localhost3

```
NameVirtualHost 127.0.0.2

<VirtualHost 127.0.0.1:80>
    ServerAdmin webmaster@localhost1
```

```
    DocumentRoot C:/Programme/xampp/vhosts/localhost1/htdocs
    ErrorLog  C:/Programme/xampp/vhosts/localhost1/logs/error_log
    CustomLog C:/Programme/xampp/vhosts/localhost1/logs/access_log common
</VirtualHost>

<VirtualHost 127.0.0.2:80>
    ServerAdmin webmaster@localhost2
    DocumentRoot C:/Programme/xampp/vhosts/localhost2/htdocs
    ServerName localhost2
    ErrorLog  C:/Programme/xampp/vhosts/localhost2/logs/error_log
    CustomLog C:/Programme/xampp/vhosts/localhost2/logs/access_log common
</VirtualHost>

<VirtualHost 127.0.0.2:80>
    ServerAdmin webmaster@localhost3
    DocumentRoot C:/Programme/xampp/vhosts/localhost3/htdocs
    ServerName localhost3
    ErrorLog  C:/Programme/xampp/vhosts/localhost3/logs/error_log
    CustomLog C:/Programme/xampp/vhosts/localhost3/logs/access_log common
</VirtualHost>
```

Achtung

Weitere Verzeichnis-Zugriffsrechte für XAMPP für Windows

Unter XAMPP für Windows müssen Sie dem Apache noch erlauben, neben dem normalen `htdocs`-Verzeichnis von XAMPP auch auf andere Verzeichnisse zugreifen zu dürfen. Ändern Sie dazu die Datei `<xampp>\apache\conf\httpd.conf` folgendermaßen:

Suchen Sie in der Datei die folgenden Zeilen:

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Order deny,allow
    Deny from all
</Directory>
```

Setzen Sie vor die letzten beiden Zeilen in diesem Directory-Container jeweils ein Doppelkreuz:

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
    #Order deny,allow
    #Deny from all
</Directory>
```

Das war's. Damit haben Sie ermöglicht, dass die Virtual Hosts auch außerhalb des normalen `htdocs`-Verzeichnis von XAMPP liegen dürfen.

Starten Sie den Apache neu. Danach kommt der obligatorische Test: Rufen Sie in Ihrem Browser *http://localhost1*, *http://localhost2* und *http://localhost3* nacheinander auf. Sie sollten nun jeweils die Startseite des jeweiligen Virtual Host sehen.

Aufgrund der Loopback-Adressen 127.0.0.1 und 127.0.0.2 funktioniert dieser Test selbstverständlich nur von dem Rechner aus, auf dem Ihr XAMPP installiert ist. Das Beispiel sollte nur zeigen, wie das Einrichten von Virtual Hosts funktioniert. Die Einrichtung von öffentlichen Virtual Hosts im Apache verlaufen aber alle nach diesem Prinzip.

Wenn Sie das Beispiel nicht mehr benötigen, löschen Sie es in der `httpd-vhosts.conf` oder kommentieren Sie das `Include` zur `httpd-vhosts.conf` in der `httpd.conf` einfach aus:

```
# Include conf/extra/httpd-vhosts.conf
```

3.2 Verzeichnisschutz mit .htaccess

Eine sekundäre Konfiguration über die Datei `.htaccess` erlaubt Ihnen, Einstellungen während des laufenden Betriebs des Apache und damit ohne den obligatorischen Neustart zu verändern. Über die `.htaccess` ist es somit möglich, weiteren nicht administrativen Benutzern die Möglichkeit einer beschränkten Konfiguration für ihr Dokumentenverzeichnis zu erlauben.

Eine typische Verwendung der `.htaccess`-Datei ist der Passwortschutz bestimmter Dateien oder Verzeichnisse. Hierbei dürfen nur über eine Passwort-Datei authentifizierte Benutzer in das geschützte Verzeichnis gelangen. Um neue Benutzer mit ihren Passwörtern anzulegen, benutzen Sie das Programm *htpasswd*:

- Linux: `/opt/lampp/bin/htpasswd`
- Windows: `<xampp>\apache\bin\htpasswd.exe`

1. Legen Sie ein Verzeichnis namens `test` in dem `htdocs`-Verzeichnis Ihrer XAMPP-Installation an.
2. Legen Sie in dieses Verzeichnis beispielhaft eine `index.html` mit einem beliebigen Inhalt. Greifen Sie danach testweise mit Ihrem Browser auf diese Datei über die URL *http://localhost/test/index.html* zu.
3. Nun erstellen Sie eine neue Passwort-Datei mit einem neuen Benutzer:

   Unter Linux:

   ```
   /opt/lampp/bin/htpasswd -c -b /opt/lampp/.htpasswd oswald geheim
   ```

   Unter Windows:

   ```
   C:\Programme\xampp\apache\bin\htpasswd -c -b
   C:\Programme\xampp\.htpasswd oswald geheim
   ```

4. Erstellen Sie eine Datei mit dem Namen `.htaccess` im Verzeichnis `test` und füllen Sie diese mit folgendem Inhalt:

Linux:

```
AuthUserFile /opt/lampp/.htpasswd
AuthName "Protected Area"
AuthType Basic
<Limit GET POST>
require valid-user
</Limit>
```

Windows:

```
AuthUserFile D:/Programme/xampp/.htpasswd
AuthName "Protected Area"
AuthType Basic
<Limit GET POST>
require valid-user
</Limit>
```

Sobald Sie die `.htaccess` geschrieben haben, ist der Passwortschutz für das Verzeichnis, in dem sich die Datei befindet, aktiv.

