

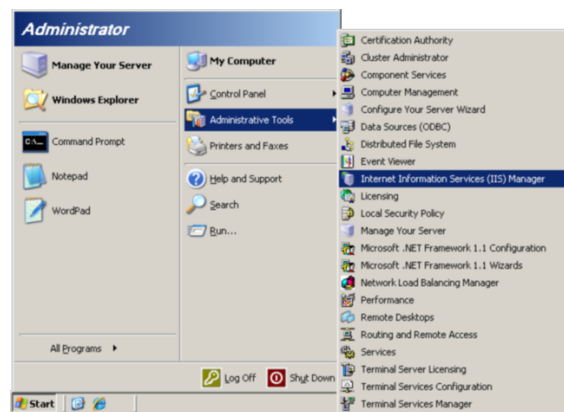
SSL-geschützte Verbindungen mit dem "Internet Information Server" (IIS) unter Windows Server 2003

Dieses Dokument beschreibt, wie man mit dem IIS Zertifikatanträge (CSRs) erzeugt und aufgrund des CSR von der DFN-PKI generierte Zertifikate in den IIS einspielt.

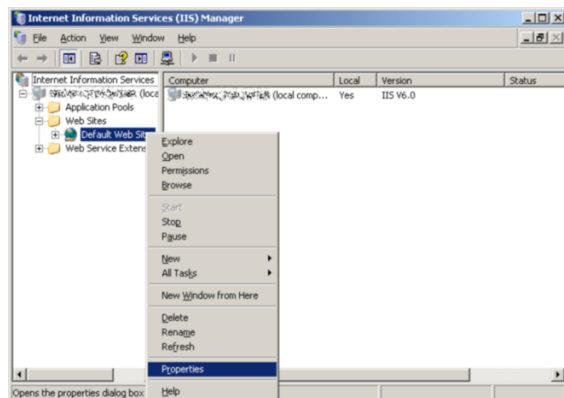
Die hier gezeigten Bildschirmfotos sind mit einer englischen Version des Windows Server 2003 entstanden, die Vorgehensweise ist jedoch bei Windows Server 2008 und mit lokalisierten Versionen vergleichbar.

1. Zertifikatsantrag erzeugen

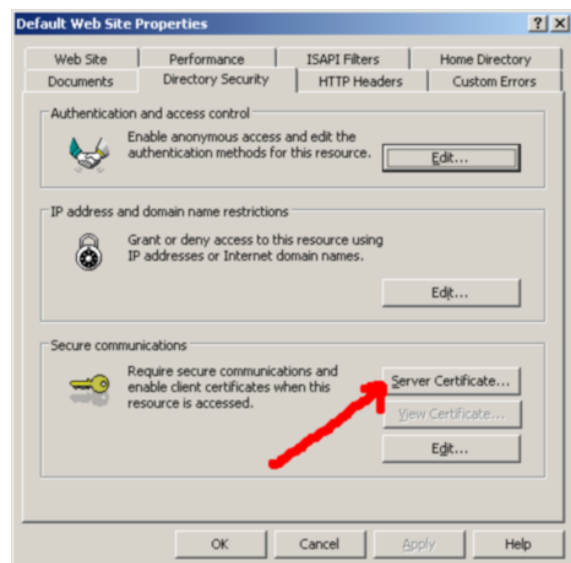
Starten Sie die Management-Oberfläche des IIS:



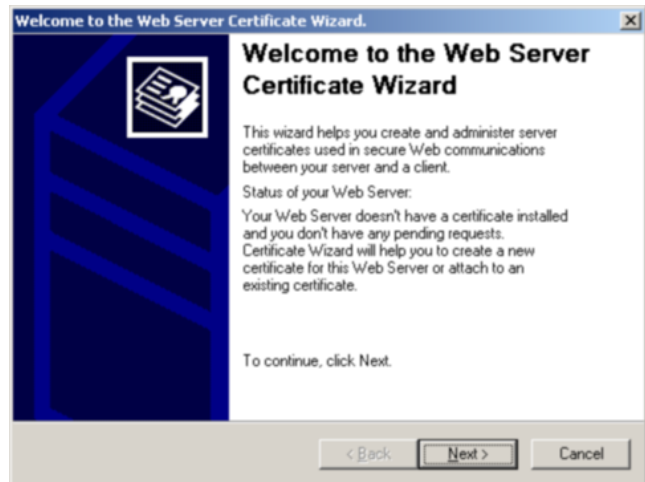
Wählen Sie mit der rechten Maustaste den gewünschten Webserver und in dem erscheinenden Aufklappmenü den Punkt "Properties":



