Benutzerhandbuch für die Zertifizierung mit dem Internet Explorer

Mit diesem Handbuch soll den Benutzern der Zertifizierungsinstanz der Leibniz Universität Hannover, der UH-CA, ein Leitfaden zur Zertifikatbeantragung und -verwendung mit dem Internet Explorer an die Hand gegeben werden. Er enthält alle wichtigen Schritte, die zu einem gültigen Zertifikat innerhalb der Zertifizierungshierarchie des Deutschen Forschungsnetzes (DFN) führen.

Lassen Sie sich vom Umfang dieses Dokumentes nicht abschrecken. Schritt für Schritt werden Sie durch das Beantragungsverfahren geführt, was letztlich nicht mehr als ein paar Minuten in Anspruch nimmt. Anschließend wird Ihnen beschrieben, wie Sie das fertige Zertifikat in Ihre Arbeitsumgebung einbinden. Für diesen Vorgang benötigen Sie ebenfalls nur wenige Minuten.

Inhaltsverzeichnis

1 Zur Einführung

1.1 Zertifizierungshierarchie

Für das Signieren und Verschlüsseln von E-Mail erhält jeder Benutzer von der Zertifizierungsstelle der Leibniz Universität Hannover (UH-CA) ein digitales Zertifikat gemäß dem Standard X.509v3 S/MIME, welches seine Identität beschreibt und den öffentlichen Schlüssel enthält. Jedes Zertifikat ist von der ausgebenden Stelle, in diesem Fall die UH-CA, beglaubigt, die ihrerseits wieder von einer höheren Stelle beglaubigt ist. Das Vertrauenssystem ist streng hierarchisch. Den gemeinsamen Vertrauensanker bildet ein sog. Wurzel-Zertifikat (Root Certificate). Dieses ist das selbstzertifizierte Zertifikat der obersten Instanz der Zertifizierungshierarchie, in unserem Fall das Deutsche Telekom Root CA 2 Zertifikat.
Die folgende Abbildung zeigt die Zertifizierungshierarchie der Leibniz Universität Hannover.

1.2 Das PKI-Portal des DFN

Das PKI-Portal des DFN

Das PKI-Portal des Deutschen Forschungsnetzes (DFN) für die Leibniz Universität Hannover ist das öffentlich zugängliche Webinterface der UH-CA. Es ist über den Link oben erreichbar. Alternativ erreichen Sie das PKI-Portal über die RRZN-Webseite http://www.rrzn.uni-hannover.de/zertifizierung.html. Wählen Sie hier „Zertifikat beantragen".

Im PKI-Portal stehen Ihnen alle wichtigen Funktionen im Zusammenhang mit der Zertifizierung zur Verfügung.

Hier können Sie

- ein Zertifikat beantragen,
- ein Zertifikat zurückrufen und
- Zertifikate suchen.

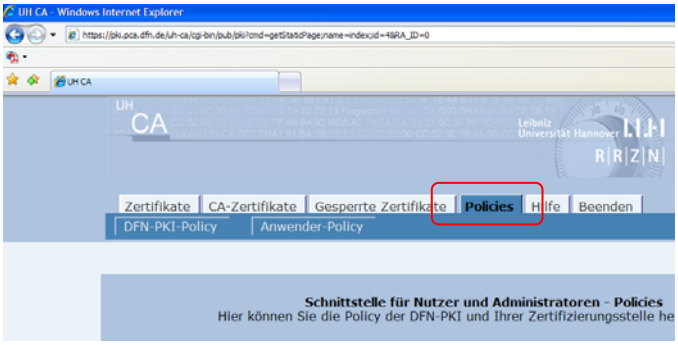
Desweiteren finden Sie hier

- die Zertifizierungsrichtlinie,
- die CA-Zertifikate und
- die Zertifikat-Sperrlisten.

