SIEMENS

Global network of innovation

optiPoint 410/420 Familie

IEEE 802.1x
Zertifikate über gesicherte Verbindung

Administrationsanleitung

Inhalt

1 Einführung

In dieser Anleitung wird beschrieben, wie Sie eine sichere Umgebung herstellen und einrichten, um Telefone mit Konfigurationsdaten zu versorgen, über XML-Dateien zu versorgen indem Sie XML-Dateien über einen Web-Server verwenden (gesicherte Datenübertragung).

Um eine gesicherte Datenverbindung zum Download-Weber-Server zu gewährleisten, werden Konfigurationsdaten über das HTTPS-Protokoll anstatt nur über HTTP (oder FTP) gesandt. HTTPS ist eigentlich eine HTTP-Verbindung über TLS V1 (oder SSL V3) bei der alle Konfigurationsdaten verschlüsselt übertragen werden. Beim Verbindungsaufbau authentifizieren sich sowohl das Telefon als auch der Download-Web-Server. Dabei wird ein gegenseitig anerkanntes Zertifikat verwendet, das auf der TLS-Authentifizierungs-Option basiert. Telefon und Web-Server können sich aber auch ohne dieses Verfahren auf eine sichere Art authentifizieren.

Diese Anleitung beschreibt die nötigen Schritte und Gesamteinstellungen, um alle Komponenten zu konfigurieren, die nötig sind, um eine XML-Konfigurationsdatei und wenn nötig auch 802.1x Zertifikate über eine gesicherte Datenverbindung zum Telefon zu senden.

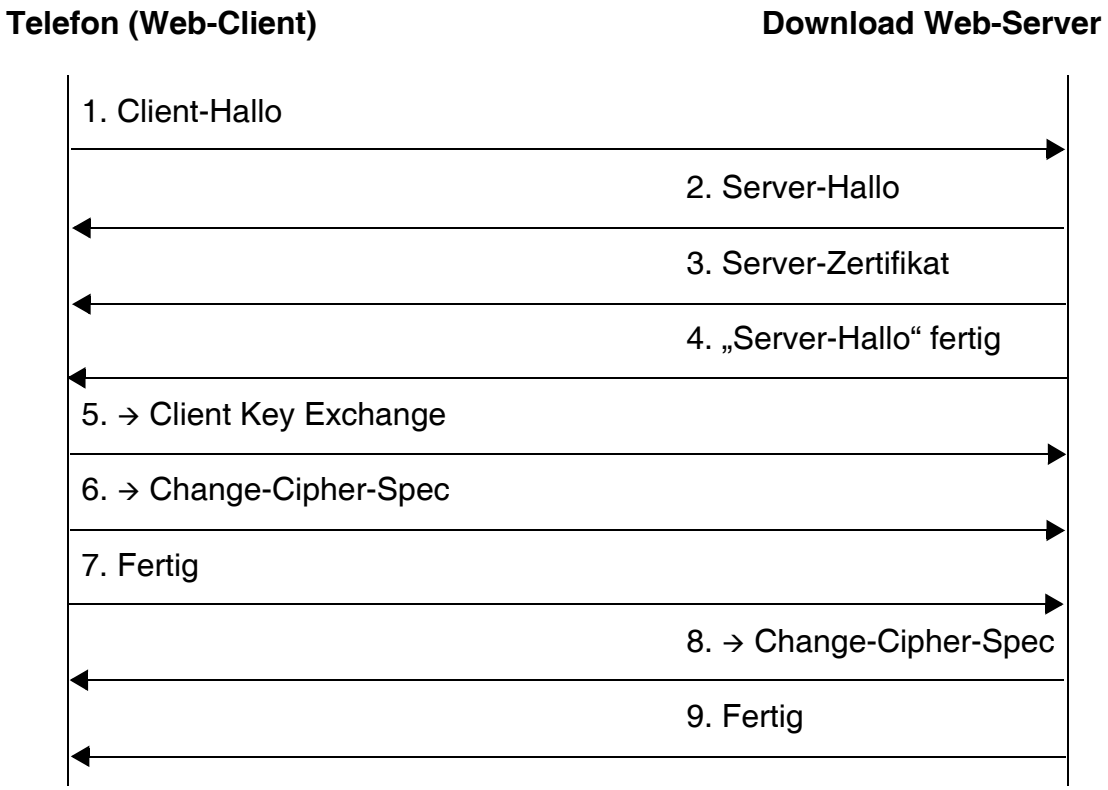
Dieses Dokument ist eine Ergänzung zu der bereits vorhandenen Dokumentation. Wie Sie XML-Konfigurationsdateien erstellen, erfahren Sie im XML Konfigurationshandbuch.

1.1 Prinzip

XML über eine sichere Verbindung arbeitet nach dem gleichen Prinzip wie XML über FTP (nicht sicher). Die einzige Unterschied ist, das die Daten, die zwischen zwei Teilnehmern gesandt werden, verschlüsselt werden, nachdem sich die beiden Teilnehmer gegenseitig authentifiziert haben. Wenn die Daten so eingekapselt sind, können sie von Dritten nicht gelesen werden.

Das folgende Diagramm zeigt die Phasen während des Aufbaus einer TLS-Verbindung vom Telefon zum „sicheren“ Web-Server, um den Download der angeforderten XML-Dateien auf eine sichere Art zu starten.

Handshake Sequenz für TLS



In der Phase „Client-Hallo“ (Schritt 1) bietet das Telefon an, TLS V1 oder SSL V3 zu unterstützen und stellt folgende → Cipher suite zur Verfügung, die auch die verschlüsselte Signalisierung des SIP-Interface unterstützt:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_3DES_EDE_CBC_SHA
- TLS_RSA_DES_CBC_SHA

Der Download Web-Server wählt TLS oder SSL und eines der → Cipher suite aus, um sie in der „Server-Hallo“ Phase (Schritt 2) in Abstimmung mit seiner Richtlinie zu verwenden.

In der Phase „Server-Zertifikat“ (Schritt 3) schickt der Server sein selbst digital-signiertes → X.509-Zertifikat, um dem Telefon zu ermöglichen, den Server zu authentifizieren.

In der Phase „→ Client Key Exchange“ (Schritt 5) generiert das Telefon einen „→ Session key“ (unter Verwendung der RSA-Methode) und verschlüsselt ihn mit dem „öffentlichen Schlüssel“ des Servers (aus dem Server-Zertifikat) bevor es ihn sendet.

Die Phase → Change-Cipher-Spec-Meldung (Schritt 6 und 8) zeigt an, das die gesamte weitere Kommunikation verschlüsselt sein wird (unter Verwendung des gültigen → Session key).

Die → TLS resume method wird vom Telefon unterstützt, indem es für eine nachfolgende TLS-Verbindung den bestehenden symmetrischen → Session key verwendet.

Ein → Session key kann nur:

- für eine begrenzten Zeitraum,
- für ein Höchstmaß an Datenübertragung
- oder bis einer von beiden verlangt, einen neuen Schlüssel auszuhandeln

wieder verwendet werden.

Die → Server Policy legt fest, ob die Wiederherstellungs-Methode zulässig ist. Beim Speichern der zugehörigen Berechtigungseinstellungen für eine große Anzahl von Telefonen können auf dem Server Leistungsprobleme auftreten.

Nachfolgend ein Trace-Beispiel:

Quelle	**Ziel**	**Protokoll**	**Information**
498972213007.gvs.lab	securexml.gvs.lab	TCP	1024 > https [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=11 TSER=0
securexml.gvs.lab	498972213007.gvs.lab	TCP	https > 1024 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
498972213007.gvs.lab	securexml.gvs.lab	TCP	1024 > https [ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=11 TSER=0
498972213007.gvs.lab	securexml.gvs.lab	TLS	Client Hello
securexml.gvs.lab	498972213007.gvs.lab	TLS	Server Hello, Certificate, Server Hello Done
498972213007.gvs.lab	securexml.gvs.lab	TCP	1024 > https [ACK] Seq=61 Ack=888 Win=8192 Len=0 TSV=12 TSER=70086061
498972213007.gvs.lab	securexml.gvs.lab	TLS	Client Key Exchange
securexml.gvs.lab	498972213007.gvs.lab	TCP	https > 1024 [ACK] Seq=888 Ack=200 Win=65336 Len=0 TSV=70086064 TSER=12
498972213007.gvs.lab	securexml.gvs.lab	TLS	Change Cipher Spec, Encrypted Handshake Message
securexml.gvs.lab	498972213007.gvs.lab	TLS	Change Cipher Spec, Encrypted Handshake Message
498972213007.gvs.lab	securexml.gvs.lab	TLS	Application Data
securexml.gvs.lab	498972213007.gvs.lab	TCP	https > 1024 [ACK] Seq=931 Ack=297 Win=65239 Len=0 TSV=70086066 TSER=12
498972213007.gvs.lab	securexml.gvs.lab	TLS	Application Data
securexml.gvs.lab	498972213007.gvs.lab	TLS	Application Data

Quelle	Ziel	Protokoll	Information
securexml.gvs.lab	498972213007.gvs.lab	TCP	https > 1024 [FIN, ACK] Seq=2005 Ack=363 Win=65173 Len=0 TSV=70086067 TSER=12
498972213007.gvs.lab	securexml.gvs.lab	TCP	1024 > https [ACK] Seq=363 Ack=2006 Win=7118 Len=0 TSV=12 TSER=70086067
498972213007.gvs.lab	securexml.gvs.lab	TCP	1024 > https [FIN, ACK] Seq=363 Ack=2006 Win=8192 Len=0 TSV=13 TSER=70086067
securexml.gvs.lab	498972213007.gvs.lab	TCP	https > 1024 [ACK] Seq=2006 Ack=364 Win=65173 Len=0 TSV=70086067 TSER=13
498972213007.gvs.lab	securexml.gvs.lab	TCP	1025 > https [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=13 TSER=0
securexml.gvs.lab	498972213007.gvs.lab	TCP	https > 1025 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
498972213007.gvs.lab	securexml.gvs.lab	TCP	1025 > https [ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=13 TSER=0
498972213007.gvs.lab	securexml.gvs.lab	TLS	Client Hello
securexml.gvs.la	498972213007.gvs.lab	TLS	Server Hello, Change Cipher Spec, Encrypted Handshake Message
498972213007.gvs.lab	securexml.gvs.lab	TLS	Change Cipher Spec
securexml.gvs.lab	498972213007.gvs.lab	TCP	https > 1025 [ACK] Seq=123 Ack=99 Win=65437 Len=0 TSV=70086071 TSER=13
498972213007.gvs.lab	securexml.gvs.lab	TLS	Encrypted Handshake Message, Application Data, Application Data
securexml.gvs.lab	498972213007.gvs.lab	TCP	[TCP segment of a reassembled PDU]
securexml.gvs.lab	498972213007.gvs.lab	TCP	[TCP segment of a reassembled PDU]
securexml.gvs.lab	498972213007.gvs.lab	TCP	[TCP segment of a reassembled PDU]
securexml.gvs.lab	498972213007.gvs.lab	TCP	[TCP segment of a reassembled PDU]
498972213007.gvs.lab	securexml.gvs.lab	TCP	1025 > https [ACK] Seq=268 Ack=4503 Win=8192 Len=0 TSV=13 TSER=70086071
securexml.gvs.lab	498972213007.gvs.lab	TLS	Application Data
498972213007.gvs.lab	securexml.gvs.lab	TCP	1025 > https [ACK] Seq=268 Ack=5076 Win=7620 Len=0 TSV=13 TSER=70086071
498972213007.gvs.lab	securexml.gvs.lab	TCP	1025 > https [FIN, ACK] Seq=268 Ack=5076 Win=8192 Len=0 TSV=13 TSER=70086071
securexml.gvs.lab	498972213007.gvs.lab	TCP	https > 1025 [ACK] Seq=5076 Ack=269 Win=65268 Len=0 TSV=70086071 TSER=13

1.2 Voraussetzung

Bevor Sie die Konfigurationselemente des Telefons über eine sichere Verbindung versorgen können, müssen folgende Komponenten oder Softwarepakete vorhanden sein oder installiert werden. Ab Kapitel → Einrichten finden Sie weitere Informationen und „Screen shots“ zu diesen speziellen Komponenten.

1. Ein Server

Es gibt keine speziellen Anforderungen an den Server. Beziehen Sie sich bitte auf die Anforderungen der Softwarepakete, die Sie für Ihr System installiert haben.

2. Web-Server

Sie können jede Web-Server-Anwendung verwenden, die gesicherte Webdienste unterstützt. Der Web-Server muss folgende Protokolle unterstützen: TCP, TLS, HTTP über TLS (HTTPS), → X.509 Zertifikate und XML. Beachten Sie, dass das verwendete XML ein kundenspezifisches Format hat. Wie Sie eine XML-Konfigurationsdatei erstellen, lesen Sie bitte im XML-Konfigurationshandbuch nach. Für das nachfolgende Beispiel wird der Microsoft Internetinformationsdienste Server (IIS) verwendet, der auf einem Windows 2003 Server installiert ist.

Bevor Sie den Microsoft Internetauthentifizierungsdienst installieren, muss zuerst der Microsoft Internetinformationsdienste Server (IIS) installiert sein.

Falls Sie einen Apache-Web-Server oder einen anderen ähnlichen Web-Server installieren wollen, müssen Sie nicht unbedingt den Microsoft Internetauthentifizierungsdienst installieren. Lesen Sie bitte hierzu die entsprechende Dokumentation.

3. Installieren einer Zertifizierungsstelle

Um einen sicheren Web-Server einzurichten, braucht der Web-Server ein Root- und Server-Zertifikat das von einer Stammauthentifizierungsstelle oder einer anderen Anwendung wie z. B. „Open SSL“ erstellt und signiert wird. Erstellen und Signieren von öffentlichen Zertifikaten ist nicht kostenlos. Sie können daher Ihre eigenen Root- und Server-Zertifikate erstellen, dafür gibt es genug Anwendungen wie z. B. Open SSL.

Für dieses Beispiel wird die Microsoft Zertifizierungsstelle verwendet, die auf dem gleichen Server installiert ist, wie der Internetinformationsdienste Server.

Da die Zertifizierungsstelle nach dem IIS installiert werden muss, wird die nötige Umgebung mitinstalliert, um http://[IP addr.]/certsrv auszuführen.

4. Erstellen einer Server-Zertifikat-Anforderungsdatei (→ CSR)

Abhängig vom verwendeten Weber-Server-Dienst oder Anwendung, kann die Art, wie man eine Zertifikatsanforderung erstellt, ziemlich unterschiedlich sein.

In dem folgenden Beispiel soll gezeigt werden, wie man die Anforderungsdatei im Rahmen des zuvor installierten IIS erstellt.

5. Signieren des → Server-Zertifikat von der → Zertifizierungsstelle

Die Zertifikatsanforderungsdatei (CSR) muss signiert werden. Das kann durch eine offizielle Zertifizierungsstelle oder unter Verwendung eines privaten Root- und Server-Zertifikats geschehen. Im nachfolgenden Beispiel wird dafür die Microsoft Zertifizierungsstelle verwendet.

6. Importieren und aktivieren des Server-Zertifikats

Nachdem Sie das Server-Zertifikat von einer offiziellen Zertifizierungsstelle erhalten oder selbst erstellt haben, müssen Sie es importieren und aktivieren.