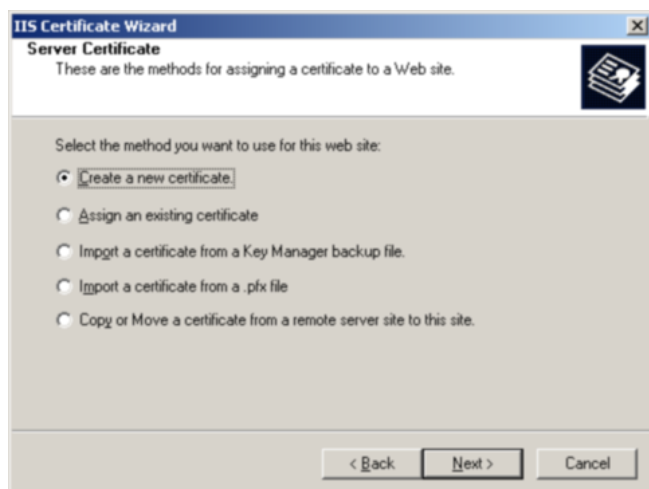
Wählen Sie im Karteireiter "Directory Security" die Aktion "Server Certificate":



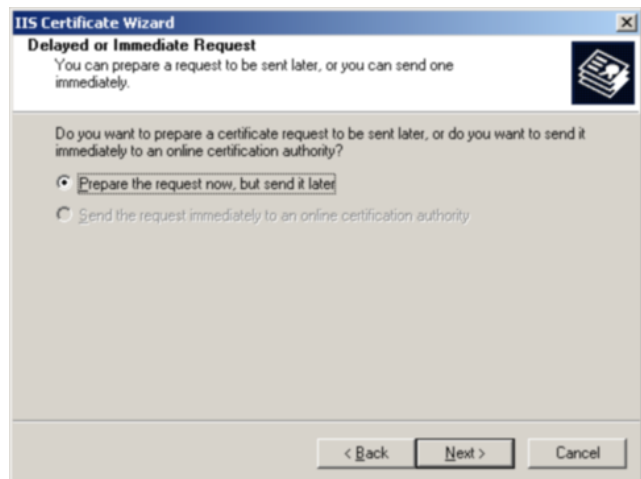
Der "Web Server Certificate Wizard" wird gestartet. Fahren Sie mit "Next" fort:



Wählen Sie "Create a new certificate" und bestätigen Sie mit "Next":



Wählen Sie "Prepare the request..." und bestätigen Sie mit "Next":



Vergeben Sie einen (beliebigen) Namen, unter dem das Zertifikat im IIS bekannt gemacht werden soll. Setzen Sie die Schlüssellänge unbedingt auf 2048:

IIS Certificate Wizard
Name and Security Settings
Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name:
Meine Website

The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length: 2048

Select cryptographic service provider (CSP) for this certificate

< Back Next > Cancel

Geben Sie bei "Organization" "Universitaet Passau" exakt ein und bei "Organizational unit" den Namen Ihrer Einrichtung, z. B. "Lehrstuhl für Sicherheit":

IIS Certificate Wizard
Organization Information
Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization:
Universitaet Passau

Organizational unit:
Einrichtungname

< Back Next > Cancel

Als "Common name" geben Sie den vollständigen Namen Ihres Servers ein, unter dem er im Internet bekannt ist:

IIS Certificate Wizard
Your Site's Common Name
Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:
meinserver.einrichtung.uni-passau.de

< Back Next > Cancel

Als "Geographical Information" geben Sie bitte "DE (Germany)", "Bayern", "Passau" an, wie rechts dargestellt:

IIS Certificate Wizard
Geographical Information
The certification authority requires the following geographical information.