5. Geben Sie nun im Browser die URL des `test`-Verzeichnisses ein: *http://localhost/test/index.html*. Sollten Sie die URL noch von Schritt 2 geöffnet haben, dann drücken Sie auf die Aktualisieren-Schaltfläche Ihres Browsers.
   Ihnen wird nun vom Browser ein Login-Dialog angezeigt. Erst wenn Sie hier den Benutzernamen und das Passwort aus Schritt 4 angeben, können Sie auf das geschützte Verzeichnis zugreifen.

Wenn Sie später einen weiteren Benutzer hinzufügen möchten, dann tun Sie das mit dem folgenden Befehl:

Linux:

```
/opt/lampp/bin/htpasswd -b /opt/lampp/.htpasswd kay geheim2
```

Windows:

```
C:\Programme\xampp\apache\bin\htpasswd -b C:\Programme\xampp\.htpasswd kay geheim2
```

Um einen Benutzer zu löschen, verwenden Sie den folgenden Befehl:

Linux:

```
/opt/lampp/bin/htpasswd -D /opt/lampp/.htpasswd kay
```

Windows:

```
C:\Programme\xampp\apache\bin\htpasswd -D C:\Programme\xampp\.htpasswd kay
```

3.3 Eine Frage der Sicherheit: SSL

Verschlüsselte Datenübertragung über den *Secure Socket Layer* (*SSL*) kennen Sie bestimmt bereits als *HyperText Transfer Protocol Secure* (*HTTPS*). Zuständig dafür ist im Apache das Modul *mod_ssl*.

Bei XAMPP ist die SSL-Unterstützung standardmäßig aktiviert und mit einem einfachen selbstzertifizierten Serverzertifikat vorkonfiguriert. Rufen Sie einfach mal *https://localhost* in Ihrem Browser auf und greifen Sie so automatisch verschlüsselt auf ihren Webserver zu.

In den folgenden Tabellen erhalten Sie eine erste Übersicht der für SSL unter XAMPP wichtigsten Dateien und Verzeichnisse:

Name	Bedeutung	Ort
`openssl`	Kommandozeilenprogramm	`/opt/lampp/bin/`
`mod_ssl.so`	Apache-SSL-Modul	`/opt/lampp/modules/`
`openssl.cnf`	OpenSSL-Konfigurationsdatei (hier als symbolischer Link)	`/opt/lampp/etc/`
`httpd-ssl.conf`	Konfigurationsdatei für mod_ssl im Apache	`/opt/lampp/etc/extra/`
`ssl.crt`	Verzeichnis für alle Zertifikate (`*.crt`)	`/opt/lampp/etc/`
`ssl.key`	Verzeichnis für die Serverschlüssel (`*.key`)	`/opt/lampp/etc/`

Tabelle 3.3: Die wichtigsten Dateien und Verzeichnisse unter Linux

Name	Bedeutung	Ort
`openssl`	Kommandozeilenprogramm	`<xampp>\apache\bin\`
`mod_ssl.so`	Apache-OpenSSL-Modul	`<xampp>\apache\modules\`
`openssl.cnf`	OpenSSL-Konfigurationsdatei (hier als symbolischer Link)	`<xampp>\apache\bin\`
`httpd-ssl.conf`	Konfigurationsdatei für mod_ssl im Apache	`<xampp>\apache\conf\extra`
`ssl.crt`	Verzeichnis für Zertifikate (`*.crt`)	`<xampp>\apache\conf\`
`ssl.key`	Verzeichnis für die Serverschlüssel (`*.key`)	`<xampp>\apache\conf\`

Tabelle 3.4: Die wichtigsten Dateien und Verzeichnisse unter Windows

3.3.1 Ein selbstzertifiziertes Serverzertifikat erstellen

Ein selbstzertifiziertes Serverzertifikat dürfte die einfachste Form einer SSL-Konfiguration sein. Mit ihr erreichen Sie, dass die Daten, die zwischen dem Browser und Ihrer Website ausgetauscht werden, verschlüsselt übertragen werden.

Allerdings bekommen Sie bei jedem ersten Zugriff eine Warnung angezeigt, da die Echtheit des Zertifikats nicht automatisch überprüft werden kann. Letzteres würde bei einem CA-zertifizierten Serverzertifikat entfallen. Dazu mehr im nächsten Abschnitt.