7. Das Telefon für HTTPS-Verbindung einstellen

Am Telefon müssen Sie die entsprechenden Parameter für die sichere Verbindung zum Web-Server entweder über das Telefonmenü oder über die Web-Schnittstelle des Telefons konfigurieren.

Es ist auch möglich, die Adresse des gesicherten Web-Servers über den DHCP-Server an das Telefon zu senden (herstellerspezifisches Informations-Element). Für diesen Fall sollten Sie die XML-Dateien auf dem Web-Server so benennen, wie sie als Voreinstellung in den Telefonen verwendet werden. Das nachfolgende Beispiel zeigt die Konfiguration über die Web-Schnittstelle (WBM).

8. Überprüfen und testen der HTTPS-Verbindung

Um sicher zu gehen, dass der Web-Server die angeforderte Datei an das Telefon schickt, oder um den Inhalt von XML-Dateien zu prüfen, kann man dafür einfach einen Web-Browser verwenden, der XML unterstützt.

9. 802.1X Zertifikate in der XML-Konfigurationsdatei

Für den Fall, dass das Telefon 802.1x-Authentifizierung braucht, ist es möglich, die benötigten 802.1x Server- und Client-Zertifikate über XML-Konfigurationsdateien an das Telefon zu senden. Das ermöglicht dem Telefon auf die 802.1X-Anfrage vom → Layer 2 Switch zu antworten und mit dem Radius-Server zu verhandeln, damit es einen freigegebenen Port auf dem → Layer 2 Switch erhält. Das von der Zertifizierunstelle signierte Server-Zertifikat ist im PEM-Format in der XML-Datei gespeichert. Das Client-Zertifikat ist Passwortgeschützt im 64 Bit binären Format (B64) gespeichert. In XML-Dateien sind solche Zertifikate XML-Elemente, wie auch alle anderen Elemente. „Cut and paste“ wird verwendet, um die Daten in den „XML-Schreib“-Elementen zu erstellen: „802.1x-Zertifikate und „radius-server-ca1“. Weitere Information zu 802.1x-Authentifizierung finden Sie im „IEEE 802.1x Configuration Management“ Administration Manual “A31003-J4200-M100-*-76A9.pdf”.

In der SIP Version 6.0.xx ist es nicht möglich, den Passwortsatz an das Telefon als XML-Element zu senden, daher muss das Zertifikat mit einem speziellen Passwortsatz, der nur einigen Siemens-Mitarbeitern bekannt ist, kodiert werden.

Im Fall, dass sich die Versionsnummer im „System- oder Gerätekonfiguration“-Element ändert (z. B. von 1 nach 2), erfolgt jedes Mal ein Neustart des Telefons, unabhängig davon, welches Element sich geändert hat. Das ist deshalb so, weil die XML-Datei das Zertifikat enthält. Beispiel:

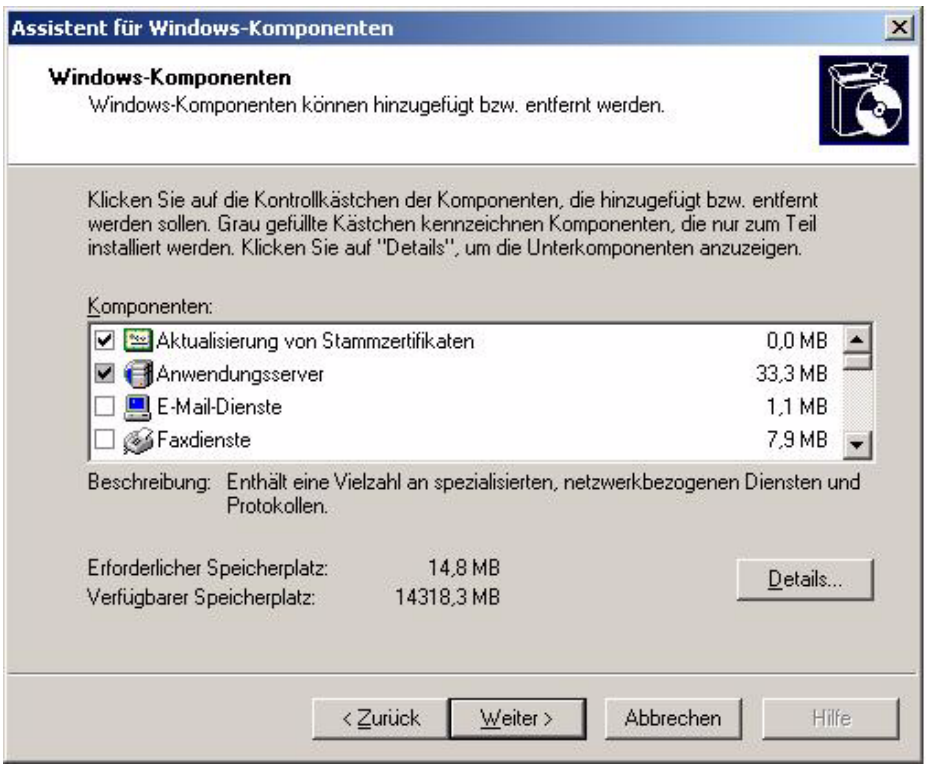
```
<Item name="system-config-version">1</Item>
```

2 Einrichten

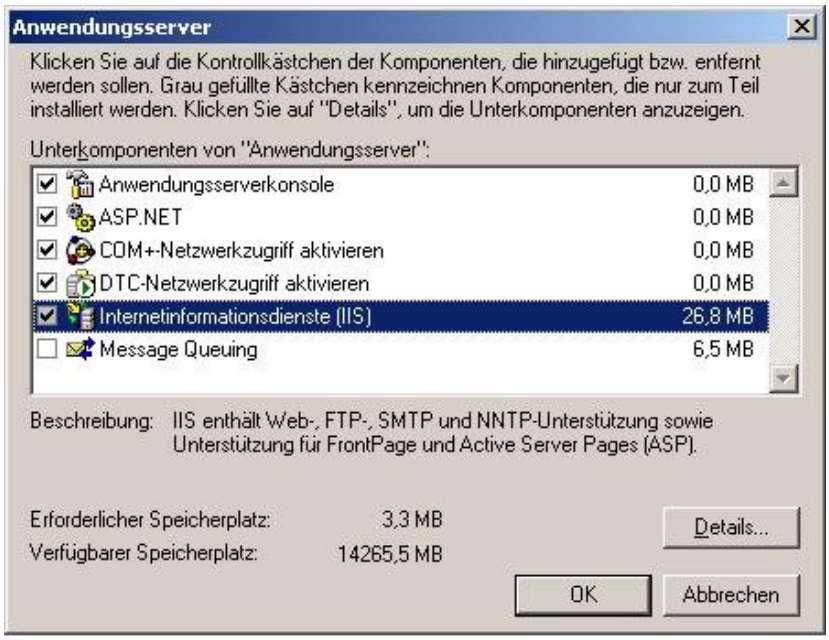
2.1 Installieren des Web-Servers

IIS ist ein zusätzliches Software-Paket für Windows. Öffnen Sie die **Systemsteuerung** und wählen Sie **Software** und anschließend die Option **Windows-Komponenten hinzufügen/entfernen**. In der aufgerufenen Liste wählen Sie **Internetinformationsdienste (IIS)**.

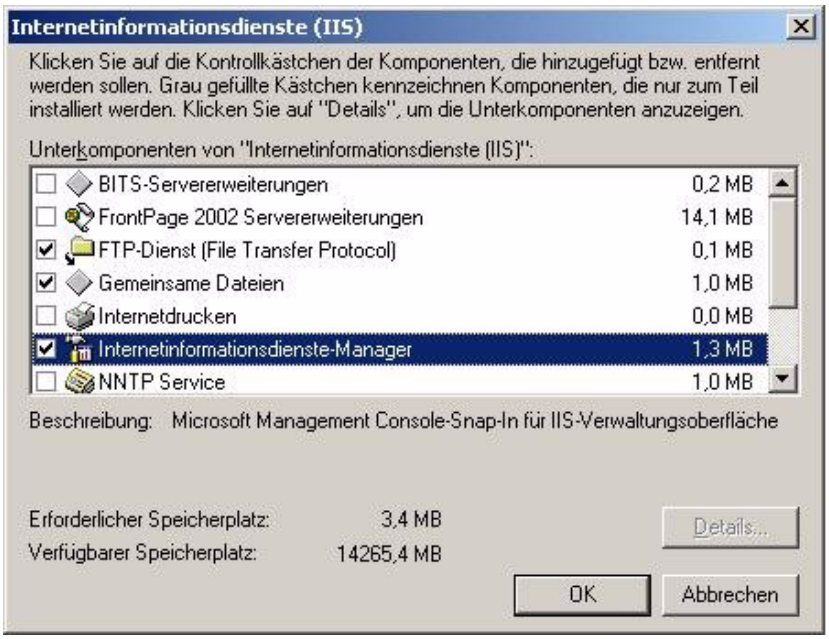
Abhängig von der Windows-Version kann sich der IIS an unterschiedlicher Stelle befinden. Entweder direkt oder in der Gruppe **Anwendungsserver** (wie nachfolgend).



Markieren Sie im Hauptmenü **Assistent für Windows-Komponenten** die Option **Anwendungsserver** und öffnen Sie mit **Details...** das Optionsmenü „**Anwendungsserver**“.



Markieren Sie “**Internetinformationsdienste (IIS)**” und öffnen Sie mit **Details...** das Optionsmenü **Internetinformationsdienste (IIS)**.



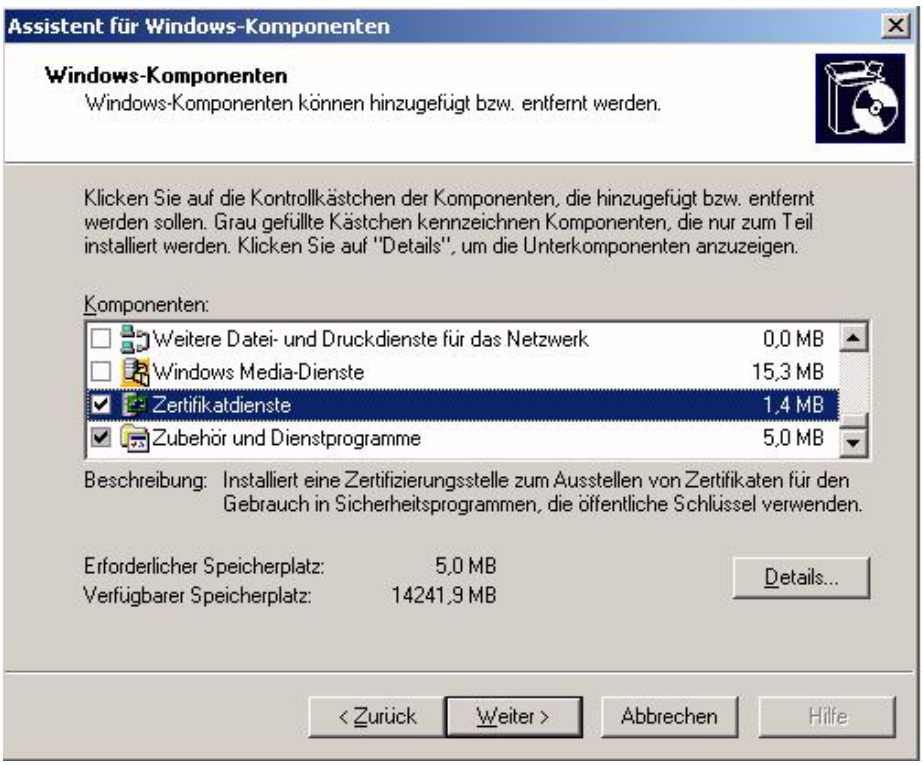
Markieren Sie hier die Option **Internetinformationsdienste-Manager**, und den **FTP-Dienst (File Transfer Protocol)** (nicht unbedingt erforderlich, um den gesicherten Download durchzuführen – kann aber als Web-Server z. B. für Wartemusik oder INI-Datein sehr nützlich sein).

Schließen Sie mit **OK** die Installation der **Internetinformationsdienste (IIS)** ab.

2.2 Installieren der Zertifizierungsstelle

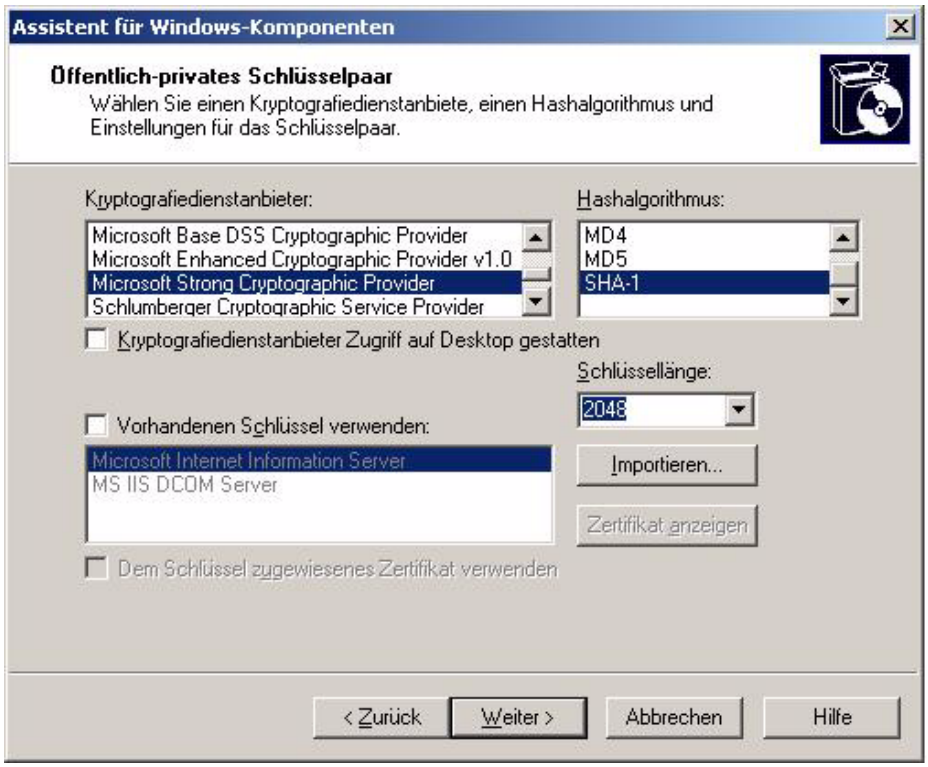
Zertifizierungsstelle(CA) ist eine zusätzliche Windows-Server Anwendung. Öffnen Sie die **Systemsteuerung** und wählen Sie **Software** und anschließend die Option **Windows-Komponenten hinzufügen/entfernen**. In der aufgerufenen Liste wählen Sie **Zertifikatdienste**.

Eine **Zertifizierungsstelle** ist nur auf einem Windows-Server verfügbar. Diese **Zertifizierungsstelle** wird als eine **Eigenständige Stammzertifizierungsstelle** installiert.