Country/Region:
DE (Germany)

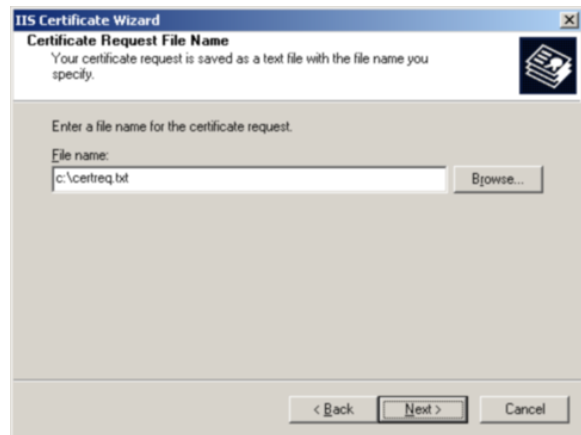
State/province:
Bayern

City/locality:
Passau

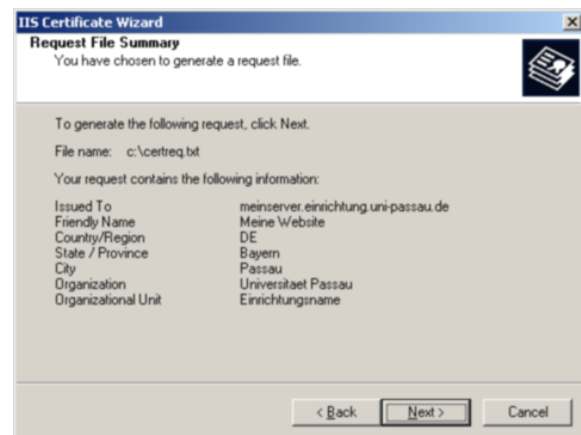
State/province and City/locality must be complete, official names and may not contain abbreviations.

< Back Next > Cancel

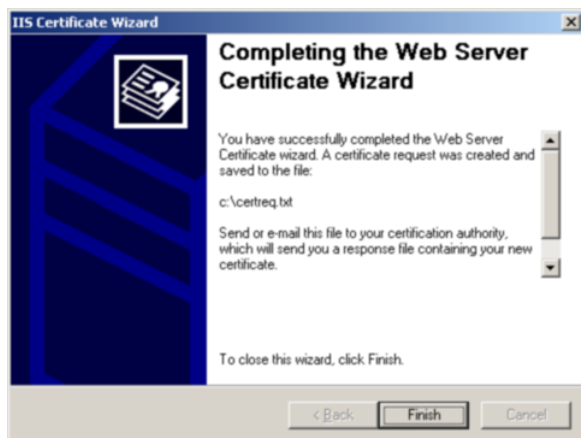
Legen Sie hier den Namen fest, unter dem der CSR abgespeichert werden soll. Normalerweise können Sie den Systemvorschlag übernehmen:



Prüfen Sie die Angaben und bestätigen Sie mit "Next":



Die Generierung des Zertifikatsantrags ist abgeschlossen, wenn nebenstehende Anzeige erscheint, die Sie mit "Finish" bestätigen:



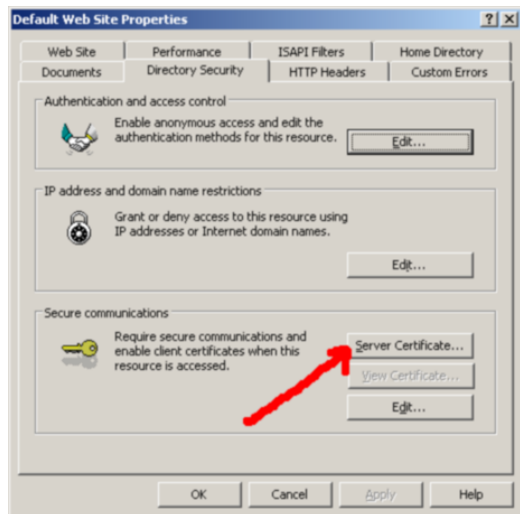
2. Zertifikat beantragen

Mit dem Zertifikatsantrag in der Datei certreq.txt können Sie nun über die Webschnittstelle der DFN-PKI ein Zertifikat beantragen, wie es im Dokument "Beantragung von Zertifikaten für Server der Universität Passau über den DFN-PKI-Dienst",* Abschnitt 3 bis 6, beschrieben ist.