1. Rufen Sie eine Root-Shell unter Linux oder die Eingabeaufforderung unter Windows auf und geben Sie die folgenden Befehle ein.

   Unter Linux:

   ```
   cd /opt/lampp/etc
   ```

   Unter Windows:

   ```
   cd C:\Programme\XAMPP\apache\conf
   set PATH=%PATH%;C:\Programme\XAMPP\apache\bin
   ```

   Mit dem `set PATH`-Befehl ersparen Sie sich das Tippen des langen Pfads vor dem `openssl`-Befehl.

2. Erstellen Sie nun einen Serverschlüssel (*server key*). Dieser Schlüssel besteht intern aus einem privaten und einem öffentlichen Teil und bildet später die Basis für die Verschlüsselung der Daten.
   Unter Linux:

   ```
   /opt/lampp/bin/openssl genrsa 1024 > ssl.key/server.key
   ```

   Unter Windows:

   ```
   openssl genrsa 1024 > ssl.key\server.key
   ```

3. Im nächsten Schritt zertifizieren Sie Ihren Serverschlüssel:
   Unter Linux:

   ```
   /opt/lampp/bin/openssl req -new -x509 -key ssl.key/server.key -out ↩
   ssl.crt/server.crt
   ```

   Unter Windows:

   ```
   openssl req -config c:\Programme\xampp\apache\bin\openssl.cnf -new -x509 -key ↩
   ssl.key\server.key -out ssl.crt\server.crt
   ```

4. Nach Aufruf dieses Kommandos werden Ihnen einige Fragen gestellt (die Eingaben wurden fett hervorgehoben):

   ```
   You are about to be asked to enter information that will be incorporated into ↩
   your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   ```

```
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:Berlin
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Apache Friends
Organizational Unit Name (eg, section) []:.
Common Name (eg, YOUR name) []:www.apachefriends.org
Email Address []:oswald@apachefriends.org
```

Wenn Sie ein Feld freilassen wollen, dann geben Sie einfach nur einen Punkt ein. Wichtig ist der leider sehr missverständliche Begriff »Common Name«: Hier geben Sie die Adresse Ihrer Website ein.

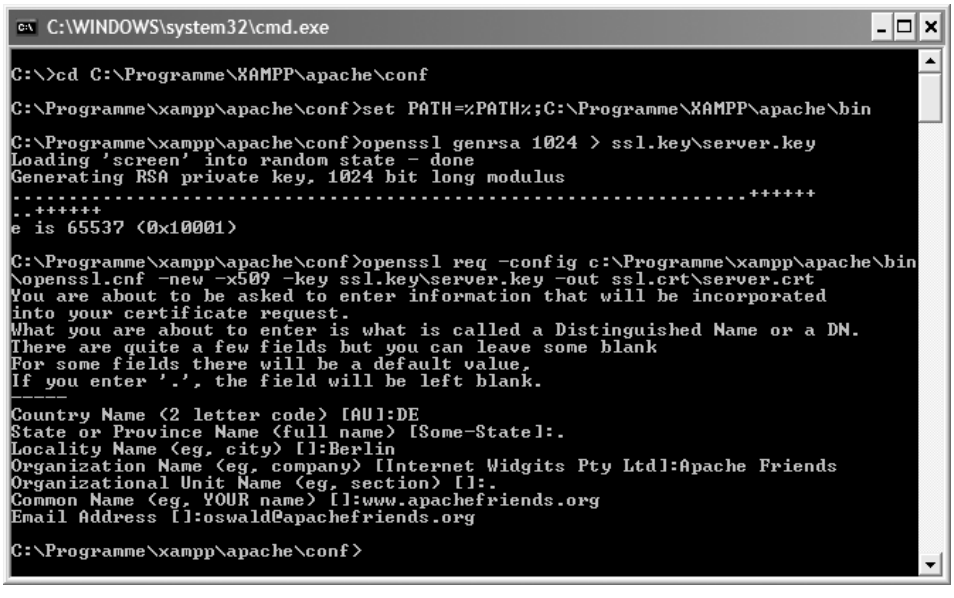


Abbildung 3.1: Die Erstellung eines selbstzertifizierten Zertifikats samt Erstellung eines neuen Serverschlüssels passt locker auf eine Bildschirmseite (Screenshot von Windows XP).

5. Starten Sie nun den Apache neu, damit er seinen neuen Schlüssel und sein neues Zertifikat lädt.
6. Zum Testen Ihres neuen Zertifikats greifen Sie mit *https://localhost* auf Ihren Webserver zu.

Abbildung 3.2: Der Nachteil eines selbstzertifizierten Zertifikats: Die Echtheit kann vom Browser nicht automatisch festgestellt werden.

3.3.2 Ein CA-zertifiziertes Serverzertifikat erstellen

In der Regel kommt für den Produktiveinsatz ein kostenpflichtiges Zertifikat einer offiziellen Zertifizierungsstelle (*Certification Authority, CA*) zum Einsatz. Für dieses Beispiel beziehen wir ein Zertifikat der Klasse 0 (kostenfreies Testzertifikat) von dem Anbieter *TrustCenter* (*http://www.trustcenter.de*).

1. Rufen Sie eine Root-Shell unter Linux oder die Eingabeaufforderung unter Windows auf und geben Sie die folgenden Befehle ein.

   Unter Linux:

   ```
   cd /opt/lampp/etc
   ```

   Unter Windows:

   ```
   cd C:\Programme\XAMPP\apache\conf
   set PATH=%PATH%;C:\Programme\XAMPP\apache\bin
   ```

   Mit dem `set PATH`-Befehl ersparen Sie sich das Tippen des langen Pfads vor dem `openssl`-Befehl.

2. Erstellen Sie nun einen Serverschlüssel (*server key*). Dieser Schlüssel besteht intern aus einem privaten und einem öffentlichen Teil und bildet später die Basis für die Verschlüsselung der Daten.

Unter Linux:

```
/opt/lampp/bin/openssl genrsa 1024 > ssl.key/server.key
```

Unter Windows:

```
openssl genrsa 1024 > ssl.key\server.key
```

3. Im nächsten Schritt erstellen Sie Ihren *Certificate Signing Request* (*CSR)*:
   Unter Linux:

   ```
   /opt/lampp/bin/openssl req -new -key ssl.key/server.key -out server.csr
   ```

   Unter Windows:

   ```
   openssl req -config c:\Programme\xampp\apache\bin\openssl.cnf -new -key ↵
   ssl.key\server.key -out server.csr
   ```

4. Nach Aufruf dieses Kommandos werden Ihnen einige Fragen gestellt (die Eingaben wurden fett hervorgehoben). Wenn Sie ein Feld freilassen wollen, dann geben Sie einfach nur einen Punkt ein. Wichtig ist der leider sehr missverständliche Begriff »Common Name«: Hier geben Sie die Adresse Ihrer Website ein.

   ```
   You are about to be asked to enter information that will be incorporated into ↵
   your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [AU]:DE
   State or Province Name (full name) [Some-State]:.
   Locality Name (eg, city) []:Berlin
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Apache Friends
   Organizational Unit Name (eg, section) []:.
   Common Name (eg, YOUR name) []:www.apachefriends.org
   Email Address []:oswald@apachefriends.org
   ```

5. Nun werden Sie noch nach einem *challenge password* und einem *optional company name* gefragt. Geben Sie in beiden Fällen nichts ein und drücken Sie die Enter-Taste:

   ```
   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []:
   An optional company name []:
   ```

   Durch den letzten Befehl wurde die Datei `server.csr` im aktuellen Verzeichnis erstellt.

6. Öffnen Sie die Datei mit einem Texteditor Ihrer Wahl. Sie sollten etwa folgenden Inhalt sehen:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBwTCCASoCAQAwgYAxCzAJBgNVBAYTAkRFMQ8wDQYDVQQHEwZCZXJsaW4xFzAV
BgNVBAoTDkFwYWNoZSBGcmllbmRzMR4wHAYDVQQDExV3d3cuYXBhY2hlZnJpZW5k
cy5vcmcxJzAlBgkqhkiG9w0BCQEWGG9zd2FsZEBhcGFjaGVmcmllbmRzLm9yZzCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxTYX6OMgDjBt4szR+2poolTKAzBL
/BWAUkS7UvHRPNTGp9nJJwnKlwWmkhmewhmArz1nO32UKwc4ZrWWsivpK4rZOCVl
GvyNcQp8UzrnEOHLSeQOj52blzvQM/mOIJacK/TsCy6hvurr2ki9cIOQhpVW1xoc
cuP7qNY3b9ubGGkCAwEAAaAAMAOGCSqGSIb3DQEBBQUAA4GBAIGZmPRxfMnVSC5a
J/HlQnxy2ZAjcRV9bJvqIWbVRl0u9gzlIClw1e9IOnToCekcPRhbbg+lvybcZeXI
5qv/PVnMZFLnLa81SOLYv7xNiAnObr7q+LGOzzpareg04dGEg3wBLVBZJD9DeeFs
ytcEVnWIsU2BBwV7l3tACHa/6eoT
-----END CERTIFICATE REQUEST-----
```

7. Übermitteln Sie diesen Inhalt an Ihre Zertifizierungsstelle. In der Regel hat diese ein Webformular, über das Sie die CSR mit Copy&Paste eingeben können.
   Die Zertifizierungsstelle wird Ihre Daten überprüfen und bei positiver Prüfung erhalten Sie per E-Mail oder per Web Ihr tatsächliches Serverzertifikat.

