

Installation eines SSL Zertifikates am Microsoft IIS 5.0 v0.4

Table of Contents

1.1 Allgemeiner Hinweis	1
1.2 Erstellen eines Zertifikatsantrages im IIS 5.0	1
1.3 Einfügen des Zertifikates im Webserver	2
1.4 Testen und einrichten von SSL	2
1.5 Screenshots zur Installation	3

1.1 Allgemeiner Hinweis

Diese Dokumentation dient als Untertützung bei der Beantragung und Installation eines a.sign corporate SSL Zertifikates. Sie erreichen den Internetdienste Manager über den Arbeitsplatz dort rechte Maustaste „Verwalten“ oder über die MMC Konsole (mmc.exe) welche über die Eingabeaufforderung aufrufbar ist.

1.2 Erstellen eines Zertifikatsantrages im IIS 5.0

1. Öffnen Sie den Internetdienste-Manager oder die angepasste MMC, die das Internet-Informationdienste-Snapin enthält.
2. Blenden Sie die Internet-Informationdienste ein (falls erforderlich) und blättern Sie zu der Website, für die Sie eine ausstehende Zertifikatsanfrage haben. Siehe Abbildung 1)
3. Klicken Sie mit der rechten Maustaste auf die Site und dann auf "Eigenschaften".
4. Klicken Sie auf das Register "Verzeichnissicherheit".
5. Klicken Sie unter "Sichere Kommunikation" auf "Serverzertifikat".
6. Klicken Sie im Website-Zertifikat-Assistenten auf "Weiter".
7. Entscheiden Sie sich, ein neues Zertifikat zu erstellen (siehe Abbildung 2). Klicken Sie auf "Weiter".
8. Wählen Sie „Anforderung jetzt vorbereiten, aber später senden“(siehe Abbildung 3). Klicken Sie auf „Weiter“.
9. Wählen Sie einen eindeutigen Namen für das Zertifikat aus und mindestens 1024 Bit als Schlüssellänge. (siehe Abbildung 4) Klicken Sie auf „Weiter“.
10. Geben Sie ihre Organisation und die Organisationseinheit ein (siehe Abbildung 5), klicken Sie auf „Weiter“.
11. Wählen Sie den CN (Common Name) für die Site aus (siehe Abbildung 6). Dieser muss dem exakten Wortlaut ihrer Website entsprechen. zB: www.mustermann.com Klicken Sie auf „Weiter“.
12. Sie sehen eine Bestätigung. Wenn Sie diese Informationen gelesen haben, klicken Sie auf "Weiter".
13. Nach dem Abschließen des Antrages öffnen sie die certreq.txt Datei und fügen den Inhalt ihrer Zertifikatsbestellung bei. (Die Bestellformular finden Sie unter <https://www.a-trust.at/html/produkte/a-sign-corporate/websrvcert.asp>)

1.3 Einfügen des Zertifikates im Webserver

https://www.a-trust.at/html/ocsp_srvcrt_verify.asp?d=www.mustermann.com

Die Antwort-Email von A-Trust enthält:

1. Den signierten Certificate-Request (das Zertifikat mit der Endung .cer oder .crt)
2. Informationen über die zugehörigen Stammzertifikate
3. Informationen, wie das verify Logo auf Ihrer Webseite plaziert werden kann
4. Einen Link zur Überprüfung der Gültigkeit ihres Zertifikates (https://www.a-trust.at/html/ocsp_srvcrt_verify.asp?d=www.mustermann.com)

Nun können Sie den Zertifikatsantrag abschließen. Dies geschieht wie folgt:

1. Öffnen Sie den Internetdienste-Manager oder die angepasste MMC, die das Internet-Informationdienste-Snapin enthält.
2. Blenden Sie die Internet-Informationdienste ein (falls erforderlich) und blättern Sie zu der Website, für die Sie eine ausstehende Zertifikatanfrage haben.
3. Klicken Sie mit der rechten Maustaste auf die Site und dann auf "Eigenschaften".
4. Klicken Sie auf das Register "Verzeichnissicherheit".
5. Klicken Sie unter "Sichere Kommunikation" auf "Serverzertifikat".
6. Klicken Sie im Website-Zertifikat-Assistenten auf "Weiter".
7. Entscheiden Sie sich, die ausstehende Anforderung zu bearbeiten und das Zertifikat zu installieren (siehe Abbildung 8). Klicken Sie auf "Weiter".
8. Geben Sie den Speicherort der Zertifikatsantwortdatei (.cer oder .crt aus Mail) an und klicken Sie dann auf "Weiter".
9. Lesen Sie die Zusammenfassung, um sicherzustellen, dass Sie das richtige Zertifikat bearbeiten, und klicken Sie dann auf "Weiter".
10. Sie sehen eine Bestätigung. Wenn Sie diese Informationen gelesen haben, klicken Sie auf "Weiter".

1.4 Testen und Einrichten von SSL

Sie haben jetzt ein Serverzertifikat installiert. Wenn SSL für alle Webdienste in einem gegebenen virtuellen Verzeichnis eingesetzt werden soll, klicken Sie mit der rechten Maustaste auf das virtuelle Verzeichnis, danach auf „Eigenschaften“ und dann auf die Registerkarte „Verzeichnissicherheit“.

Klicken Sie unter „Sichere Kommunikation“ auf „Bearbeiten“.

Das Kontrollkästchen Sicheren Kanal verlangen (SSL) ist standardmäßig deaktiviert. Aktivieren Sie es, um SSL zu verlangen. SSL unterstützt sowohl 40-Bit- als auch 128-Bit-Verschlüsselung. Je mehr Bits bei der Verschlüsselung verwendet werden, desto schwieriger ist es, die Originaldaten unbefugt zu entschlüsseln.

Den SSL Port (standardmäßig ist 443 eingestellt) können Sie unter den Eigenschaften der Website im Karteireiter „Website“ überprüfen/ändern.

Folgende Punkte müssen noch angepasst werden:

1. Links ggf. von http auf „https“ ändern.
2. Kunden die Information mitteilen, dass nun <https://IhreDomain> möglich oder zwingend ist
3. Login/Passwort durch Client-Zertifikate ersetzen

Hinweis: Die Antwortdatei enthält Ihren öffentlichen Schlüssel, der von A-Trust signiert wurde. Damit ein Client-Computer erfolgreich eine Verbindung zu Ihrer Site (mittels SSL/TLS) aufbauen kann, muss er auch dieser Stammzertifizierungsstelle vertrauen. Wenn Sie Certificate Server 2.0 verwenden, müssen Sie das Stammzertifizierungsstellen-Zertifikat (CA-Zertifikat) auf dem Client-Computer installieren.

1.5 Screenshots zur Installation

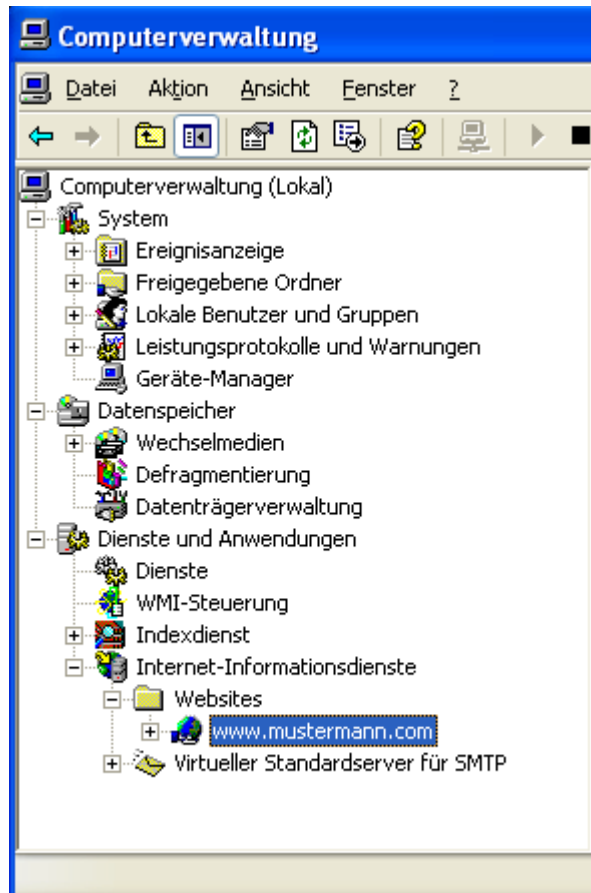


Abbildung 1: Website öffnen für die das Zertifikat laufen soll.