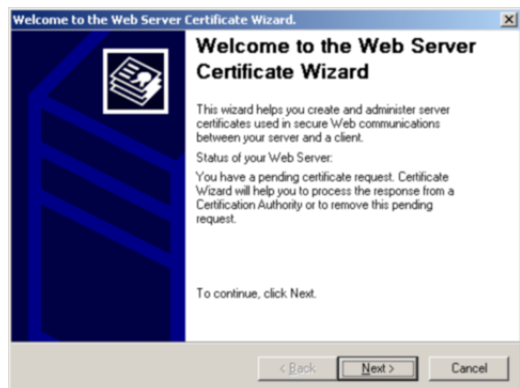
* siehe http://www.rz.uni-passau.de/fileadmin/Dateien/Dokumente/serverzertifikat_howto.pdf

3. Zertifikat im IIS installieren

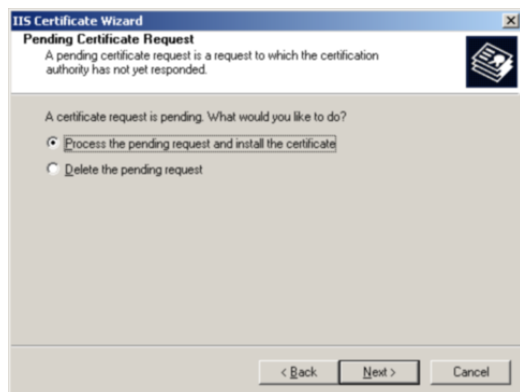
Speichern Sie das von der DFN-PKI per E-Mail erhaltene Zertifikat (Mailanhang) zunächst lokal ab. Dann wählen Sie in der Management-Oberfläche des IIS bei den Eigenschaften Ihrer Website nochmals "Server Certificate":



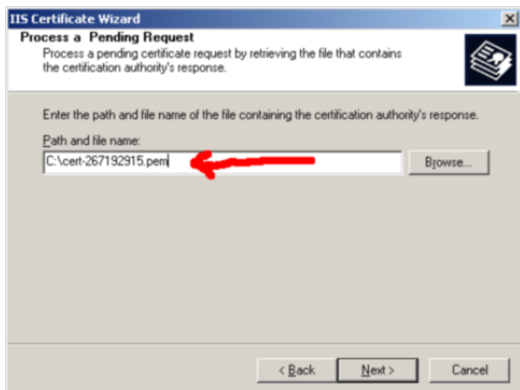
Der "Web Server Certificate Wizard" informiert Sie, dass bereits ein Zertifikatsantrag vorliegt. Bestätigen Sie mit "Next":



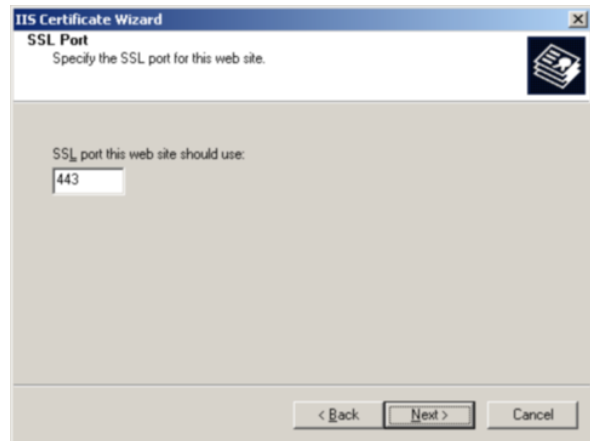
Wählen Sie "Process the pending request...":



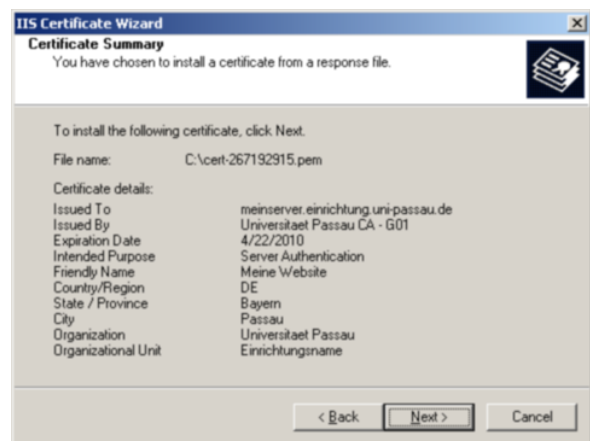
Geben Sie den vollständigen Dateinamen zu dem abgespeicherten Zertifikat ein (beachten Sie, dass der Dateiname mit .pem endet):