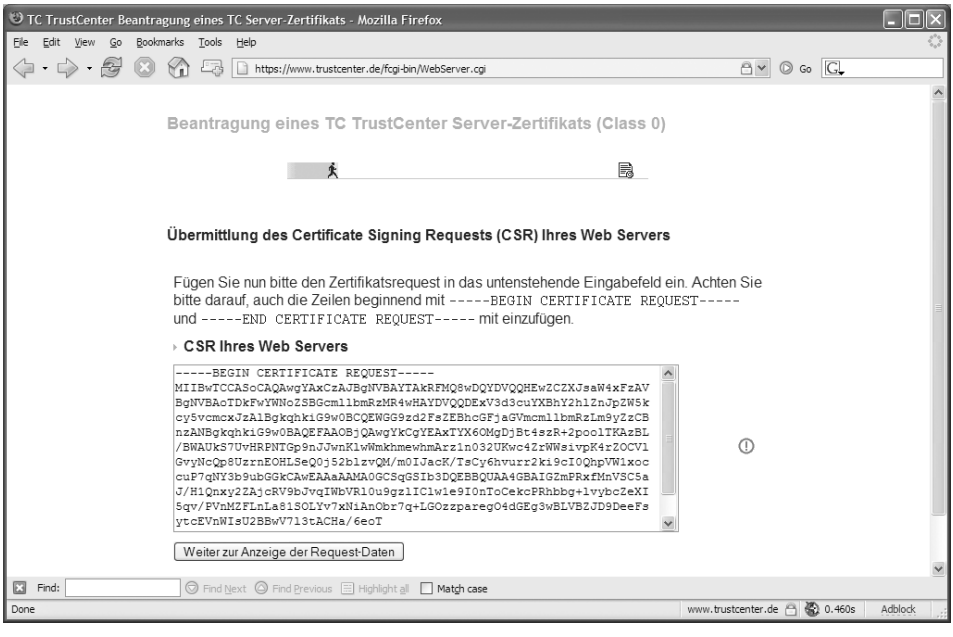


Abbildung 3.3: Übermitten Sie Ihr CSR an Ihre Zertifizierungsstelle. Von ihr erhalten Sie dann das Serverzertifikat.

8. Wenn Sie das Serverzertifikat der CA erhalten haben, tragen Sie es in die Datei `server.crt` ein. Starten Sie Ihren Apache neu und greifen Sie danach über HTTPS auf Ihren Webserver zu.

   Wenn alles richtig gelaufen ist, dann kann der Browser nun automatisch die Echtheit des Zertifikats überprüfen und zeigt Ihnen keine Warnung wie bei dem selbstzertifizierten Zertifikat an.

Achtung

Wenn Sie nur ein Testzertifikat einer CA verwenden, dann wird auch in diesem Fall eine Warnung angezeigt. Die Warnung verschwindet wirklich erst dann, wenn Sie ein richtiges Zertifikat erworben haben.

3.4 WebDAV

Das *WebDAV*-Protokoll (*DAV = Distributed Authoring and Versioning*) ermöglicht Benutzern, über passwortgeschützte Verzeichnisse Dokumente direkt am Zielserver zu verändern. In der Praxis ist WebDAV mit den Programmen *Dreamweaver* und *Adobe GoLive* zu einer gewissen Bekanntheit gekommen. Aber auch *Netzwerklaufwerke* können über WebDAV freigegeben werden.

Zwei Authentifikationsmethoden sind im Apache HTTPD erlaubt:

3.4.1 Digest

Hierbei werden die Passwörter über einen speziellen Algorithmus mit dem Programm *htdigest* generiert. Beispiele dazu:

Apache-Direktive: `AuthType Digest`

Nachteil: `AuthType Digest` wird von *Dreamweaver MX* als Client **nicht unterstützt**!

3.4.2 Basic

Ein bekannter Algorithmus, der auch schon bei dem Beispiel des Verzeichnisschutzes mit einer `.htaccess` Verwendung fand.

Apache-Direktive: `AuthType Basic`

3.4.3 XAMPP-Spezifika

In XAMPP ist die WebDAV-Unterstützung bereits standardmäßig aktiviert. Sie müssen selbst nur noch eine Passwort-Datei über das Apache-Programm *htpasswd* erstellen. In diesen XAMPP-Versionen ist `AuthType Basic` die Standardmethode der Authentifizierung. Die WebDAV-Verzeichnisse im XAMPP lauten unter

Linux: `/opt/lampp/webdav`

Windows: `<xampp>\webdav`

Um in den älteren XAMPP-Versionen die WebDAV-Unterstützung des Apache in der `httpd.conf` zu aktivieren, kommentieren Sie die folgenden Zeilen aus:

```
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule setenvif_module modules/mod_setenvif.so
```

Überprüfen Sie ebenfalls in der `httpd.conf`, ob die `httpd-dav.conf` hier bereits geladen ist.

```
Include conf/extra/httpd-dav.conf
```

Alles Weitere passiert nun in der `httpd-dav.conf`:

Linux: `/opt/lampp/etc/etxra/httpd-dav.conf`

Windows: `<xampp>\apache\conf\extra\httpd-dav.conf`

3.4.4 Die Beispielkonfiguration im XAMPP für Linux

Bei älteren XAMPP-Versionen müssen Sie vielleicht das Beispiel selbst erstellen. Hierfür müssen Sie zu Beginn als `su` noch zwei wichtige Schritte vollziehen:

1. Erstellen Sie ein WebDAV-Verzeichnis und setzen Sie Benutzerrechte.

   ```
   mkdir /opt/lampp/webdav
   chown -R nobody.root /opt/lampp/webdav
   ```

2. Erstellen Sie eine Passwort-Datei mit `htpasswd`.

   ```
   /opt/lampp/bin/htpasswd -c -b /opt/lampp/htpasswd.webdav username secret
   ```

3. Passen Sie die `httpd-dav.conf` an.
   Ihre Konfiguration der `httpd-dav.conf` könnte wie folgt aussehen:

   ```
   <IfModule dav_module>
   <IfModule dav_fs_module>
   <IfModule setenvif_module>
   <IfModule authn_file_module>
   ```

```
DavLockDB "/tmp/DavLock"
Alias  /webdav "/opt/lampp/webdav"

<Directory  "/opt/lampp/webdav">
    Dav On
    Order  allow,deny
    Allow from all
    AuthName "XAMPP with WebDAV"
    AuthType Basic
    AuthUserFile "/opt/lampp/htpasswd.webdav"

       <LimitExcept GET HEAD OPTIONS>
        require valid-user
       </LimitExcept>
</Directory>
BrowserMatch "Microsoft Data Access Internet Publishing Provider" ↩
redirect-carefully
BrowserMatch "MS FrontPage" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
BrowserMatch "^gnome-vfs/1.0" redirect-carefully
BrowserMatch "^XML Spy" redirect-carefully
BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully
BrowserMatch "MSIE" AuthDigestEnableQueryStringHack=On
</IfModule>
</IfModule>
</IfModule>
</IfModule>
```

4. Starten Sie den Apache neu.

Ihre WebDAV-Konfiguration in der Übersicht:

Verzeichnis	**/opt/lampp/webdav**
URL	`http://localhost/webdav`
Benutzer	`[von Ihnen gewählt]`
Passwort	`[von Ihnen gewählt]`
Passwort-Datei (mit *htpasswd*)	`/opt/lampp/htpasswd.webdav`

3.4.5 Die Beispielkonfiguration im XAMPP für Windows

Der XAMPP liegt in diesem Beispiel erneut unter `C:\Programme` vor. Für alle älteren XAMPP-Versionen haben Sie, wie eben unter Linux beschrieben, alle notwendigen Apache-Module geladen und die `httpd-dav.conf` in der `httpd.conf` aktiviert.

1. Erstellen Sie eine Passwort-Datei mit *htpasswd*.

```
C:\Programme\xampp\apache\bin\htpasswd -c ↵
C:\Programme\xampp\security\htpasswd.webdav username
```

2. Passen Sie die `httpd-dav.conf` an.

```
<IfModule  dav_module>
<IfModule dav_fs_module>
<IfModule setenvif_module>
<IfModule authn_file_module>
DavLockDB  "D:/Programme/xampp/tmp/DavLock"
Alias  /webdav "D:/Programme/xampp/webdav"
<Directory  "D:/Programme/xampp/webdav">
    Dav On
    Order allow,deny
    Allow from all
    AuthName "XAMPP with WebDAV"
    AuthType Basic
    AuthUserFile "D:/Programme/xampp/security/htpasswd.webdav"
    <LimitExcept GET HEAD OPTIONS>
        require valid-user
    </LimitExcept>
</Directory>
BrowserMatch "Microsoft Data Access Internet Publishing Provider" redirect-
carefully
BrowserMatch "MS FrontPage" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
BrowserMatch "^gnome-vfs/1.0" redirect-carefully
BrowserMatch "^XML Spy" redirect-carefully
BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully
BrowserMatch "MSIE" AuthDigestEnableQueryStringHack=On
</IfModule>
</IfModule>
</IfModule>
</IfModule>
```

3. Starten Sie den Apache neu.

Ihre WebDAV-Konfiguration in der Übersicht:

Verzeichnis	**<xampp>\webdav**
URL	`http://localhost/webdav`
Benutzer	`[von Ihnen gewählt]`
Passwort	`[von Ihnen gewählt]`
Passwort-Datei (mit htpasswd)	`<xampp>\security\htpasswd.webdav`

3.4.6 AuthType Digest

An dieser Stelle soll noch eine Beispielkonfiguration mit `htdigest` vorgestellt werden.