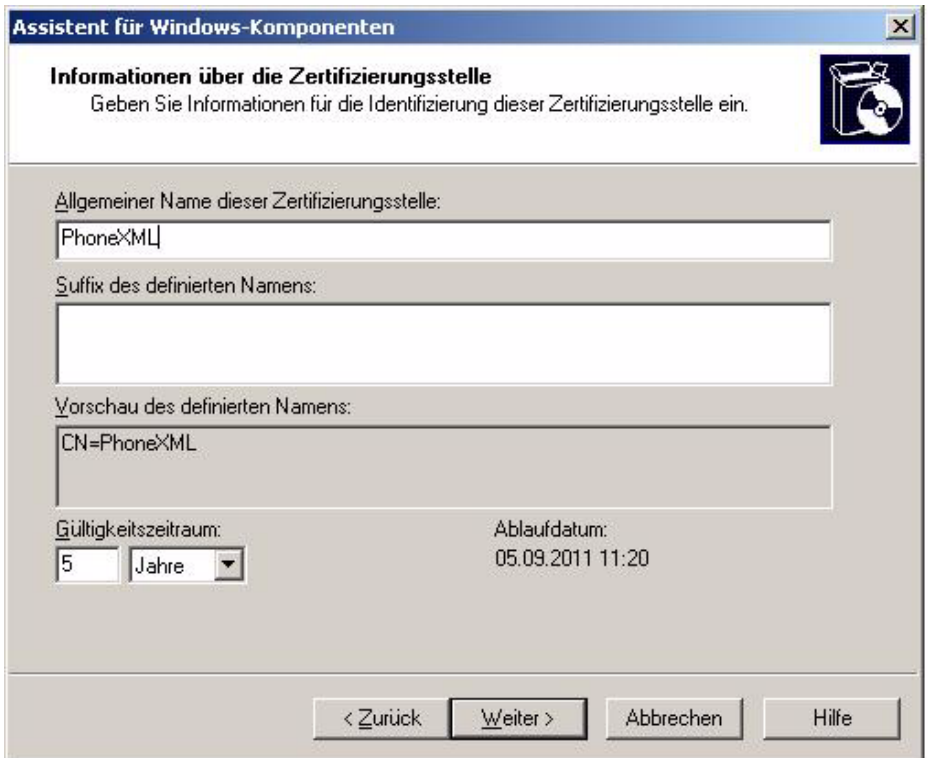


Wählen Sie im Optionsmenü **Assistent für Windows-Komponenten** die “**Zertifikatdienste**” – Sie erhalten das Optionsmenü für den Zertifizierungsstellentyp:

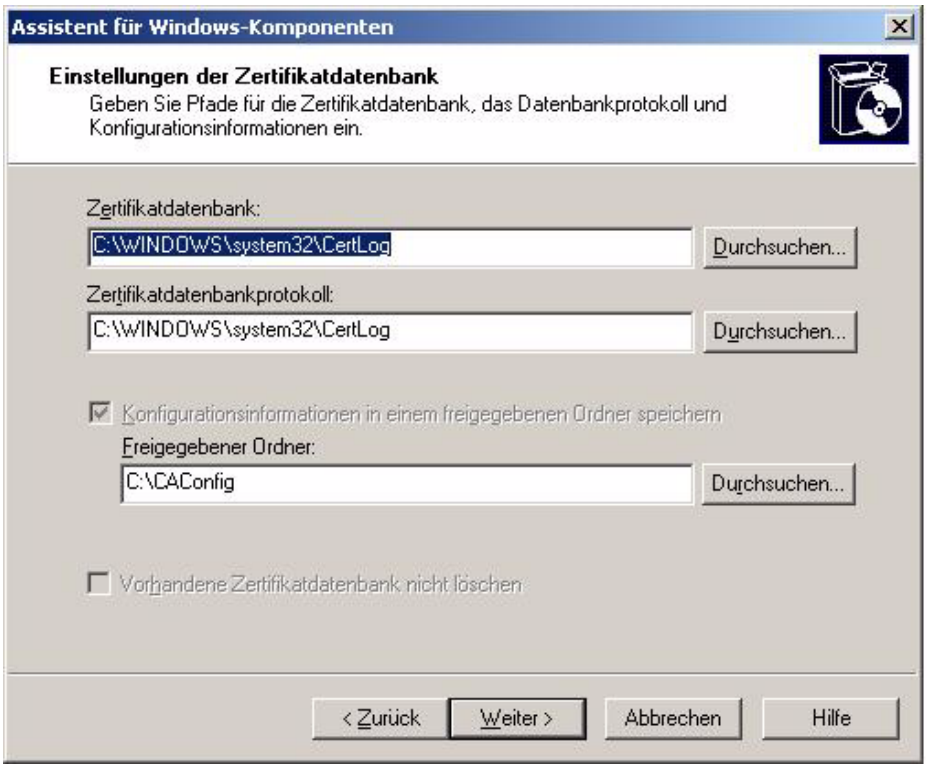
Wählen Sie die Option “**Eigenständige Stammzertifizierungsstelle**” und markieren Sie die Option **Schlüsselpaar und ein Zertifizirungsstellenzertifikat mit diesen Einstellungen erstellen**. Rufen Sie mit **Weiter** das nächste Menü auf.



Wählen Sie die erforderlichen Parameter wie im obigen Screen-Shot dargestellt. Wählen Sie eine Schlüssellänge. Bestätigen Sie Ihre Eingaben mit **Weiter**. Sie erhalten folgenden Dialog.

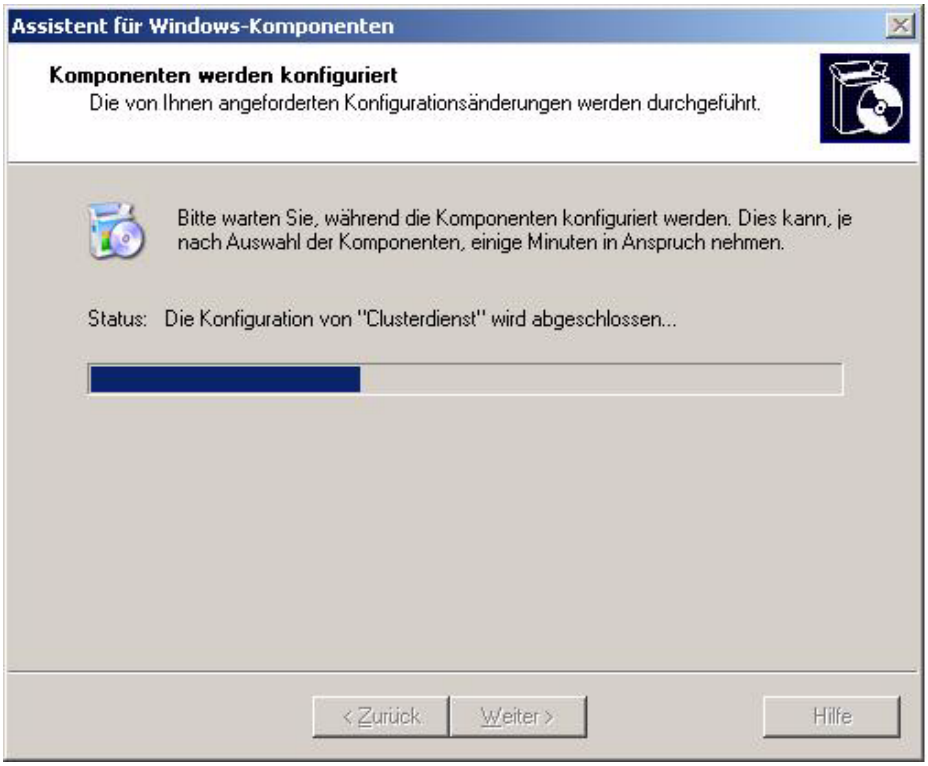


Geben Sie einen bezeichnenden Namen und eine Gültigkeitsdauer für Ihre **Zertifizierungsstelle** an. Bestätigen Sie Ihre Eingaben mit **Weiter**. Sie erhalten folgenden Dialog.

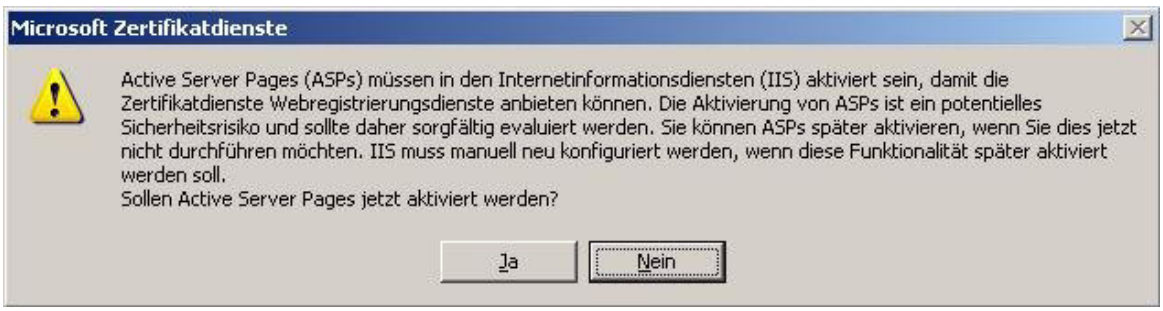


Falls gewünscht, ändern Sie hier die Zielordner für Datenbank-Dateien und andere. Bestätigen Sie Ihre Eingaben mit **Weiter**. Sie erhalten folgenden Dialog.

Hier einfach mit **Ja** weiter.



Alle benötigten Dateien werden installiert.



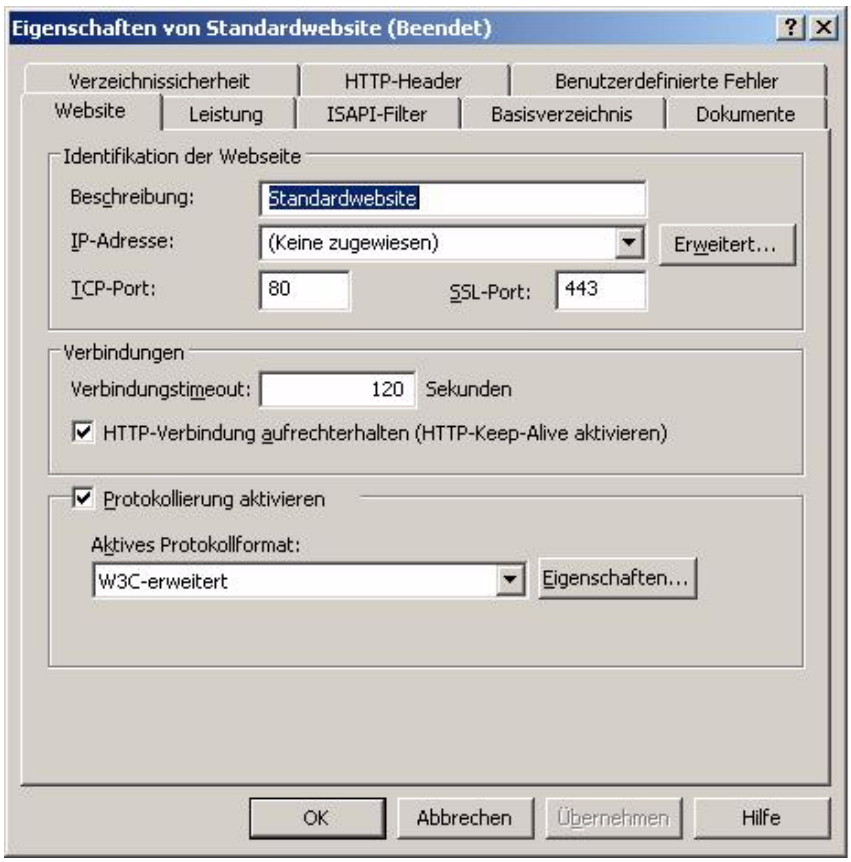
Wählen Sie **Ja**, um die „Aktiven Server-Seiten (ASPs)“ zu aktivieren.

Beenden Sie mit **Fertig stellen**.

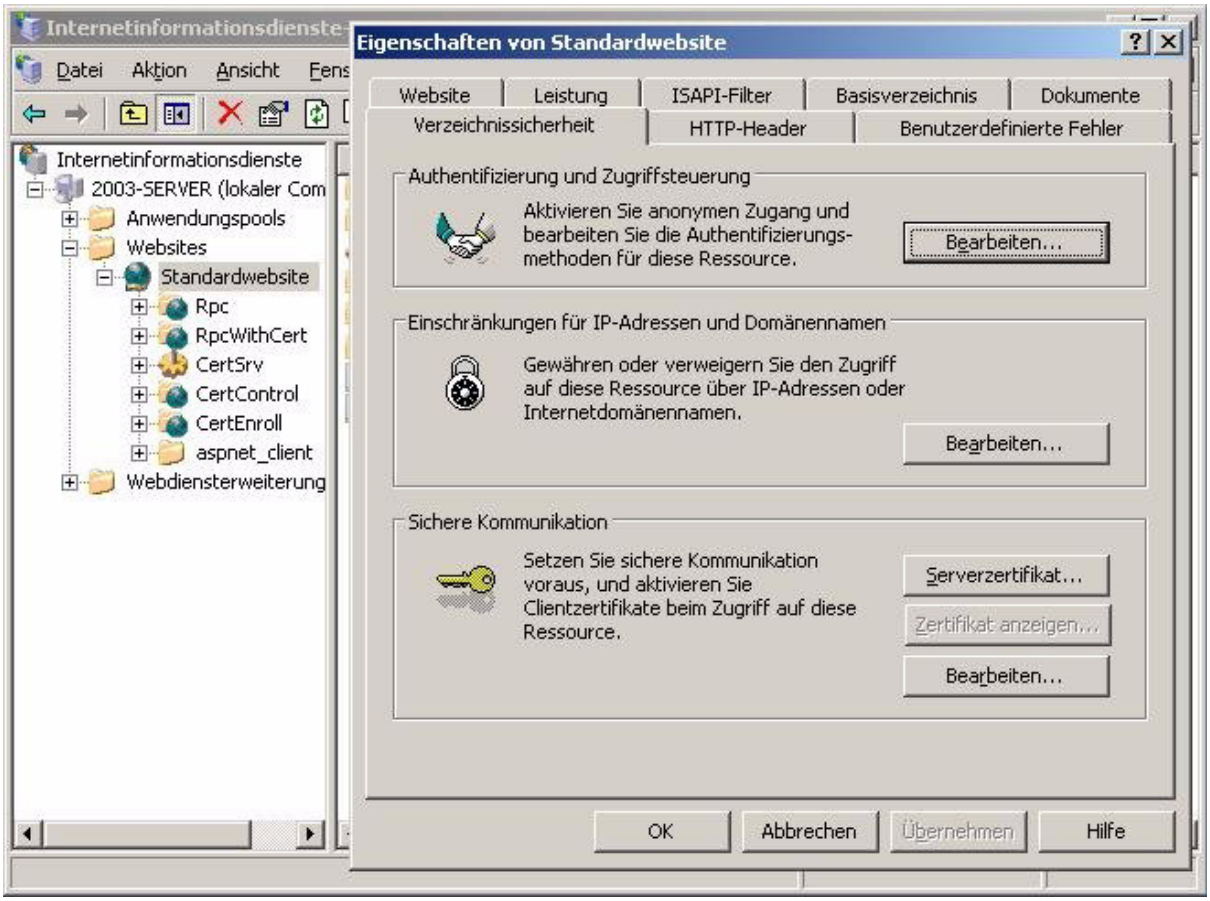
2.2.1 Erstellen einer Server-Zertifikats-Anforderungsdatei (CSR).