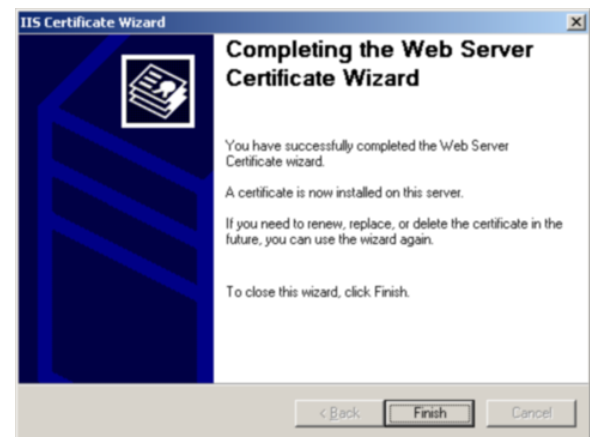
Geben Sie die Portnummer an, die für SSL-gesicherte Verbindungen genutzt werden soll (im Normalfall ist die Vorgabe 443 korrekt):



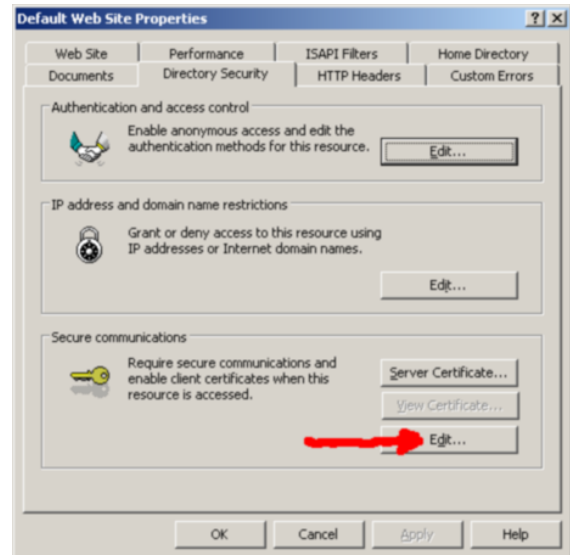
Bestätigen Sie die Richtigkeit der Zertifikatsdaten mit "Next":



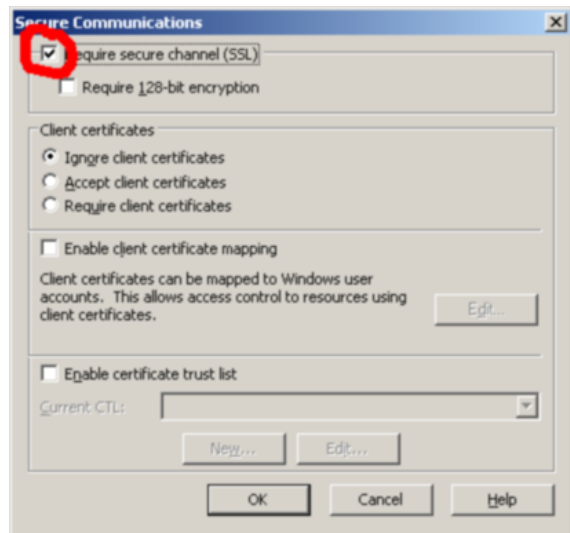
Sie können die Zertifikatsinstallation mit "Finish" abschließen:



Sie sollten nun noch dafür sorgen, dass nur noch SSL-gesicherte Verbindungen zu Ihrem Server aufgebaut werden können. Wählen Sie dazu die Aktion "Edit":



Markieren Sie "Require secure channel" und bestätigen Sie mit "OK":