1. Erstellen Sie eine Passwort-Datei.
   Linux:

   ```
   /opt/lampp/bin/htdigest -c "/opt/lampp/htpdigest.webdav" "XAMPP with WebDAV" ↵
   username
   ```

   Windows:

   ```
   C:\Programme\xampp\apache\bin\htdigest -c ↵
   "C:\Programme\xampp\security\htpdigest.webdav" "XAMPP with WebDAV" username
   ```

2. Editieren Sie die `httpd-dav.conf`.
   Linux:

   ```
   <IfModule dav_module>
   <IfModule dav_fs_module>
   <IfModule auth_digest_module>
   <IfModule setenvif_module>
   <IfModule authn_file_module>
   DavLockDB "/tmp/DavLock"
   Alias /webdav "/opt/lampp/webdav"
   <Directory "/opt/lampp/webdav">
       Dav On
       Order allow,deny
       Allow from all
       AuthName "XAMPP with WebDAV"
       AuthType Digest
       AuthDigestDomain / http://localhost/
       AuthUserFile "/opt/lampp/htdigest.webdav"
       <LimitExcept GET HEAD OPTIONS>
           require valid-user
       </LimitExcept>
   </Directory>
   BrowserMatch "Microsoft Data Access Internet Publishing Provider" ↵
   redirect-carefully
   BrowserMatch "MS FrontPage" redirect-carefully
   BrowserMatch "^WebDrive" redirect-carefully
   BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
   BrowserMatch "^gnome-vfs/1.0" redirect-carefully
   BrowserMatch "^XML Spy" redirect-carefully
   BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully
   BrowserMatch "MSIE" AuthDigestEnableQueryStringHack=On
   </IfModule>
   </IfModule>
   </IfModule>
   </IfModule>
   </IfModule>
   ```

Windows:

```
<IfModule dav_module>
<IfModule dav_fs_module>
<IfModule auth_digest_module>
<IfModule setenvif_module>
<IfModule authn_file_module>
DavLockDB "D:/Programme/xampp/tmp/DavLock"
Alias /webdav "D:/Programme/xampp/webdav"
<Directory "D:/Programme/xampp/webdav">
    Dav On
    Order allow,deny
    Allow from all
    AuthName "XAMPP with WebDAV"
    AuthType Digest
    AuthDigestDomain / http://localhost/
    AuthUserFile "D:/Programme/xampp/security/htdigest.webdav"
    <LimitExcept GET HEAD OPTIONS>
        require valid-user
    </LimitExcept>
</Directory>
BrowserMatch "Microsoft Data Access Internet Publishing Provider" ↩
redirect-carefully
BrowserMatch "MS FrontPage" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
BrowserMatch "^gnome-vfs/1.0" redirect-carefully
BrowserMatch "^XML Spy" redirect-carefully
BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully
BrowserMatch "MSIE" AuthDigestEnableQueryStringHack=On
</IfModule>
</IfModule>
</IfModule>
</IfModule>
</IfModule>
```

3. Starten Sie den Apache neu.

3.4.7 Anwendungsmöglichkeiten mit WebDAV

Dreamweaver MX

Bitte beachten Sie: *Dreamweaver MX* kann ***nicht*** mit einer Digest-Authentifizierung umgehen. Also müssen Sie in diesem Fall mit *AuthType Basic* und *htpasswd* arbeiten. Dann sollte auch Dreamweaver MX problemlos funktionieren.

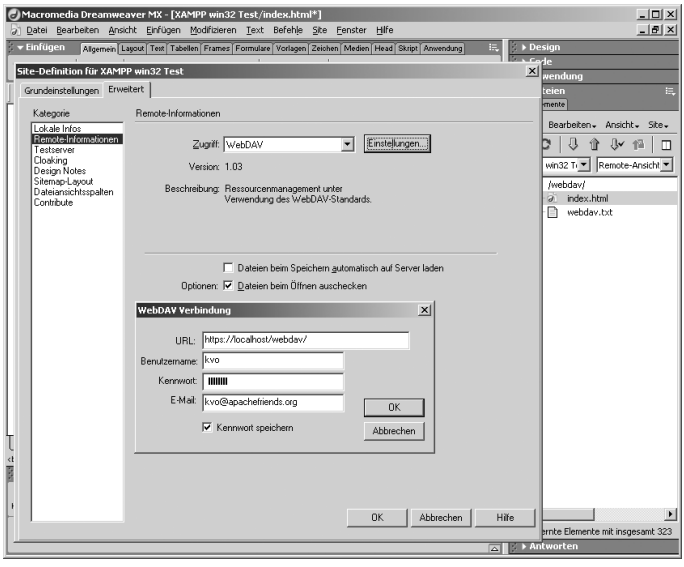


Abbildung 3.4: WebDAV-Konfiguration mit Dreamweaver MX

GoLive CS2

Adobe GoLive CS2 konnte in unseren Versuchen sowohl mit der Authentifizierung über Digest als auch mit Basic problemfrei umgehen. Der Kontakt mit WebDAV erfolgt hier über das Menü unter DATEI > SERVER > MIT WEBDAV VERBINDEN. Sie können wie auch beim *Dreamweaver MX* mehrere Server oder Verzeichnisse angeben.