In diesem Beispiel wird keine eigene Website erstellt. Es wird die Standard Website des Beispiels verwendet (sie können aber auch zuerst eine neue Website erstellen und anschließend alle Schritte, ausgehend von Ihrer erstellten Website, ausführen.

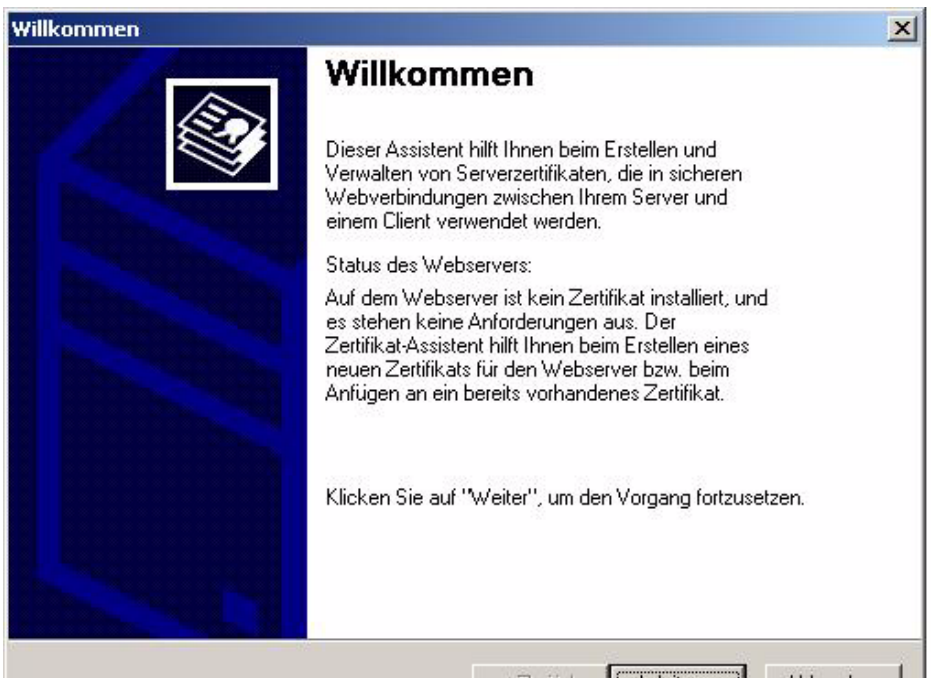
Wählen Sie über **Verwaltung** den **Internetinformationsdienste-Manager** aus. Wählen Sie die gewünschte Website aus (z. B. Standardwebsite) aus. Über die rechte Maustaste öffnen Sie die **Eigenschaften** der Website. Das Register „Website“ wird angezeigt.



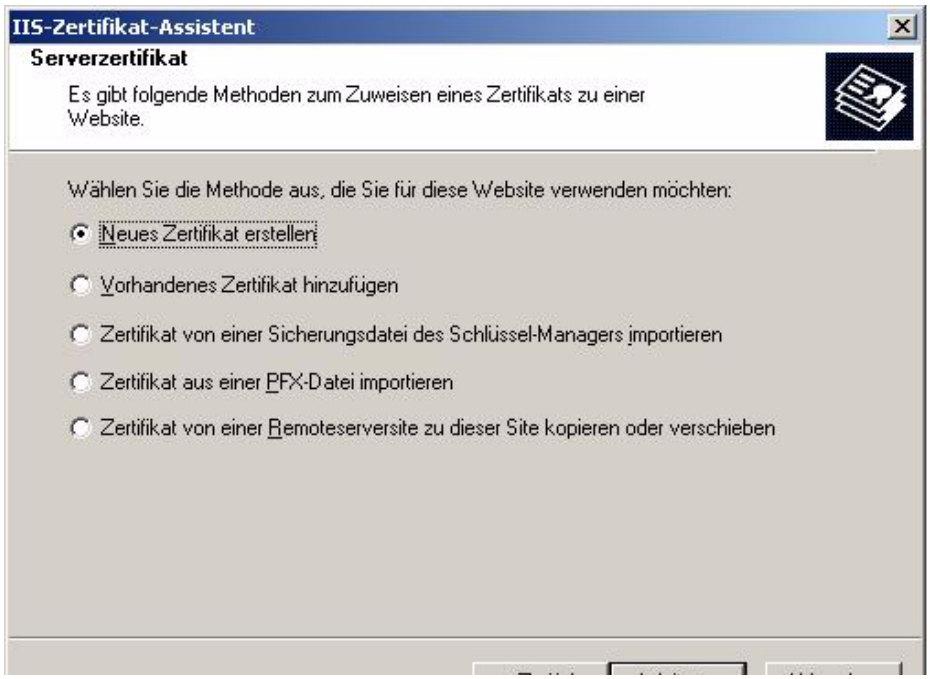
Im Register „**Website**“ der Eigenschaften stellen Sie die gewünschte Port-Nummer die Sie für den SSL-Port verwenden wollen, ein. Die Voreinstellung für den gesicherten Web-Server-Port ist „443“. Sie können hier ggf. auch den **TCP-Port** deaktivieren.



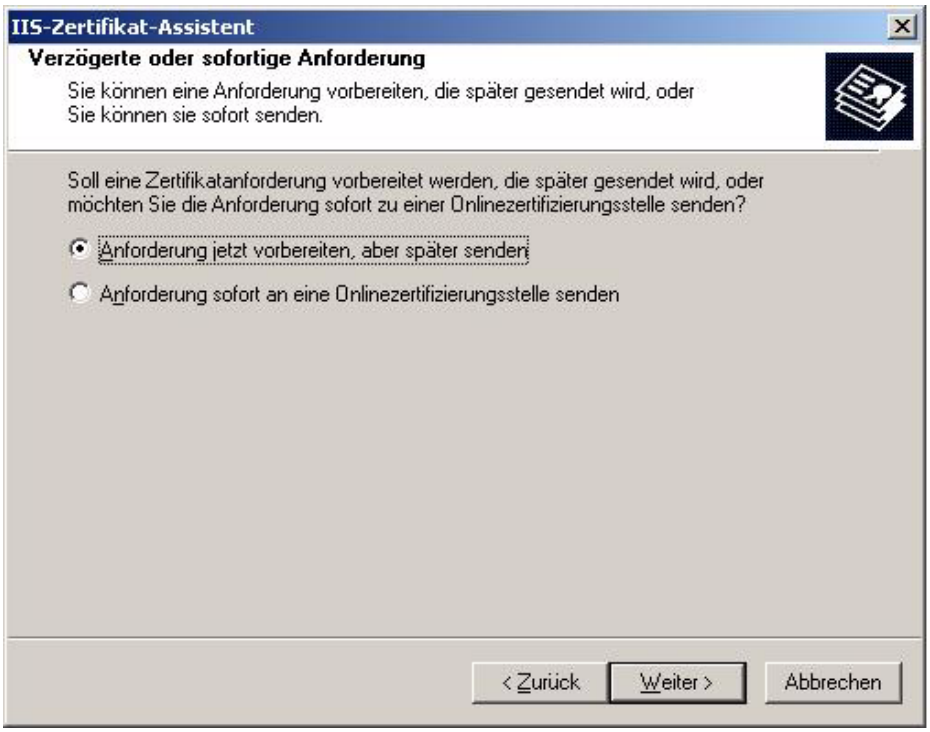
Klicken Sie im Register **Verzeichnissicherheit** auf die Schaltfläche **Serverzertifikat...**



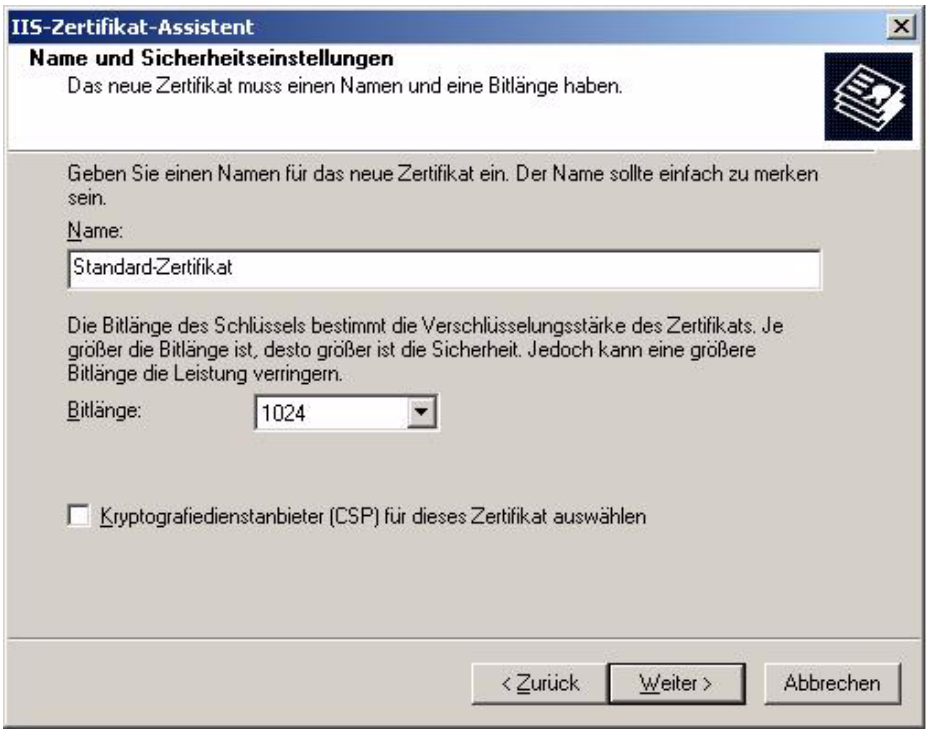
Klicken Sie auf **Weiter**, um den Zertifikats-Assistenten zu starten.



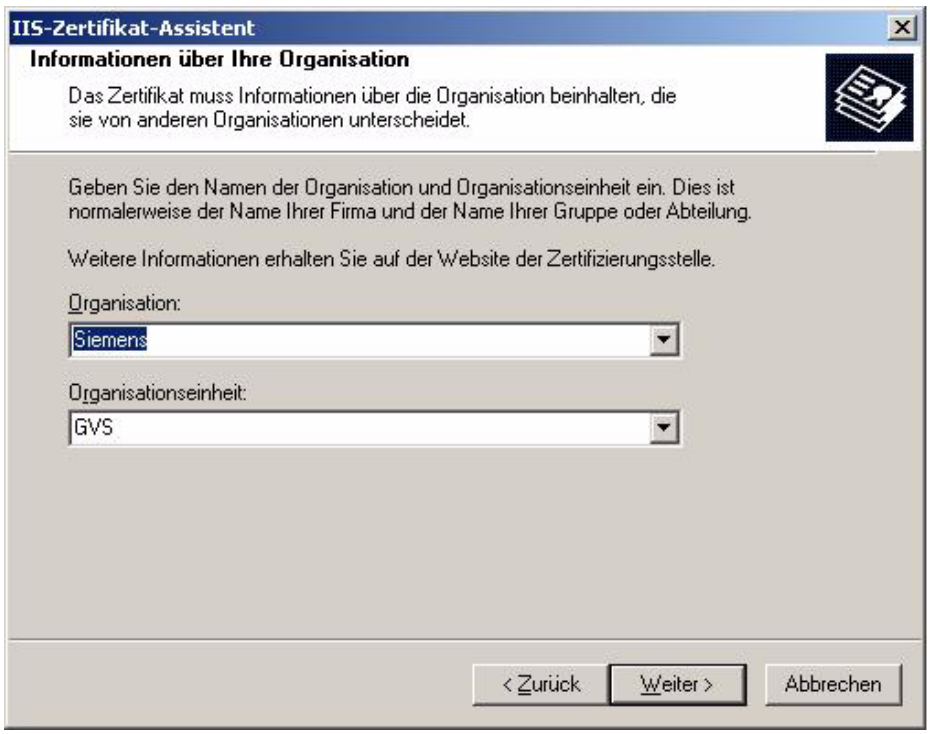
Markieren Sie die Option “**Neues Zertifikat erstellen**”.



Markieren Sie die Option **Anforderung jetzt vorbereiten, aber später senden**. => Klicken Sie auf **Weiter**.

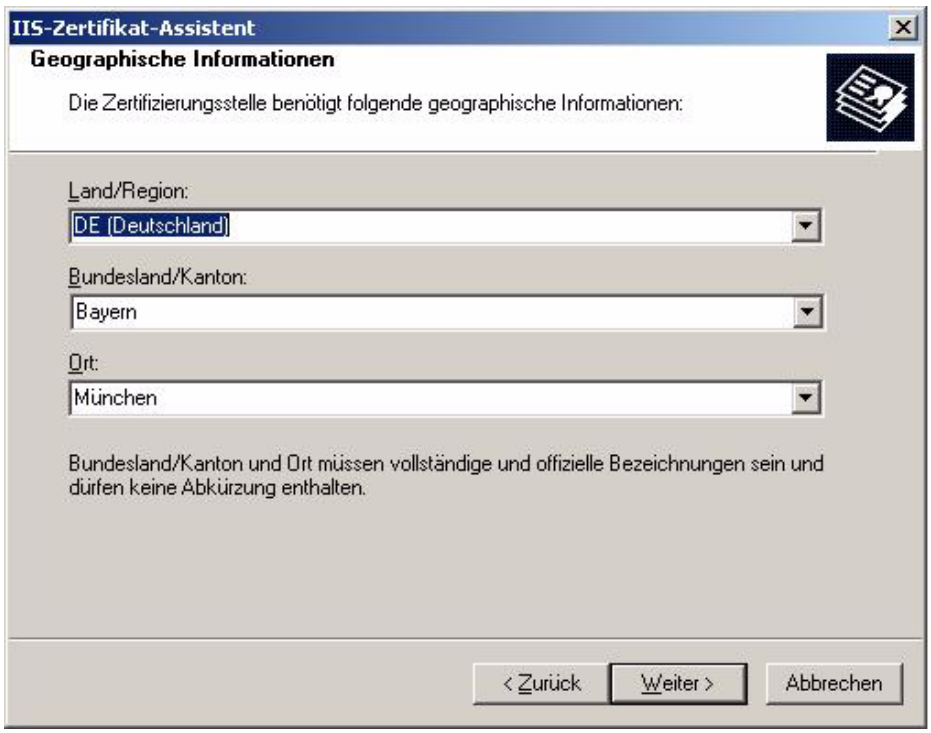


Bestimmen Sie den Namen Ihres Zertifikats und die Schlüssellänge. Klicken Sie auf **Weiter**.