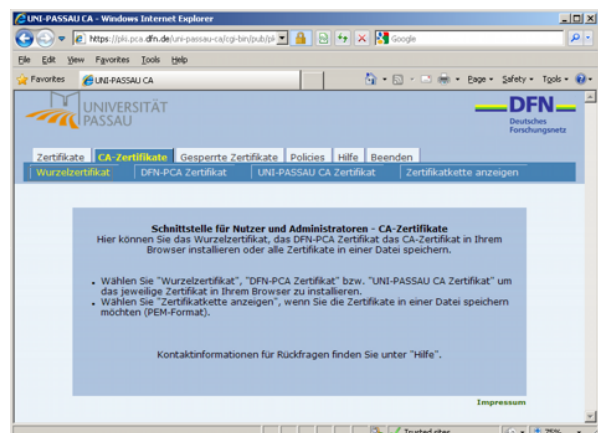


4. Zertifikatskette installieren

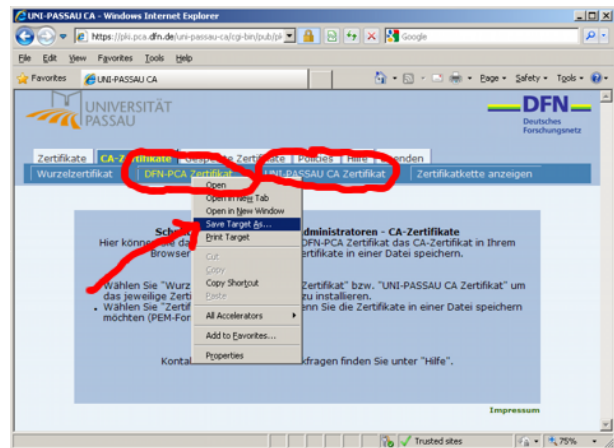
Damit das installierte Zertifikat von den Webbrowsern der Benutzer korrekt überprüft werden kann, müssen Sie noch einmalig die Zertifikate der sog. Zwischenzertifizierungsstellen installieren. Diese erhalten Sie, indem Sie mit dem Browser folgende Seite aufrufen:

<https://pki.pca.dfn.de/uni-passau-ca/pub>

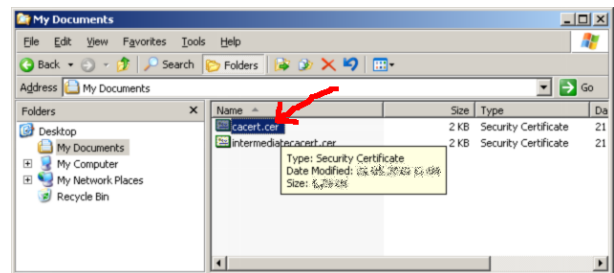
Klicken Sie auf den Reiter "CA-Zertifikate".



Klicken Sie mit der rechten Maustaste auf "DFN PCA-Zertifikat" und speichern Sie mit "Save target as ..." die Datei "intermediatecacert.crt" auf der Festplatte ab.

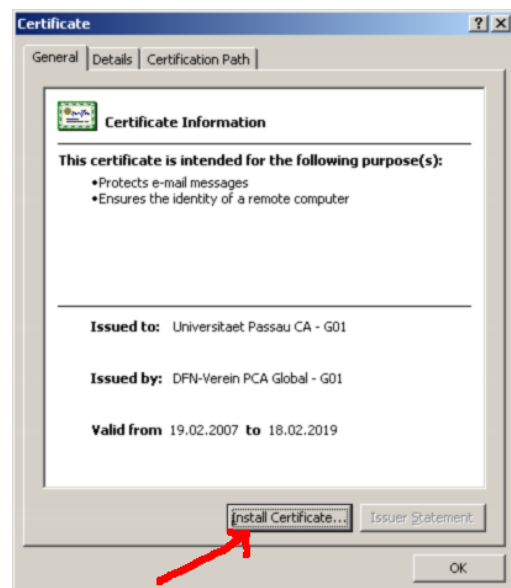


Verfahren Sie ebenso bei "UNI-PASSAU CA Zertifikat"; die betreffende Datei sollte als "cacert.crt" auf der Festplatte abgespeichert werden.