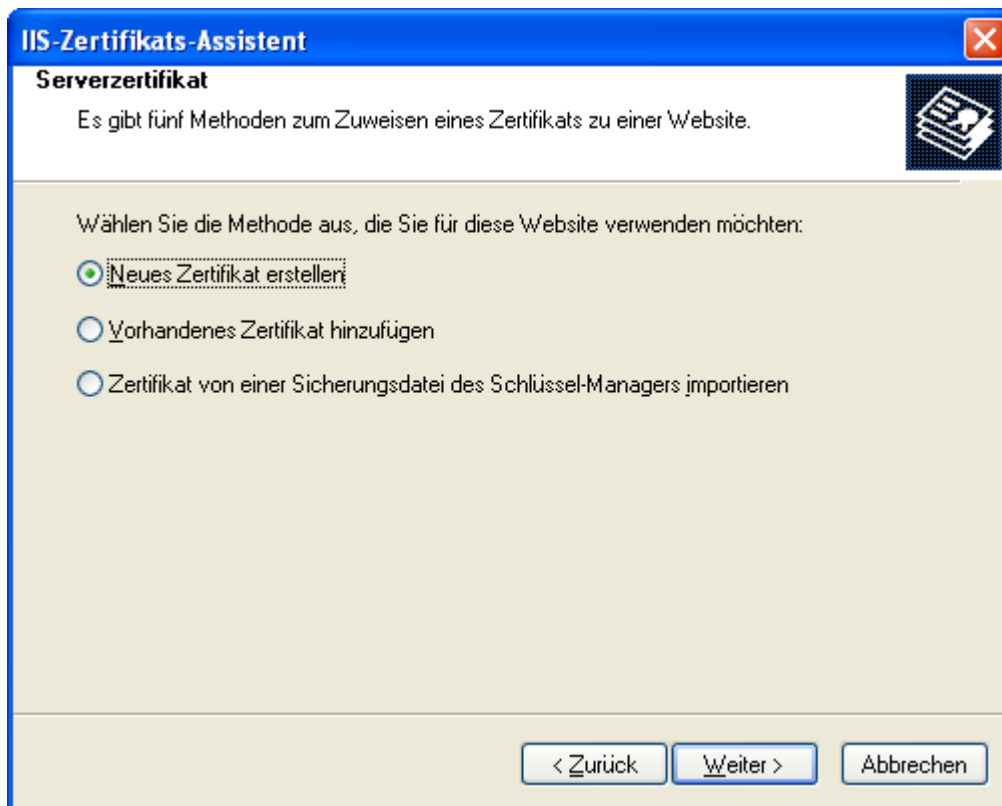


Abbildung 2: Zertifikatserstellung

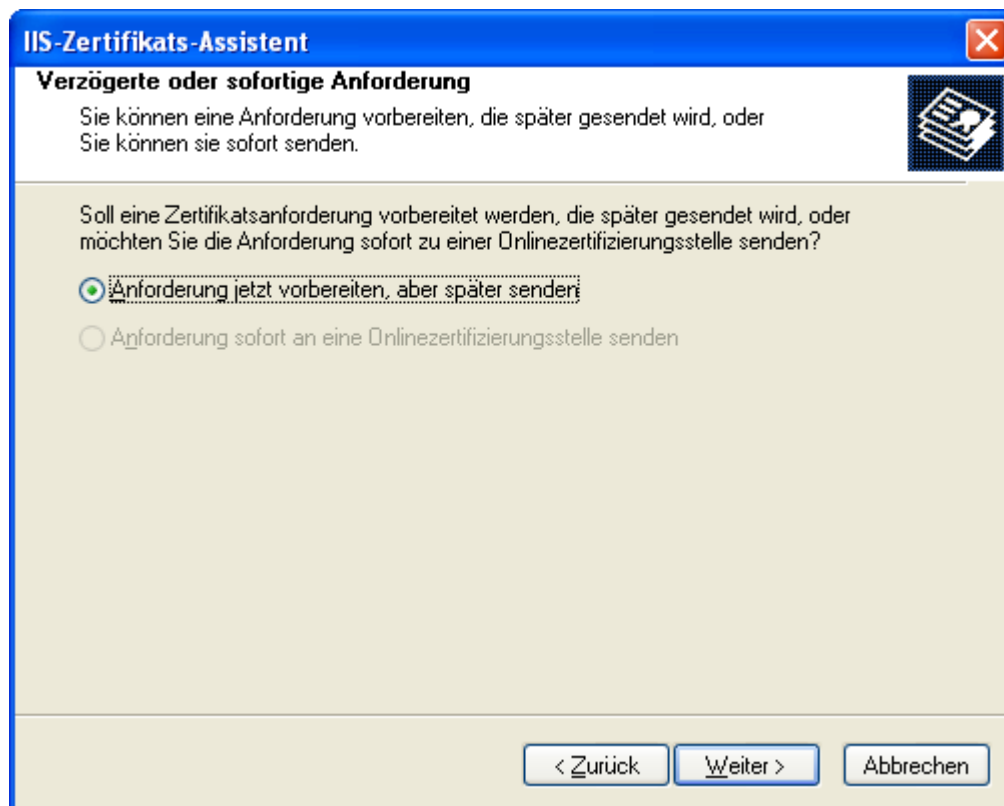


Abbildung 3: Die Anforderung vorbereiten

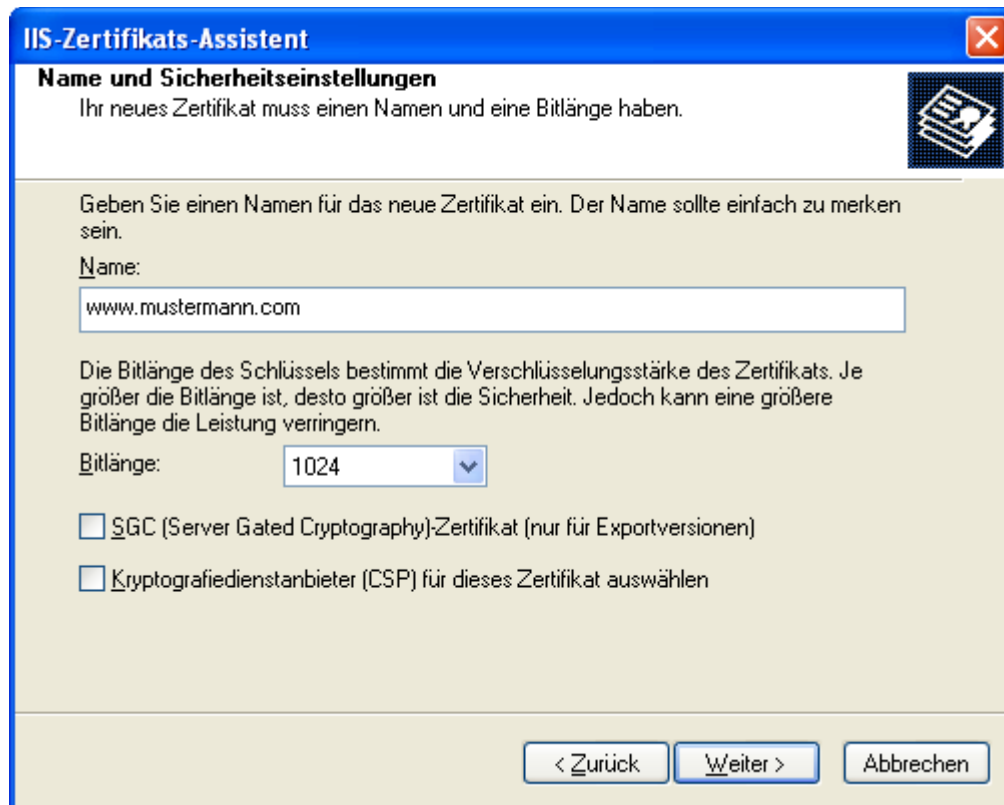
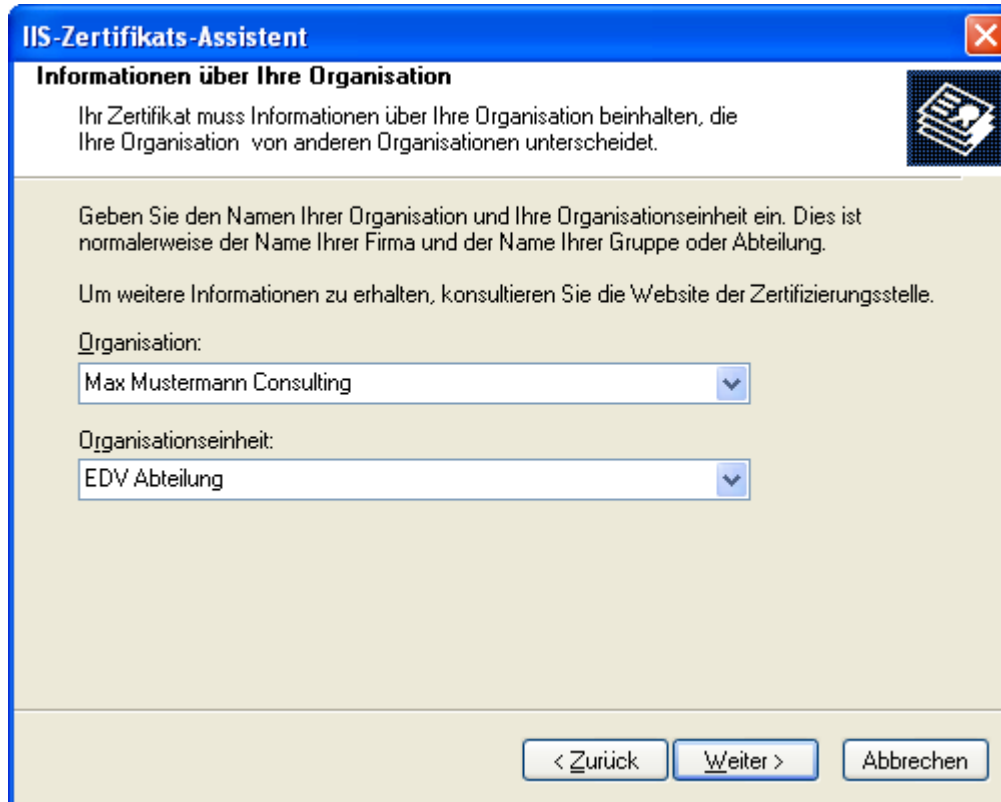


Abbildung 4: Auswählen des Zertifikatnamens



IIS-Zertifikats-Assistent

Informationen über Ihre Organisation

Ihr Zertifikat muss Informationen über Ihre Organisation beinhalten, die Ihre Organisation von anderen Organisationen unterscheidet.

Geben Sie den Namen Ihrer Organisation und Ihre Organisationseinheit ein. Dies ist normalerweise der Name Ihrer Firma und der Name Ihrer Gruppe oder Abteilung.

Um weitere Informationen zu erhalten, konsultieren Sie die Website der Zertifizierungsstelle.