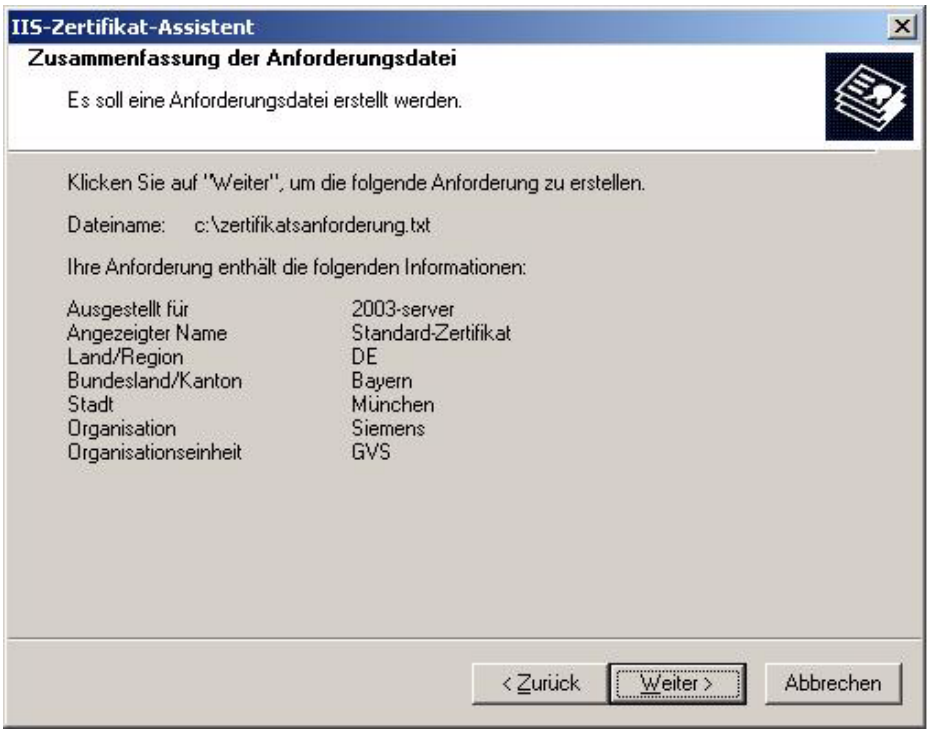
Geben Sie den Namen der Organisation und der Organisationseinheit ein und klicken Sie auf **Weiter**.

Bestimmen Sie **Gemeinsamer Name**" und klicken Sie auf **Weiter**. (Beachten Sie dazu die Erläuterunen im Dialog).



Füllen Sie die Felder "**Land**", "**Bundesland**" und "**Stadt**" aus. Klicken Sie auf **Weiter**.

Bestimmen Sie das Zielverzeichnis und den Dateinamen Ihrer Anforderungsdatei. Klicken Sie anschließend auf **Weiter**.



Prüfen Sie die Parameter. Wenn alles stimmt, dann klicken Sie auf **Weiter**. Andernfalls gehen Sie zurück und korrigieren Sie die Eingaben.

Auf “**Fertig stellen**” klicken. Das Ergebnis dieser Anwendung ist, dass Sie ein Zertifikat erhalten haben, das von einer vertrauenswürdigen Zertifizierungsstelle signiert werden muss.