1.3 Die Zertifizierungsrichtlinien der Leibniz Universität Hannover

Eine Zertifizierungsrichtlinie (Certification Policy, CP) definiert die Regeln, nach denen eine oder mehrere Zertifizierungsstellen arbeiten. Die in der Leibniz Universität Hannover angesiedelte Zertifizierungsstelle (UH-CA) formuliert ihre Zertifizierungsrichtlinie in der Weise, dass die „Zertifizierungsrichtlinie der Public Key Infrastruktur im Deutschen Forschungsnetz – Global, Classic, Basic" Anwendung findet.
Eine Erklärung zum Zertifizierungsbetrieb (*Certification Practice Statement*, CPS) beschreibt die Verfahrensweisen, mit denen eine Zertifizierungsrichtlinie von einer Zertifizierungsstelle umgesetzt wird. Die in der Leibniz Universität Hannover angesiedelte Zertifizierungsstelle (UH-CA) formuliert ihre Erklärungen zum Zertifizierungsbetrieb in der Weise, dass die „Erklärung zum Zertifizierungsbetrieb der Public Key Infrastruktur im Deutschen Forschungsnetz – Global, Classic, Basic " Anwendung findet.

Der Inhalt beider Dokumente wird an einigen Stellen durch die „Erklärung zum Zertifizierungsbetrieb der UH-CA in der DFN-PKI" um eigene Spezifikationen erweitert.



Mit Hilfe der Zertifizierungsrichtlinien ist es für jeden Teilnehmer möglich, eine Einschätzung über die Qualität der ausgestellten Zertifikate zu treffen. Sie beschreiben die Mindestanforderungen und Abläufe der Zertifizierung und sind Teil der Vereinbarung zwischen der CA und den Benutzern. Daher sollte jeder, der ein Zertifikat der UH-CA beantragen will, diese Richtlinien genau studieren.

2 Beantragen eines persönlichen Nutzer-Zertifikates

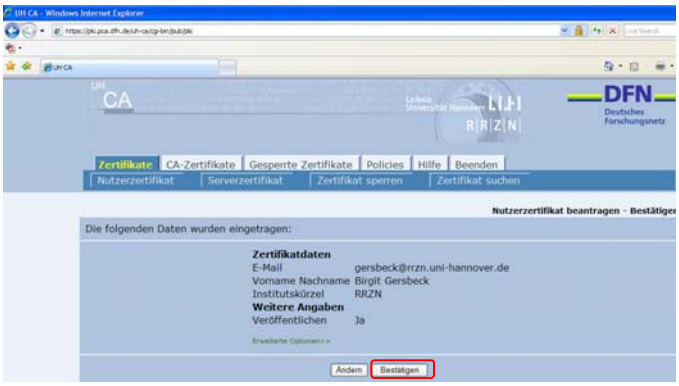
Für die Beantragung Ihres persönlichen Nutzer-Zertifikates, wählen Sie im PKI-Portal des DFN unter dem Reiter **Zertifkate** den Punkt **Nutzerzertifikat** aus, der zum folgenden Fenster führt.

Füllen Sie den Antrag mit Ihren Daten aus und wählen Sie **Weiter**.

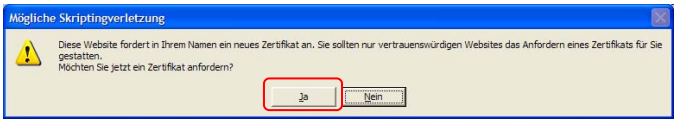
Unter **Zertifikatdaten** werden die Daten erfasst, die in das Zertifikat mit aufgenommen werden. Jedes Zertifikat beinhaltet u.a. einen eindeutigen Namen (Distinguished Name, DN). Dieser wird von den Feldern **E-Mail, Name** und **Institutskürzel** zusammen mit den festgelegten Einträgen O= Leibniz Universitaet Hannover und C=DE gebildet.