Organisation:
Max Mustermann Consulting

Organisationseinheit:
EDV Abteilung

< Zurück Weiter > Abbrechen

Abbildung 5: Auswahl der Organisation

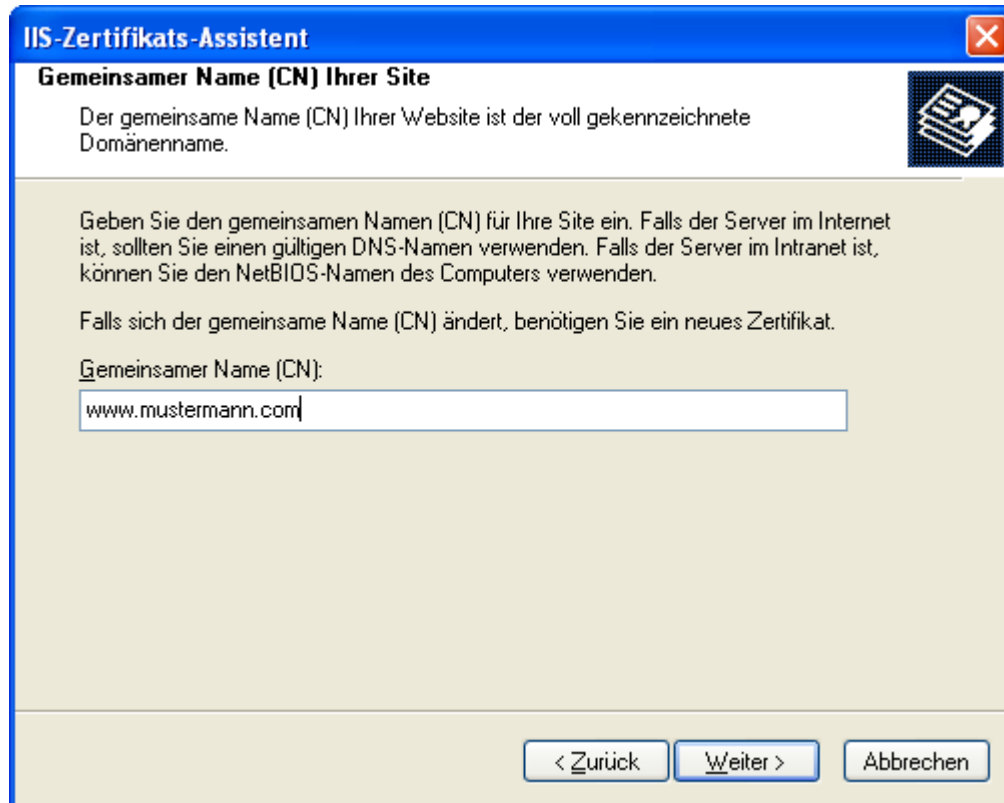
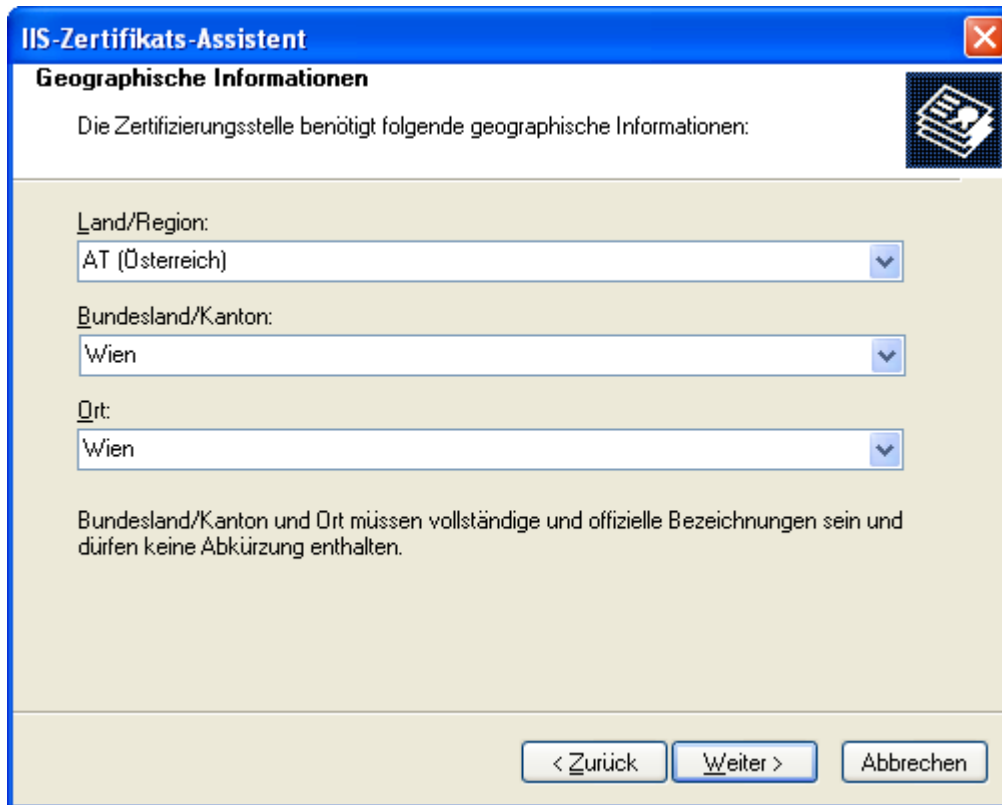