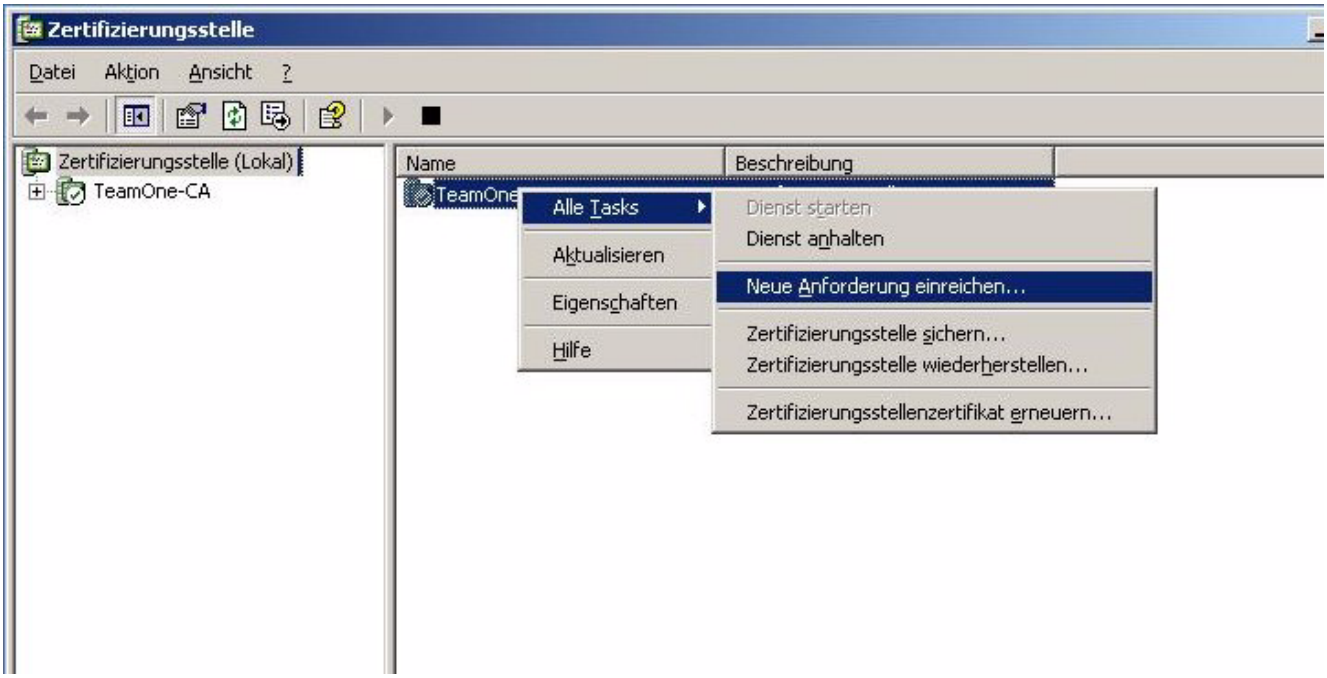
Hier ein Beispiel für den Inhalt einer Anforderungs-Datei.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDSDCCArECAQAwbTELMAkGA1UEBhMCREUxDzANBgNVBAgTBkJheWVybjEXMBUG
A1UEBx4OAE0A/ABuAGMAaABlAG4xEDAOBgNVBAoTB1NpZW1lbnMxDDAKBgNVBAsT
A0dWUzEUMBIGA1UEAxMLMjAwMy1zZXJ2ZXIwgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMBdGVOGbq8UFFmPkHSgBOzDndMcKFzikKiFR9kmT8ZWSjoGRwGUK+kf
35UsD1vJ2xmgkiEclzDOuxmfyljz/O9K/BpNRx/eeACKRQisBiRxGmWN9crkzGvM
7dXfcSVlXAalJFwpMZsmyZeEyRJ0CZztSAbtYlpIqqD9EVVYA/4/AgMBAAGgggGZ
MBoGCisGAQQBgjcNAgMxDBYKNS4yLjM3OTAuMjB7BgorBgEEAYI3AgEOMW0wazAO
BgNVHQ8BAf8EBAMCBPAwRAYJKoZIhvcNAQkPBDcwNTAOBggqhkiG9w0DAgICAIAw
DgYIKoZIhvcNAwQCAgCAMAcGBSsOAwIHMAoGCCqGSIb3DQMHMBMGA1UdJQQMMAoG
CCsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHloATQBpAGMAcgBvAHMA
bwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcgB5AHAAdABvAGcA
cgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABlAHIDgYkAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAADANBgkqhkiG9w0BAQUFAAOBgQAfqpUA
wciHTLKrja3Of6PWg1ZEmhptMg17gCPeApmJhW281H1rWcoyQ+gD5GWHVJDJo+Lx
Ktm3i5pTDNNPez/HKPV/c6PHSSF70wWVvZ59ZOm/Nt7mTCG080R2SxAxH9BbKUBs
```

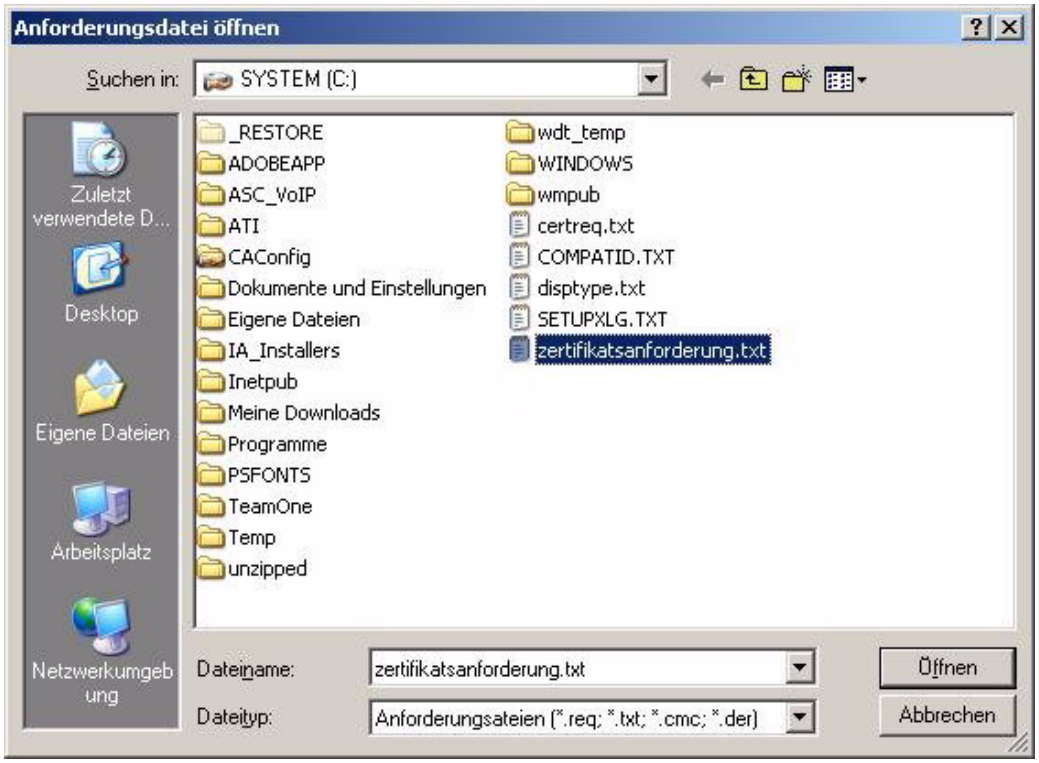
```
0lyM+9t6oGKzxa+EfpA9TTiHwDmzVWP01Z3Chw==
-----END NEW CERTIFICATE REQUEST-----
```

2.2.2 Signieren des Server-Zertifikats über die Zertifizierungsstelle

Öffnen Sie über **Verwaltung** das Menü für die **Zertifizierungsstelle**

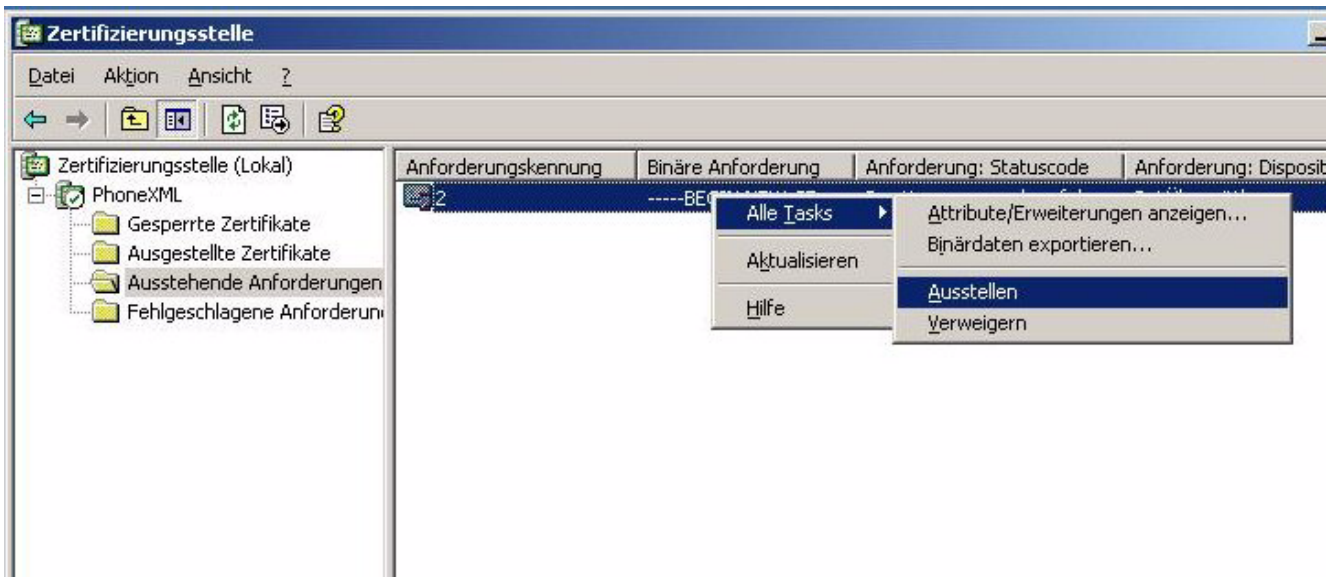


Markieren Sie im rechten Fenster die **Zertifizierungsstelle „TeamOne-CA“**. Markieren Sie mit der rechten Maustaste **Alle Tasks** und **Neue Anforderung einreichen** und öffnen Sie damit das folgende Fenster:

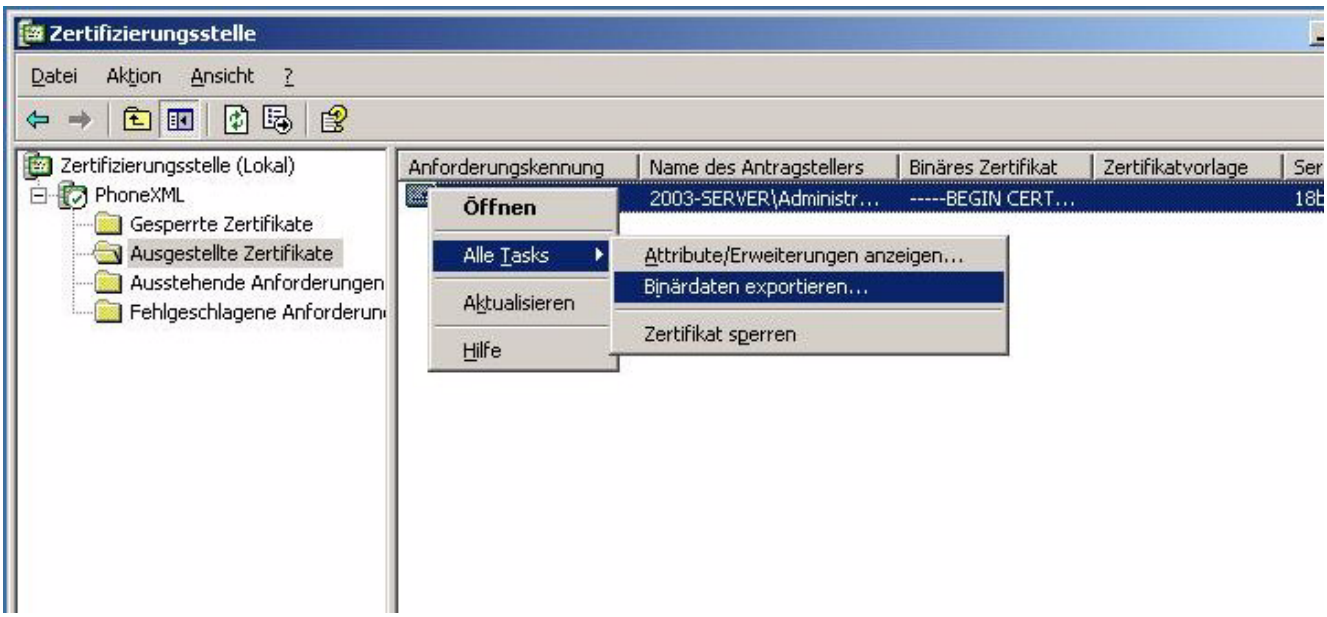


Suchen und wählen Sie die Anforderungsdatei aus. Mit der Schaltfläche **Öffnen** öffnen Sie die Zertifizierungsanforderungs-Datei.

Die Datei „zertifikatsanforderung.txt“ ist die Anforderungsdatei, die vorher im IIS erstellt wurde.



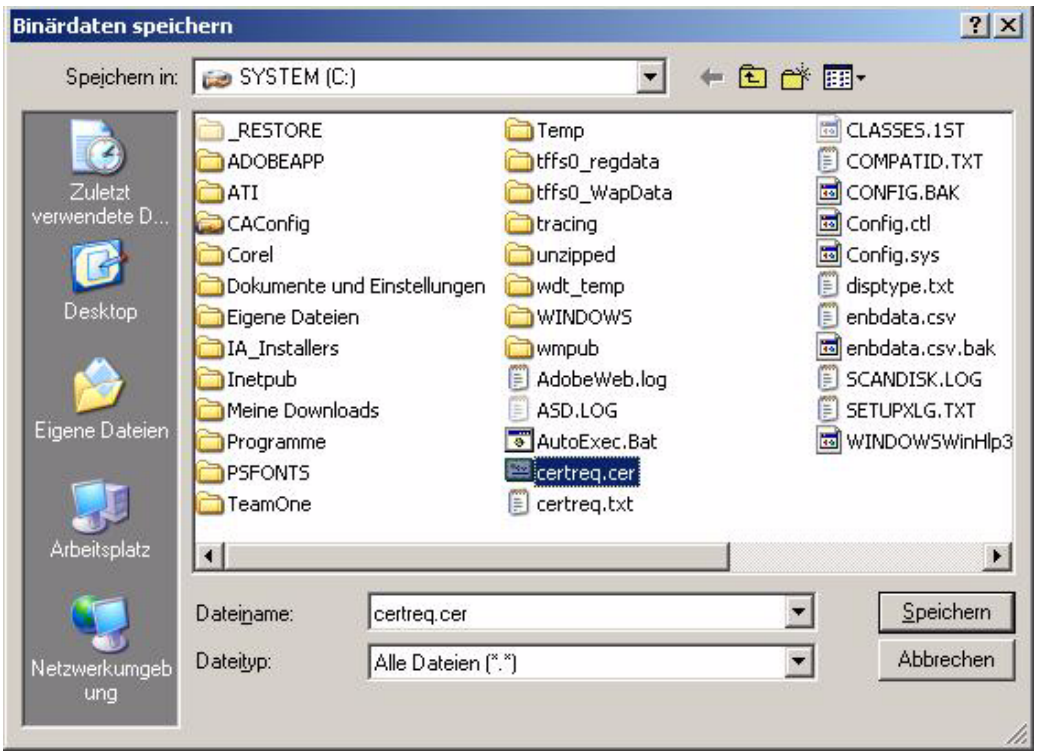
Selektieren Sie im linken Fenster **Ausstehende Anforderungen**. Klicken Sie im rechten Fenster auf die Anforderung und wählen Sie im Menü **Alle Tasks** die Funktion **Ausstellen**.



Selektieren Sie im linken Fenster “**Ausgesetllte Zertifikate**” Im rechten Fenster werden die entsprechenden Zertifikate aufgelistet. Klicken Sie im rechten Fenster auf das gewünschte Zertifikat und wählen Sie im Menü **Alle Tasks** die Funktion **Binärdaten exportieren...** .

Wählen Sie in der Liste **Binäres Zertifikat**, markieren Sie **Binärdaten in Datei speichern** und bestätigen Sie mit **OK**.

Wenn Sie sich das Zertifikat in Textform ansehen wollen, so wählen Sie die Option **Formatierte Textversion der Daten anzeigen**.

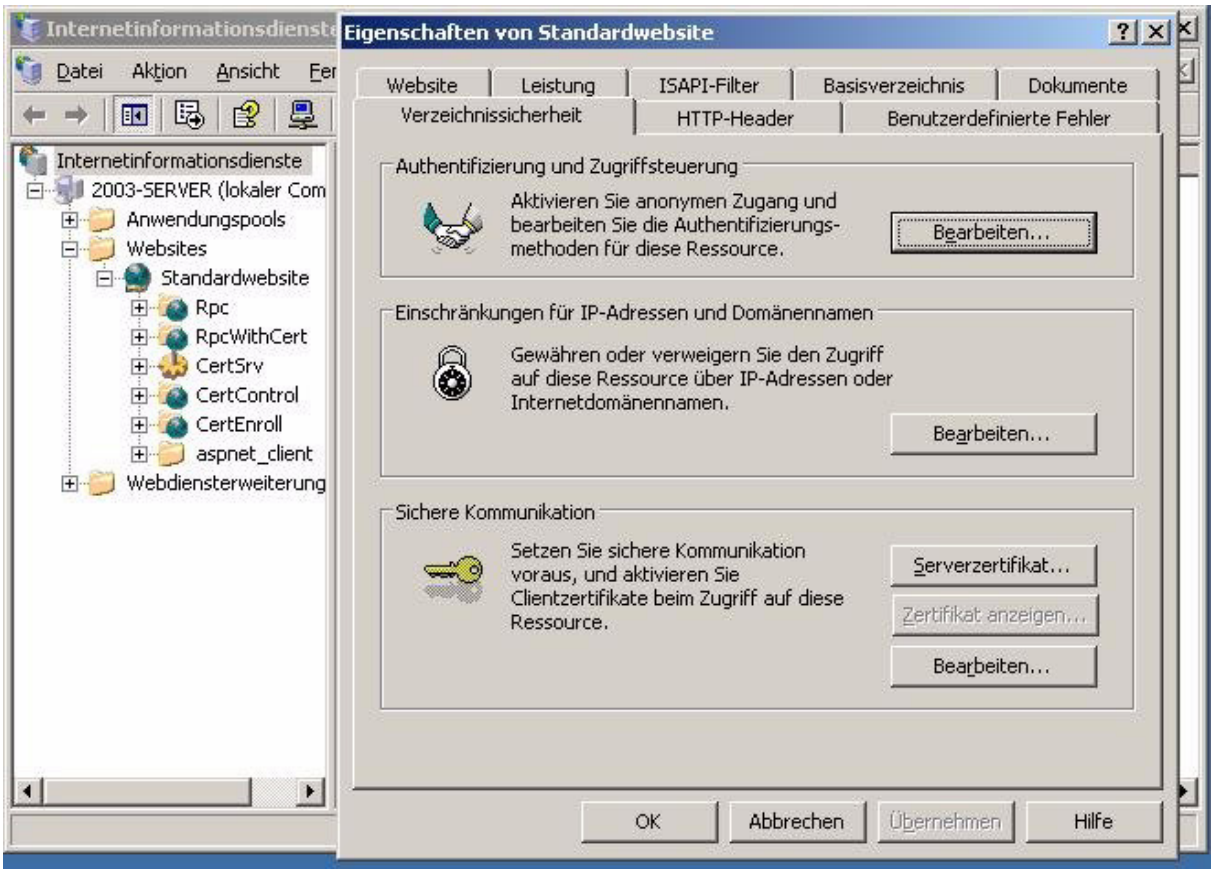


Wechseln Sie in das Verzeichnis, in das Sie das exportierte Zertifikat ablegen wollen. Geben Sie als Dateinamen eine aussagekräftige Bezeichnung ein und speichern Sie das Zertifikat.

Verwenden Sie für den Dateinamen den für Zertifikate gebräuchlichen Anhang **cer.**

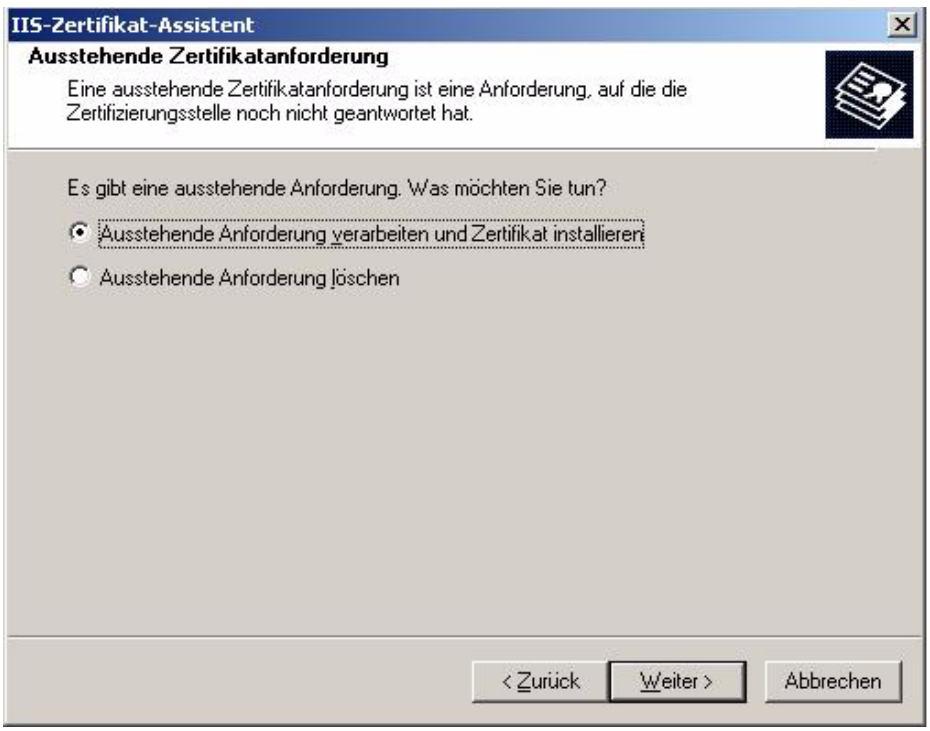
2.2.3 Serverzertifikat importieren und aktivieren

Rufen Sie im Menü **Verwaltung** die Anwendung **Internetinformationsdienste (IIS)** auf. Markieren Sie die gewünschte Website unter **Websites** (z. B. Standardwebsite) und öffnen Sie über die rechte Maustaste die **Eigenschaften** dieser Website.

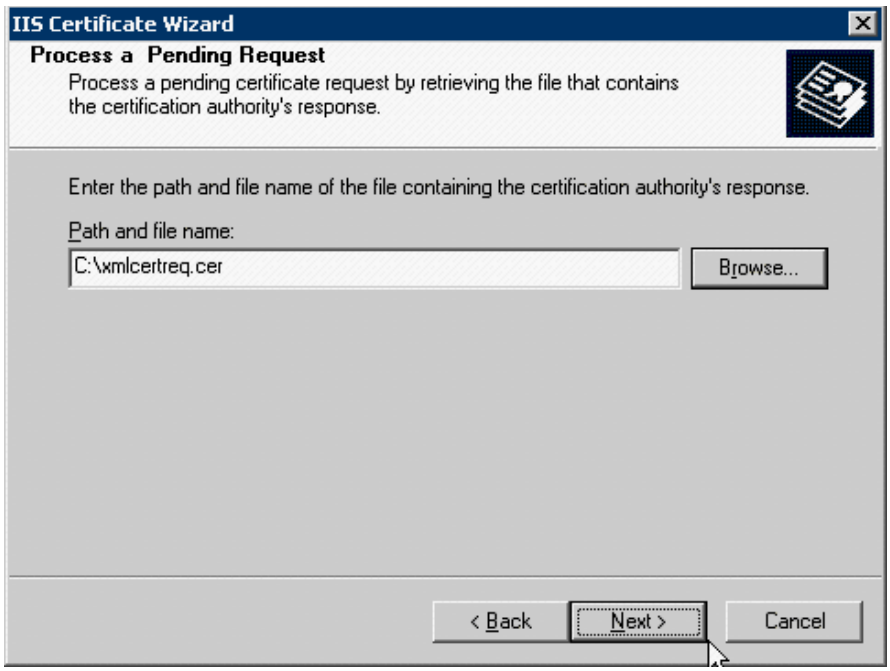


Wechseln Sie in das Register **Verzeichnissicherheit** und klicken Sie auf die Schaltfläche **Serverzertifikat...**

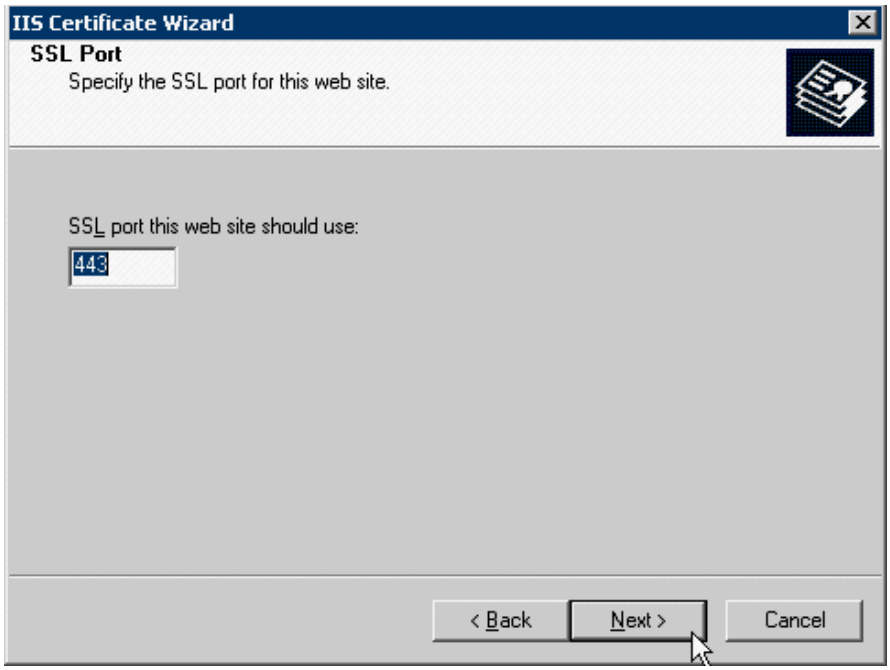
Im Startfenster des Assistenten auf **Weiter** klicken.



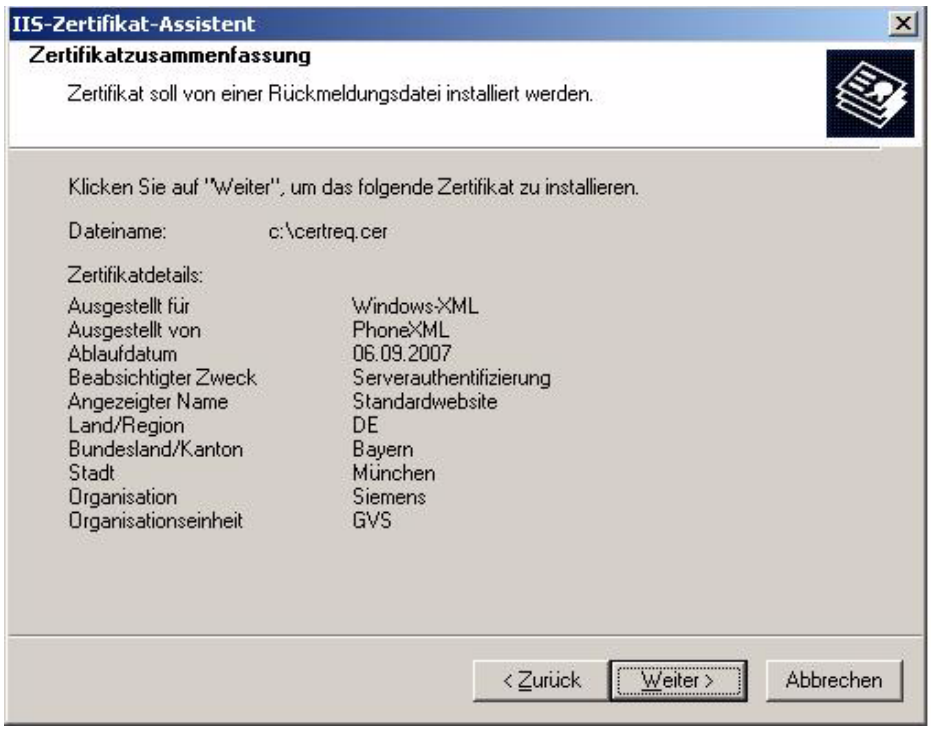
Markieren Sie die Option **Ausstehende Andorderung verarbeiten und Zertifikat installieren**”



Wechseln Sie zum Verzeichnis, in dem das Zertifikat abgelegt ist und klicken Sie auf **Weiter**.



Geben Sie den **SSL-Port, den diese Webseite verwenden soll** ein und klicken Sie auf **Weiter**

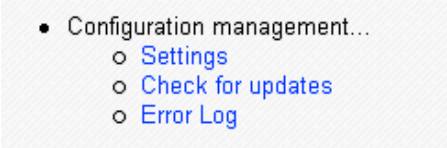


Überprüfen Sie die Parameter des Zertifikats und klicken Sie auf “**Weiter**

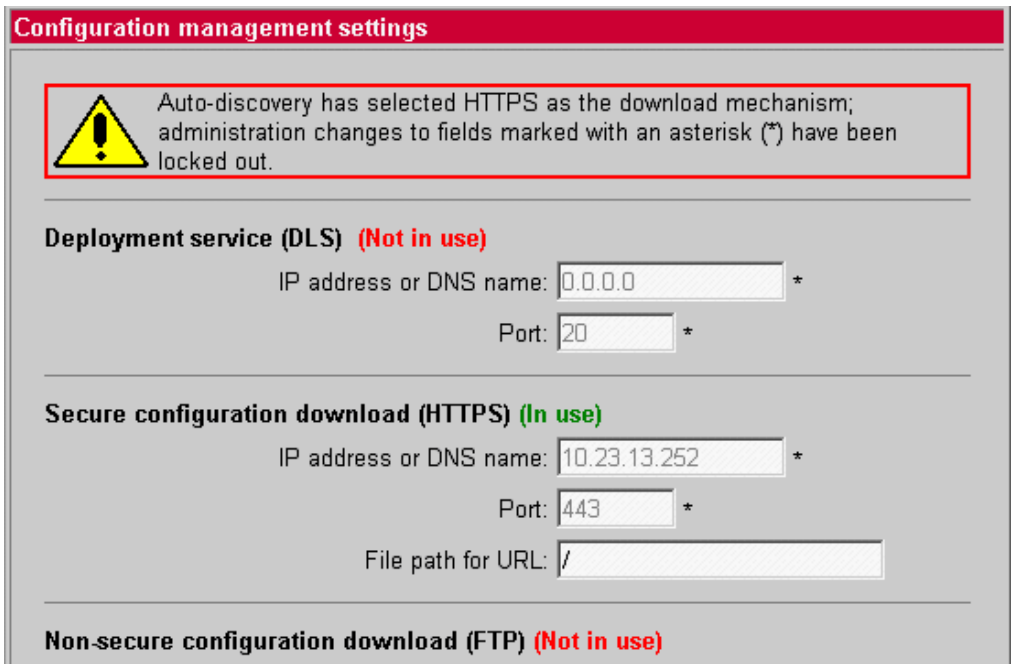
Beenden Sie mit **Fertig stellen**

2.3 Das Telefon für HTTPS-Vergindung einstellen

Rufen Sie die Web-Schnittstelle des betreffenden Telefon im Browser auf und öffnen Sie die Administrator-Seite.



Öffnen Sie im Administrator-Hauptmenü unter „Configuration management“ den Dialog „**Settings**“.

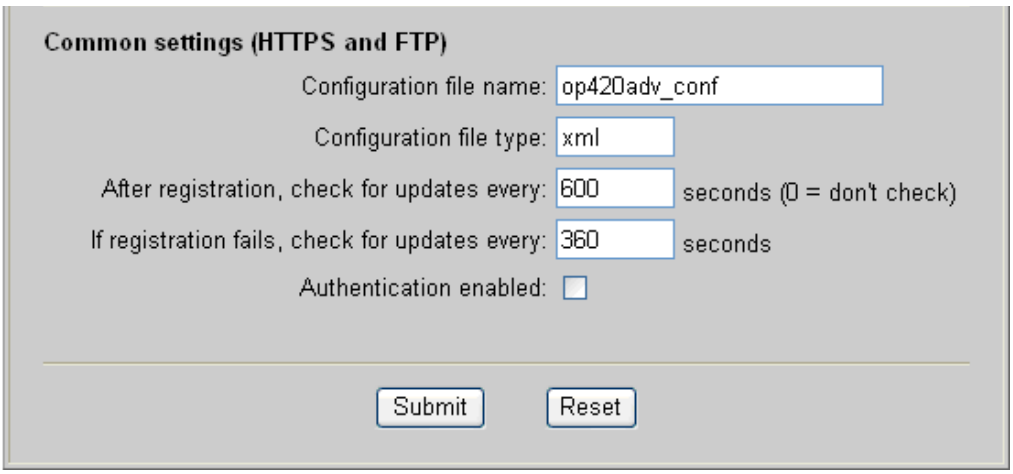


Im Bereich „**Secure configuration download (HTTPS)**“ geben Sie im **Feld**

- „**IP address or DNS name**“ die URL des gesicherten Web-Servers ein.
- „**Port**“ die Nummer, wie sie im Web-Server konfiguriert ist, ein (Voreinstellung für HTTPS-Port ist 443
- „**File path for URL**“ das Verzeichnis, in dem die XML-Dateien gespeichert sind. Sollten die XML-Dateien im Root-Verzeichnis des Web-Servers liegen, geben Sie einfach „/“ ein. In allen anderen Fällen muss der vollständige Pfad, beginnend beim Root-Verzeichnis, eingetragen werden.

Diese Konfiguration kann ggf. auch über einen DHCP-Server unter Verwendung von „herstellerspezifischen Informations-Element und/oder „Herstellerklassen“ erfolgen. In diesem Fall können die so übertragenen Informationen nicht über das Telefonmenü oder die Web-Schnittstelle geändert werden.

Format des „herstellerspezifischen Informations-Elements“: https://[base URL of link on Download Web Server][:Port#]



Der **Konfigurationsdateiname** ist der Name der Gerätedatei ohne Dateierweiterung. Die Benutzerdatei muss nicht konfiguriert werden weil der Benutzerdateiname aus Namen + der MAC-Adresse besteht (siehe XML-Dokumentation).

Der **Datei-Typ** ergibt sich aus der Dateierweiterung (Standard: „xml“).

Die Option „Authentication Enabled“ ermöglicht dem Telefon Konfigurationsdateien downzuloaden und sich damit anhand einer SIP NOTIFY Nachricht (check_sync) zu synchronisieren. Diese Option sollte nur aktiviert werden, wenn die Funktion vom SIP-Provider unterstützt wird.

Konfigurationsdateiname und **Konfigurationsdateityp** können nicht über DHCP versorgt werden.

2.3.1 Prüfen und testen der HTTPS-Verbindung

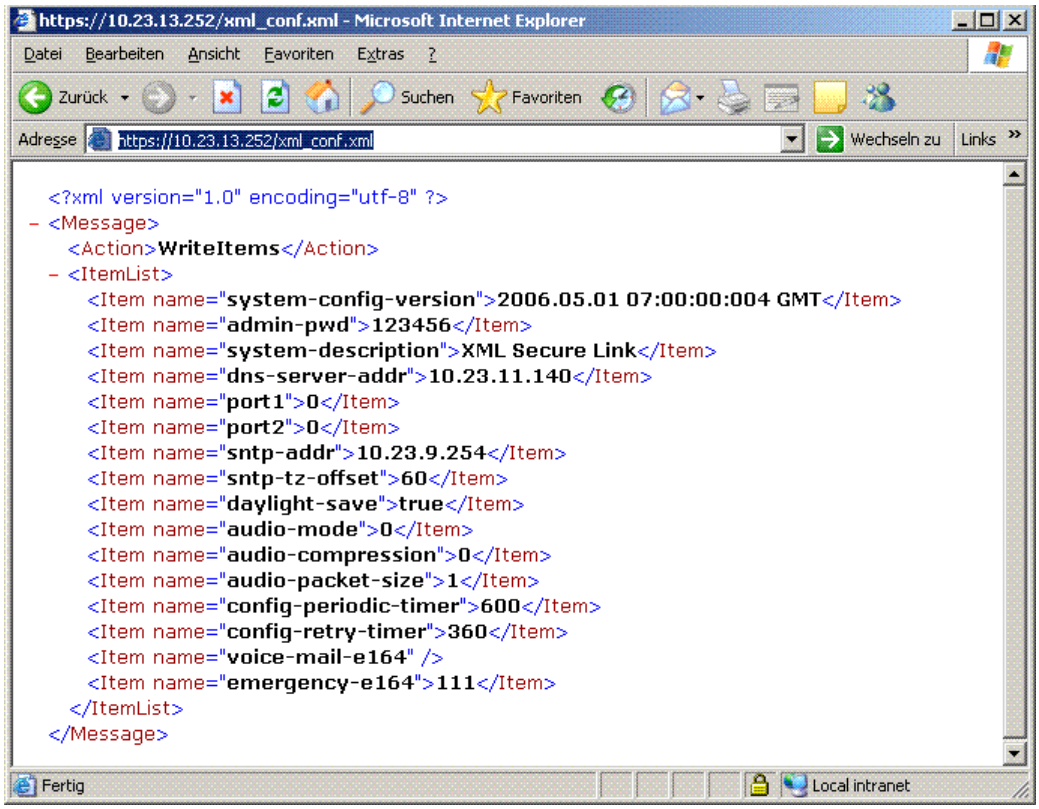
Um den XML Web-Server zu testen, müssen Sie den Browser öffnen und die IP-Adresse eingeben, die Sie in dem Dialog „Configuration management settings“ verwendet hatten. Wenn Sie jetzt noch den richtigen Dateinamen hinzufügen, sollten Sie den Inhalt der XML-Datei angezeigt bekommen.

Als Zieladresse ist folgendes einzugeben:

- https:// [IP XML web server]/[Name der Konfigurationsdatei + Dateierweiterung] für die Systemdatei und
- https:// [IP XML web server]/[Name der Konfigurationsdatei[MAC addr] + Dateierweiterung] für die Gerätedatei.

Nachdem Sie die erforderliche URL im Browser abgeschickt haben, erhalten Sie eine Warnmeldung – klicken Sie auf „Weiter“ um fortzufahren. Sie erhalten die Meldung deshalb, wie die eingegebene URL nicht mit der administrierte URL des Zertifikats übereinstimmt. Wenn alles funktioniert, können Sie auch sicher sein, dass der Web-Server richtig arbeitet und die Dateien zur Verfügung stehen.

Beispiel:



2.4 9: 802.1X Zertifikate in den XML-Konfigurationsdateien

In der SIP Version 6.0.xx ist es nicht möglich, den Passwortsatz an das Telefon als XML-Element zu senden, daher muss das Zertifikat mit einem speziellen Passwortsatz, der nur einigen Siemens-Mitarbeitern bekannt ist, kodiert werden.

So wie alle XML-Elemente sind auch die Zertifikate ganz normale Elemente, ändert sich jedoch der „Inhalt“ der XML-Datei, so führt das jedes Mal zu einem Neustart des Telefons. Das ist so, weil der XML-Parser im Telefon einen Neustart erzeugt, wenn er ein Zertifikat feststellt. Darum ist es empfehlenswert, das Zertifikat in die System-Konfigurationsdatei zu legen, weil bei normalen Operationen der Inhalt dieser Datei nicht so regemäßig geändert wird wie die Geräte-Konfigurationsdatei.

Das Server-Zertifikat muss im PEM-Format und das Client-Zertifikat im Binär-64-Format erstellt werden. Das Client-Zertifikat muss mit dem eingebauten Passwortsatz des Telefons verschlüsselt werden. Dieses Zertifikat kann deshalb nur vom Siemens-Fachpersonal in das B64-Format konvertiert werden.

Wenn der Kunde ein 802.1x Client-Zertifikat haben möchte, dann muss er das Client-Zertifikat im PK12-Format zusammen mit dem Passwortsatz übergeben. Dieses Client-Zertifikat muss in das erforderliche B64-Format mit dem eingebauten Passwortsatz des Telefons verschlüsselt werden kann anschließend dem Kunden wieder übergeben werden. Die Konvertierung kann in drei Schritten unter Verwendung von „OpenSSL“ nur vom Siemens-Fachpersonal vorgenommen (siehe Hinweis).

1. Einlesen der PK12-Datei und Konvertierung zu PEM (hier wird das PK12-Passwort des Kunden benötigt)

   OpenSSL> pkcs12 -in [Dateiname des vom Kunden angelieferten Zertifikats] -out certconv.pem

2. Rückkonvertierung der PEM-Datei in das P12-Format aber mit dem eingebauten Passwortsatz des Telefons

   OpenSSL>pkcs12 -export -in certconv.pem -out certnew.p12

3. Konvertierung der P12-Datei mit dem eingebauten Passwortsatz des Telefons in das erforderliche B64-Format.

   OpenSSL> base64 -in certnew.p12 -out [Vom Kunden gewünschter Dateiname].b64

Beachten Sie bitte die XML-Elemente in den Zertifikaten.

Beispiel eines Server-Zertifikats im PEM-Format:

```
<Item name="radius-server-ca1">
-----BEGIN CERTIFICATE-----
MIICrDCCAhWgAwIBAgIJANv25GBRph+iMA0GCSqGSIb3DQEBBAUAMIGKMQswCQYD
VQQGEwJERTEPMA0GA1UECBMGQmF5ZXJuMQ8wDQYDVQQHEwZNdW5pY2gxEDAOBgNV
BAoTB1NpZW1lbnMxEzARBgNVBAsTClN5c3RlbXRlc3QxDzANBgNVBAMTBkx1ZHdp
ZzEhMB8GCSqGSIb3DQEJARYSTHVkd2lnLnNpZW1lbnMuY29tMB4XDTA1MDYwODA5
MTk0MFoXDTA2MDYwODA5MTk0MFowgYsxCzAJBgNVBAYTAkRFMQ8wDQYDVQQIEwZC
YXllcm4xDzANBgNVBAcTBk11bmljaDEQMA4GA1UEChMHc2llbWVtczEUMBIGA1UE
CxMLZW5naW5lZXJpbmcxDzANBgNVBAMTBnNlcnZlcjEhMB8GCSqGSIb3DQEJARYS
c2VydmVyQHNpZW1lbnMuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCa
jFqWTqGOuwzb39NDjFnkomTFA6+8IlxKmbyTq+U6aW3RX88aWn1JbOcMH7sOz0kk
NkxBQO/ErnvMlwPEk11Lx4oexz+gpk63hlbi6jUs/ovraYyCl/sDqihXR6ldyHya
hiAfkZRzpdclrPzFtdX3ENE52j8KTdqdY0oWZabbUwIDAQABoxcwFTATBgNVHSUE
DDAKBggrBgEFBQcDATANBgkqhkiG9w0BAQQFAAOBgQAhbrtPB40v6xGrdfYDyy2s
nUBjsHhyB5yRIcZb2LX5aK9DmFPSF93Xj20XVOrQKIq5QjmnAidkPXQyNNNcYv4I
N06Ujy2YdnNdkJFX+ihQfnA5KzGYeVN2FMTh3RFvPF94HwNt1ry1jdza2ywj/h/g
keRyV/blKtcJeexS6kZOlg==
-----END CERTIFICATE-----</Item>
```

Beispiel eines Client-Zertifikats im B64-Format:

```
<Item name="802.1x-certifica-
te">MIIGqQIBAzCCBm8GCSqGSIb3DQEHAaCCBmAEggZcMIIGWDCCA1cGCSqGSIb3DQEH
BqCCA0gwggNEAgEAMIIDPQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI2IDu
BBdjnd4CAggAgIIDEEG9w263Sd2V1MYUHeUl1JTJ6BoMVk1B3q6+rix0MCfnR70a
aj9n1dP2ZJPXL1nRZJQ9QKvZrxoqrpR/v7NV+TSiOwRVqQH6NYo/AmKQlertFbde
ZYkBIkszjt2S9C9DhD/ACuZHw3cmHb3N3yqkQ6gjPwXFylfeYYuoasoxadn36Dr7
gu6cPEoG1B/EIemW67I7OB9BlbuWYGd/9aLX+G0mqoDDH2sx5gAU9nLR7XNw32A4
+HHFGzP/if0LCfIa47fK9QAwjDqsPesINE+cCBOqpG8kHH4VyvluvDl2xhs/Jomz
Rvc5S3d2qq//tc3nSS3TB0Dovdu8TDLTDk3J16bOZEKJlF8Y+N2sk6VbCV0exOIP
iMsqYLKQzSXYxdhY5mzeIwKkQvMzQMSz+LUlNjYk3R1KCpifZ1brtzXV6yPv9m68
HCUUlOSUSfCvKGlxjUH+UTXtsgkbpGvGQSNJI1mYhjB+WJ5ZAeHac0bJI9dYS2yt
OH0XiaRxeAX6QgcjSj1IeGmSCyMy8JuGH4LzJghvYz3p2AKYnIryYxM4QQ1aoQlx
w7lE2q9+PHspogtp2sU0jVsUFgkeSHo6pcSEwZutYElvekWo3PElnjBaSrt+Obxu
VEqC7EzlmBCcpVudPJdbCjbHZP0xtucisdBJG6QnUnendZqXnlShOCM2XYZjEj6m
pcZNkzCSRu98XB7KzoGFOotq5en8Jo+9lUEe1EeL7dkCg1fzajGzwcmJFYpUMth0
Mw8g2WIjuAe3BiMnhTIrNBflKpJrL5e8R70Jtz3b95YHKRCDntKAycJClzD0OfCi
coAX4WDN/37Hl+pWoO6iHu1+Z7VgjNBBfa44tltLxlZc/+sohBVettKDF+0/o5ws
f3MB0b8kqyHouQQMOYq5wYvTeQKW9OeJ5E1szIZYfc7K0MSr1p06wkt+Rgqu256Q
9lbOacoBBE96jRYZY8aYzuXbYcIuR+phDV3tgdAOsjLWIa4OZNge155hzf7aT3Wh
xcVrpywes80CdBHodg6IMLP6jPy4UfXHcicKSx0wggL5BgkqhkiG9w0BBwGgggLq
BIIC5jCCAuIwggLeBgsqhkiG9w0BDAoBAqCCAqYwggKiMBwGCiqGSIb3DQEMAQMw
DgQIcRC43gulfRoCAggABIICgCsL2VkVatmTyQx0732cstmsWTOHStSI57Zo9smD
```

kqtQrJ611n35+dK/FBUnqsvKuHCPScP4nLSZ4a5QNt4OcuzfnlPJvdqqPg4SOtMU
5ysq9dvH4xxvGi9/SzxyksrfQHroap4qZ5CAjt1nMFmu1w+GHhneEdOZZOzmOCQl
0rt98pJ5gO8LIIfm0bpHBrsrEqHAeSCavjd1qPJWBmbb+5Q1EPQBqZDK764zJxka
9ibYabgng+Ecq/6UODbUN6K8gQN5Ma6xAkS+/S1KCNwjkQzp07jy7bwSdL6rlewM
HzGFaDB1hRrcCnNH/sBfyEl28R8ixuBCv2GeUAQotipUq7CY/tDEA3mIfn8537MG
i5Ctt8vK+3i4LJJzmmqkk0juYaN2Bapad1aDZroVsxxkNtFjrDBMhIXDgB0PZTrf
XoyWeX/5zHIb5FNapW/VOJgbGg9Ch4irK/VqfismMNYfksy+VM+sDS5fUnsM0BEq
weraQPcwtzMwbCmaHJuS7YAKWDgk7QbeHC6YnUNUPQPSctGXL2GhTYugSztH/Znp
BkiX3jSh8XV35X2fg5QHGt0Ee36ylSzDeM+UZHzh8ML1RX7RMVe6eusVEN5uBcLu
hnIHuJg8hyp6LK8MF5JAAHkz0mZ0NisOdnj808dr+g/E1OAt5fLWXFMrZBkYQDPt
zz9gGSGkh0a8s6mCuyNevnw2eoMkayszrmTNaiF0ptekdf3iWThjx6XtVOr1ouqO
ob8SfiMqKEZL6HW5m+KVeeA2PdGEvb9UJIiWnpdhbTTjTXEpKARNy+NuFKqE4XiR
T5Ttxw3QPlBePjG06aoUP6z3m2aQiJX2RQ0AtxvyIMIkjegxJTAjBgkqhkiG9w0B
CRUxFgQUoTCMpc4uJFdVNVO/ENUBxDCvVYswMTAhMAkGBSsOAwIaBQAEFOz/l0MI
/CW+QKABtIZvuo5TD2j8BAgB6Z/fqKb2egICCAA=</Item>

3 Glossar

CA

siehe Zertifizierungsstelle

Certificate Authority

siehe Zertifizierungsstelle

Change-Cipher-Spec

Das Change-Cipher-Spec-Protokoll regelt den Wechsel einer neu ausgehandelten → Cipher suite

Cipher suite

Die Cipher-Suite enthält den verwendeten symmetrischen Verschlüsselungsalgorithmus, den Schlüsselaustauschalgorithmus, sowie die Hash-Funktion.

In den RFCs sind die möglichen Cipher-Suites definiert. Jede Cipher-Suite definiert mögliche Kombinationen aus Schlüsselaustausch- und Authentifizierungsalgorithmus, Verschlüsselungsalgorithmus (inklusive Schlüssellänge) und einem MAC-Algorithmus (HMAC). Eine Liste der Cipher-Suites welche der jeweilige Kommunikationsteilnehmer kennt wird zwischen den beiden Kommunikationspartnern ausgetauscht.

- MAC- Algorithmen sind: MD5 und SHA-1, wobei bei neueren Cipher-Suites MD5 nicht mehr verwendet wird.
- Schlüsselaustausch: RSA, DH-RSA, DH-DSS, Kerberos5 mit RFC2712, ECDH-ECDSA und ECDH-RSA als Draft
- Verschlüsselung: DES40-CBC, DES-CBC, 3DES-EDE-CBC, RC2-CBC-40, RC4-40, RC4-128, IDEA-CBC, AES-128-CBC und AES-256-CBC mit RFC 3268,

Client-Zertifikat

Ein Zertifikat, das sowohl einen öffentlichen als auch einen privaten Schlüssel enthält. Das Zertifikat ist im PK12-Format abgespeichert. (siehe auch → Server-Zertifikat)

Client Key Exchange

Dient zur Übermittlung des Master Key und ist mit public key des Servers verschlüsselt. Anschließend werden aus dem Master Key in Abhängigkeit der ausgewählten Verschlüsselungsverfahren neue Schlüssel erzeugt. Dazu werden für jedes Verschlüsselungsverfahren spezifische Algorithmen benutzt. Diese sind in der SSL Spezifikation enthalten.

CSR

Certificate Signing Request. Anforderungsdatei für die Signierung durch eine Zertifizierungsstelle.

IIS

HTTP-Server der Firma Microsoft

Layer 2 Switch

Ein auf MAC-Adressen basierter Switch (OSI-Modell Schicht 2)

Public Key Infrastruktur (PKI)

Eine Infrastruktur öffentlicher Schlüssel ist eine Kombination von Software, Verschlüsselungstechnologien und Diensten, für den Umgang mit öffentlichen Schlüsseln. Eine PKI sollte folgende Funktionen zur Verfügung stellen:

- Zertifizierungsstellen, die Zertifikate ausstellen und zurückziehen können
- Zertifikatsveröffentlichungsstellen, bei denen Zertifikate zum Nachschlagen hinterlegt sind
- Tools für die Schlüssel- und Zertifikatsverwaltung
- Programme und Anwendungen, die öffentliche Schlüssel verwenden können

RADIUS

RADIUS ist ein Protokoll, das zu Autorisierungszwecken in verteilten RAS-Lösungen eingesetzt wird. Es erlaubt den Austausch von Authentifizierungs-, Autorisierungs- und Konfigurationsdaten zwischen einem zentralen Autorisierungsserver und den dezentralen Network Access Servern (NAS). Der NAS arbeitet als Client des Radius-Servers. Wählt sich ein entfernt arbeitender Nutzer in den NAS ein, so stellt dieser eine Anfrage mit Benutzername, Passwort, NAS-ID und Port-ID. Der Server überprüft die Angaben und die eventuell festgelegten Anforderungen an die Session und die Dienst-Ports anhand der RADIUS-Datenbank. Dies gestattet es, für jeden Benutzer getrennt bestimmte höhere IP-Protokolle zu erlauben oder zu verbieten und dies zentral zu administrieren.

Server-Zertifikat

Ein Zertifikat, das den öffentlichen Schlüssel enthält. Das Zertifikat ist im PEM-Format abgespeichert (siehe auch → Client-Zertifikat).

Server Policy

Satz von Regeln in der Server-Konfiguration.

Session key

Wird auch Sitzungsschlüssel oder Einmalschlüssel genannt. Für eine verschlüsselte Übertragung benutzter Schlüssel, der nur für eine kurze Zeit (eine Session oder eine Übertragung) gültig ist. In der Regel werden solche Schlüssel in hybriden Verschlüsselungssystemen eingesetzt. Mit dem zufällig gebildeten Session-Key wird eine Nachricht symmetrisch verschlüsselt. Danach wird der Session-Key asymmetrisch mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und an die Nachricht angehängt. Der Empfänger benutzt seinen geheimen Schlüssel, um den Session-Key wieder zu entschlüsseln und damit die eigentliche Nachricht wieder lesbar zu machen.

Die Verwendung von Session-Keys ermöglicht daher, die Vorteile von symmetrischer und asymmetrischer Verschlüsselung zu koppeln. Die Sicherheit von Verfahren, die mit Session-Keys arbeiten, hängt wesentlich davon ab, dass die Session-Keys wirklich zufällig gebildet werden.

TLS resume method

Wiederherstellung einer TLS-Verbindung.

X.509

X.509 ist ein ITU-T-Standard für eine Public- Key-Infrastruktur und derzeit der wichtigste Standard für digitale Zertifikate. Die aktuelle Version ist X.509v3 (wie in [RFC3280] definiert).

Zertifizierungsstelle

Eine Zertifizierungsstelle (englisch Certificate Authority, kurz CA) ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist gewissermaßen das Cyberspaceäquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie sie mit ihrer eigenen digitalen Unterschrift versieht.

Die Zertifikate enthalten „Schlüssel“ und Zusatzinformationen, die zur Authentifizierung sowie zur Verschlüsselung und Entschlüsselung sensitiver oder vertraulicher Daten dienen, die über das Internet und andere Netze verbreitet werden. Als Zusatzinformationen sind zum Beispiel Lebensdauer, Verweise auf Zertifikatsperrlisten, etc. enthalten, die durch die CA mit in das Zertifikat eingebracht werden.

Die Aufgabe einer Beglaubigungsinstitution ist es, solche digitalen Zertifikate herauszugeben und zu überprüfen. Sie ist dabei für die Bereitstellung, Zuweisung und Integritätssicherung der von ihr ausgegebenen Zertifikate verantwortlich. Damit ist sie ein wichtiger Teil der Public-Key-Infrastruktur.

Eine Zertifizierungsstelle kann sowohl eine spezielle Firma darstellen (z. B. GlobalSign / Cybertrust VeriSign) oder eine Institution innerhalb einer Firma, die einen eigenen Server installiert hat (ein Beispiel hierfür ist der Microsoft Certificate Server). Auch öffentliche Organisationen oder Regierungsstellen können als Zertifizierungsstelle dienen, z.B. die Bundesnetzagentur.

4 Abkürzungen

Diese Liste enthält für das Thema übliche Abkürzungen.

Abkürzung	Definition
DHCP	Dynamic Host Configuration Protocol.
DLS	Deployment and Licensing Service
DNS	Domain name server
EAP	**E**xtensible **A**uthentication **P**rotocol
EAPOL	**E**xtensible **A**uthentication **P**rotocol **O**ver **L**AN
FTP	**F**ile **T**ransfer **P**rotocol“.
IAS	Internet Authentication Service
IETF	Internet Engineering Task Force; Internet standards body
IIIS	Internet Information Server
IP	Internet Protocoll
PEAP	**P**rotected **E**xtensible **A**uthentication **P**rotocol
RFC	Request For Comments; A IETF Protocol Specification
TAP	**T**echniker **A**rbeits**P**latz (Meist ein speziell mit Soft- und Hardware ausgestattetes Notebook des Technikers.)
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
VID	Virtual LAN ID (0-4095)
VLAN	Virtual LAN

www.siemens.de/hipath

Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können.
Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.
Die verwendeten Marken sind Eigentum der Siemens AG bzw. der jeweiligen Inhaber.

CE Die Konformität des Gerätes zu der EU-Richtlinie 1999/5/EG wird durch das CE-Kennzeichen bestätigt.

Dieses Gerät wurde nach unserem zertifizierten Umweltmanagementsystem (ISO 14001) hergestellt.
Dieser Prozess stellt die Minimierung des Primärrohstoff- und des Energieverbrauchs sowie der Abfallmenge sicher.

Hofmannstraße 51 • D-81359 München
Bestell-Nr.: A31003-J4260-M102-1-A9 unverbindlicher Vorabzug
Liefermöglichkeiten und technische Änderungen vorbehalten.