Geben Sie auch eine PIN (diese PIN wird nur wichtig, wenn Sie einen elektronischen Sperrantrag für das Zertifikat erstellen wollen, eine Sperrung kann aber auch mittels Anruf bei der RA in die Wege geleitet werden). Bestätigen Sie die PIN noch einmal, stimmen Sie der Zertifizierungsrichtlinie zu und stimmen Sie bitte unbedingt auch einer Veröffentlichung Ihres Zertifikates zu. Bei Nichtzustimmung benötigt die RA eine Begründung von Ihnen. Nur wenn Sie der Veröffentlichung zustimmen, ist Ihr Zertifikat später über den Button „Zertifikate suchen" zu finden und Sie sind damit für andere Teilnehmer nachvollziehbar vertrauenswürdig. Genauso aber werden Sie auch andere Teilnehmer als vertrauenswürdig einstufen können, wenn diese Ihr Zertifikat veröffentlicht haben zugestimmt haben.

Wenn alle Angaben korrekt sind, bestätigen Sie mit **Weiter**.



Wenn alle Angaben korrekt sind, **bestätigen** Sie.



Bestätigen Sie mit **JA**.

Im Dialog „Ein neuer RSA-Austauschschlüssel wird erstellt" sollte zunächst die Sicherheitsstufe eingestellt werden: Automatisch wird eine mittlere Sicherheitsstufe gewählt. Über das Button Sicherheitsstufe kann die Sicherheitsstufe geändert werden.

Wählen Sie **Hoch** und klicken Sie dann auf **Weiter**.

Zum Schutz Ihres Schlüssels werden Sie zur Eingabe eines **Kennwortes** aufgefordert. Nachdem Sie dieses eingegeben und bestätigt haben, wählen Sie **Fertig stellen**.

Internet Explorer 7 veranlasst nun die Generierung Ihres Schlüsselpaares auf Ihrem Rechner. Privater und öffentlicher Schlüssel ermöglichen später im Zusammenhang mit dem Zertifikat das Unterschreiben und Verschlüsseln von E-Mail. Bestätigen Sie mit **OK**.

Sie werden nun aufgefordert, sich den Zertifikatantrag auszudrucken.

3 Aufsuchen des Rechenzentrums

Sind alle Angaben auf dem Ausdruck korrekt, unterschreiben Sie ihn und suchen Sie nach telefonischer Absprache die Registrierungsstelle (RA) im RRZN auf:

Herr Andreas Anft
Rechenzentrum der Leibniz Universität Hannover
Schloßwenderstraße 5
30167 Hannover
Telefon: 0511-762 19792
Terminabsprachen sind für den Vertretungsfall auch unter -19789 und -799042 möglich!

Folgendes ist mitzubringen:

1. Die vollständig ausgefüllte Zertifikatantrag,
2. den Personalausweis oder Pass,
3. ein Dokument, das die Zugehörigkeit zur Universität bestätigt.

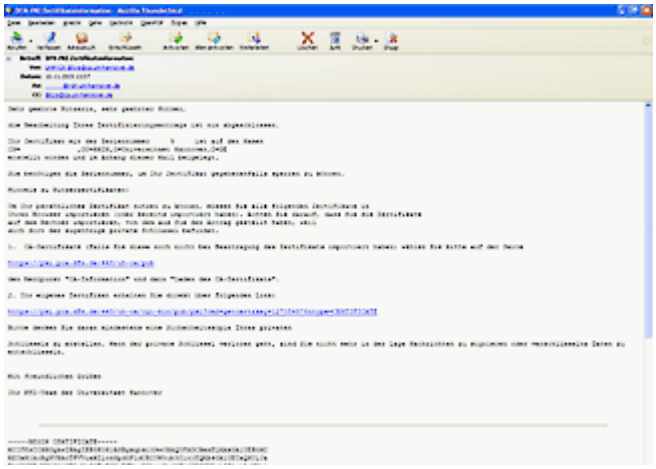
Wenn Sie den Mitarbeitern persönlich bekannt sind, kann auf das Dokument über die Zugehörigkeit (3.) verzichtet werden.