Abbildung 6: Eintragen des Common Names



IIS-Zertifikats-Assistent

Geographische Informationen

Die Zertifizierungsstelle benötigt folgende geographische Informationen:

Land/Region:
AT (Österreich)

Bundesland/Kanton:
Wien

Ort:
Wien

Bundesland/Kanton und Ort müssen vollständige und offizielle Bezeichnungen sein und dürfen keine Abkürzung enthalten.

< Zurück Weiter > Abbrechen

Abbildung 7: Angabe der Geographischen Informationen

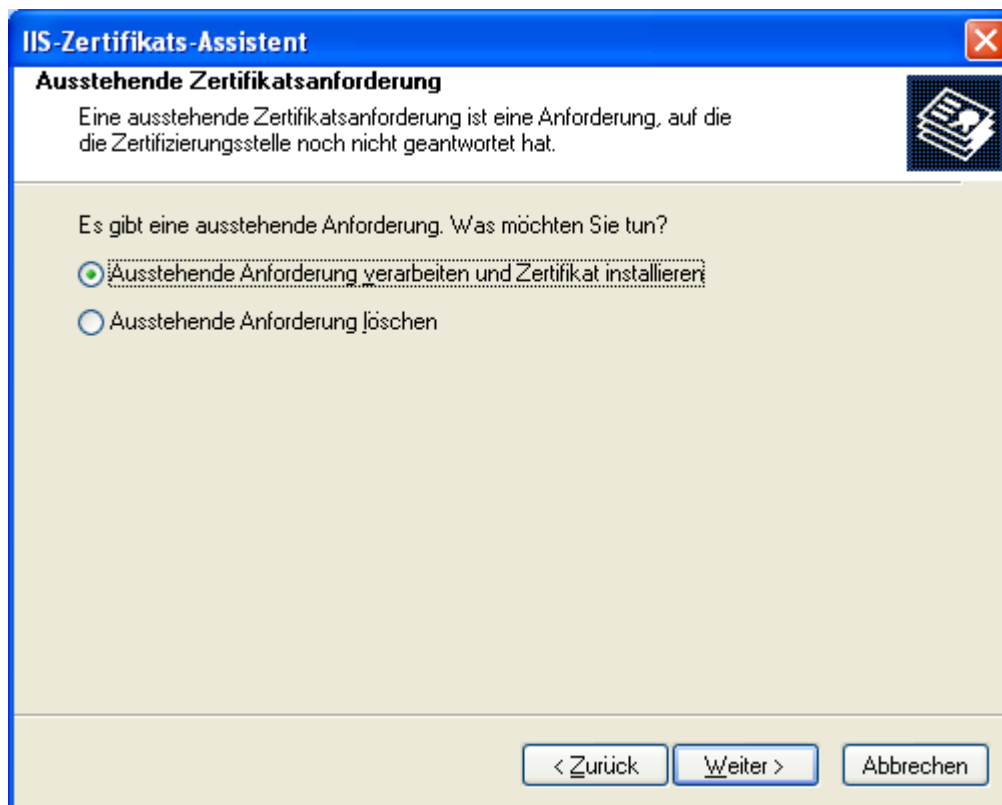


Abbildung 8: Zertifikat auswählen und installieren.