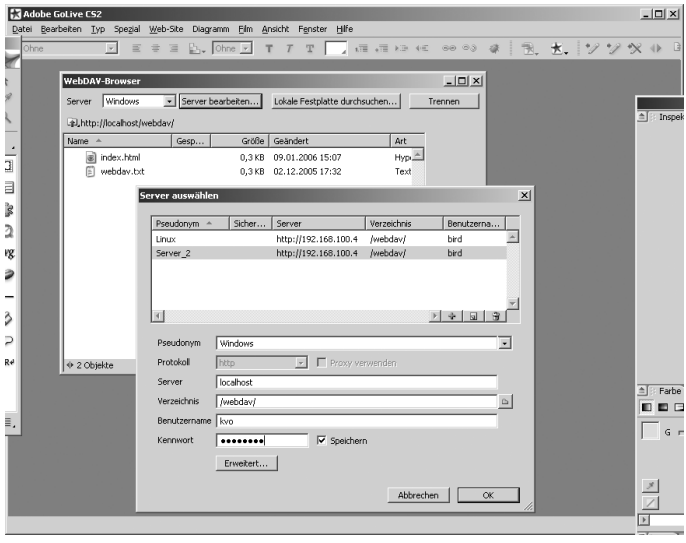


Abbildung 3.5: Adobe Golive CS2 mit WebDAV

WebDAV als Netzwerkordner unter Windows XP

Gehen Sie in die NETZWERKUMGEBUNG, um sich über NETZWERKRESSOURCE VERBINDEN mit dem WebDAV-Netzwerkordner zu verbinden.

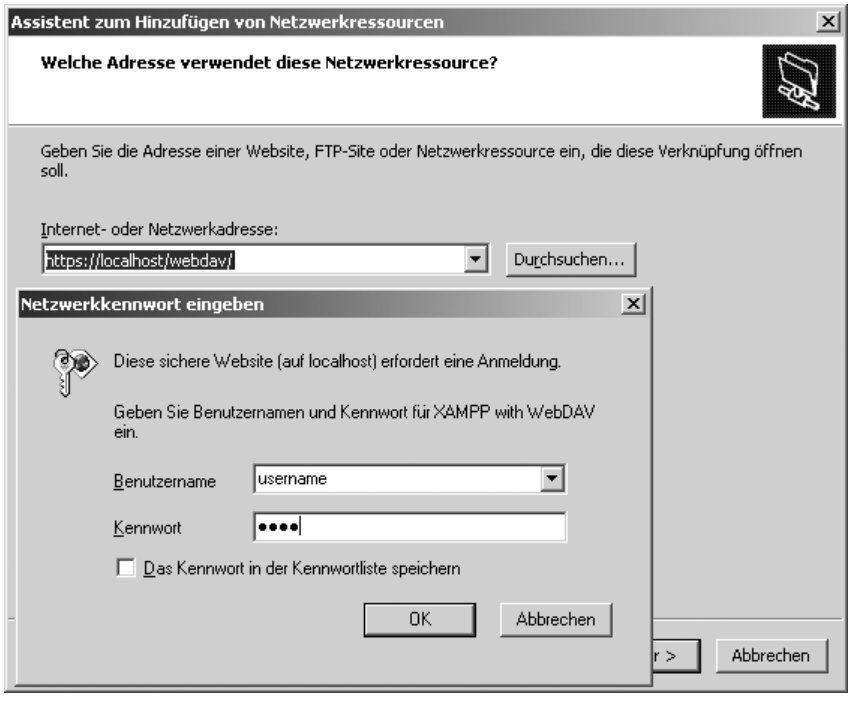


Abbildung 3.6: Anmelden am WebDAV-Ordner

Alles erfolgreich eingerichtet? Dann testen Sie Ihren neuen Webordner im Bereich NETZWERKUMGEBUNG.

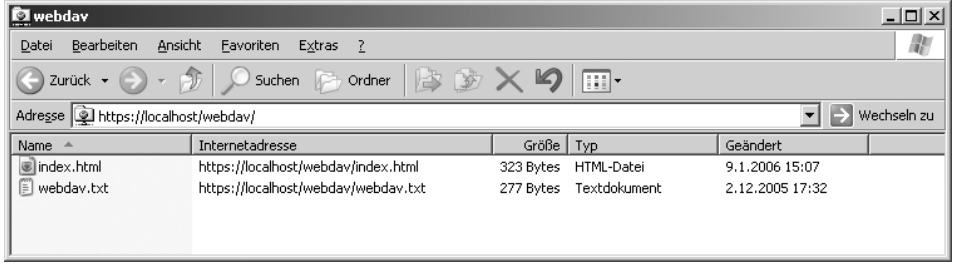


Abbildung 3.7: Der neue Netzwerkordner