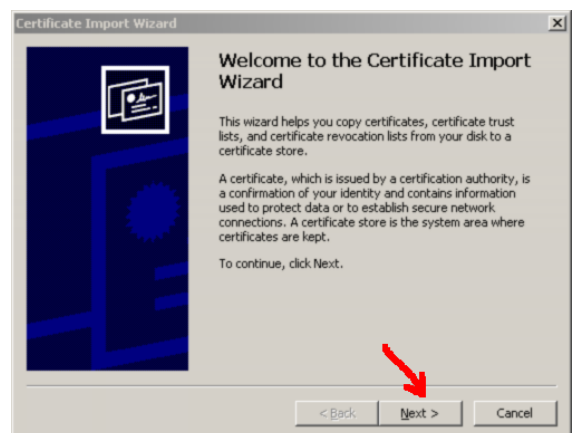


Öffnen Sie nun den Ordner, in dem Sie die beiden Dateien abgespeichert haben. Doppelklicken Sie auf die erste Datei "cacert.crt".

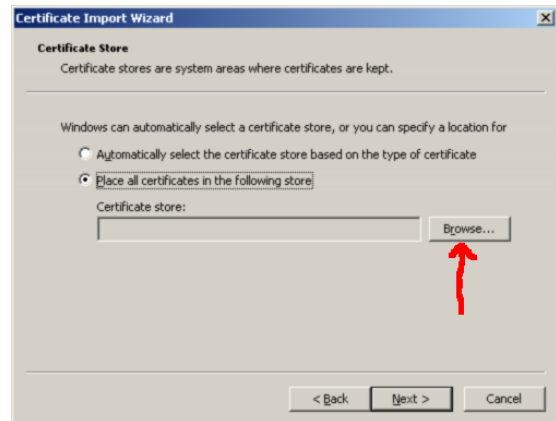
Es wird eine Information zu diesem Zertifikat angezeigt. Klicken Sie auf "Install Certificate ..."



Es startet der "Certificate Import Wizard". Klicken Sie auf "Next".



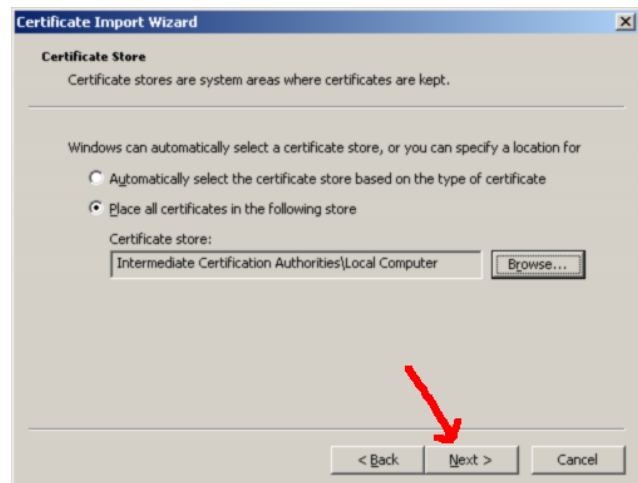
Wählen Sie "Place all certificates in the following store" und klicken Sie auf "Browse...".



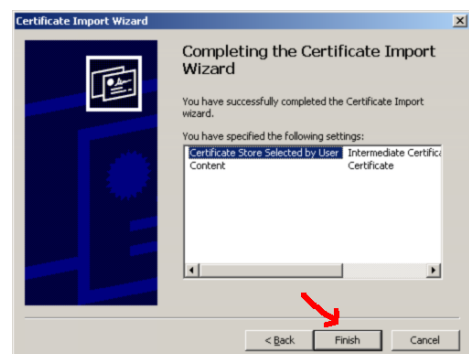
Nun aktivieren Sie das Kästchen "Show physical stores" und wählen in der angezeigten Struktur "Local Computer" im Zweig "Intermediate Certification Authorities". Bestätigen Sie mit "OK".



Jetzt können Sie den vorhergehenden Dialog mit "Next" fortsetzen.



Sie können den "Certificate Import Wizard" jetzt mit "Finish" beenden.



Bestätigen Sie nun nochmals mit "OK".



Wiederholen Sie den Importvorgang in der gleichen Weise mit der Datei "intermediatecacert.crt".