Prüfung und Beglaubigung des Zertifikatantrages:

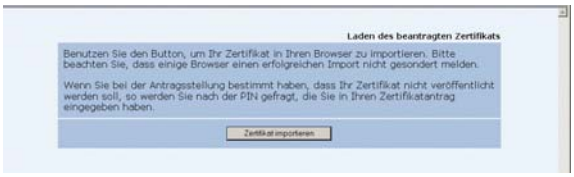
Nach Kontrolle des Zertifikatantrages wird dieser beglaubigt von der RA an die CA weitergeleitet. Dort wird das Zertifikat erstellt und Sie erhalten umgehend eine Benachrichtigung per E-Mail.

4 Antwort E-Mail und Zertifikat in den Browser importieren

Nachdem die UH-CA Ihr Zertifikat erstellt hat, erhalten Sie eine Mail vom PKI-Team der Leibniz Universität Hannover...

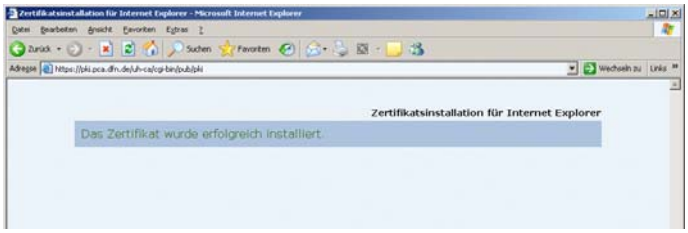


... mit der Information, dass Sie Ihr Zertifikat nun abholen können. Es reicht ein Mausklick auf den markierten Link, um Ihr persönliches Zertifikat in Ihren Browser zu integrieren.
Ihr Zertifikat ist außerdem noch als PEM-Datei als Anlage der E-Mail beigefügt (in diesem Format müssen die Sie es aber nicht nutzen).



Sie werden nun aufgefordert, das Zertifikat zu importieren.

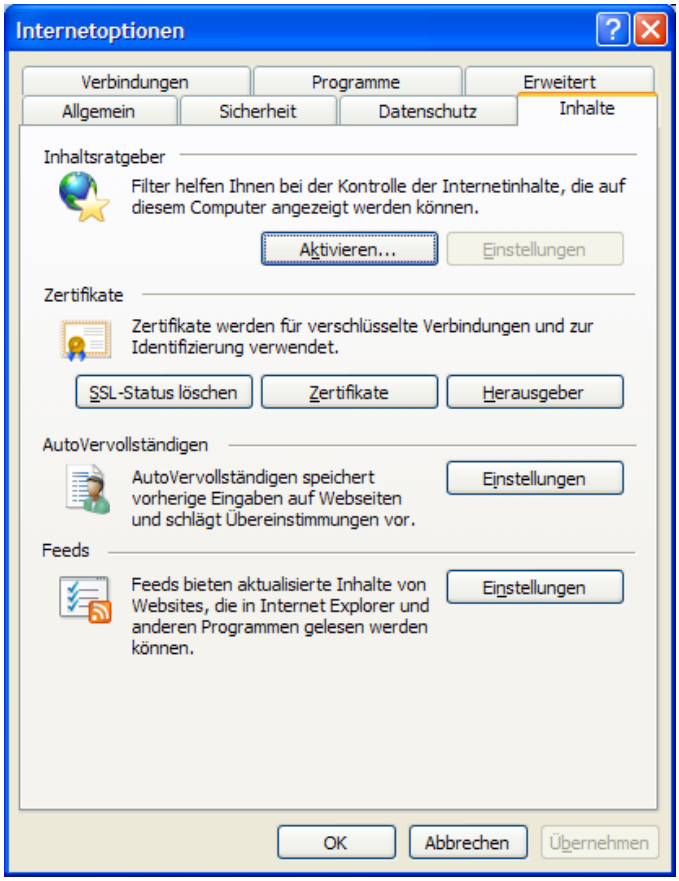
Bestätigen Sie mit JA.



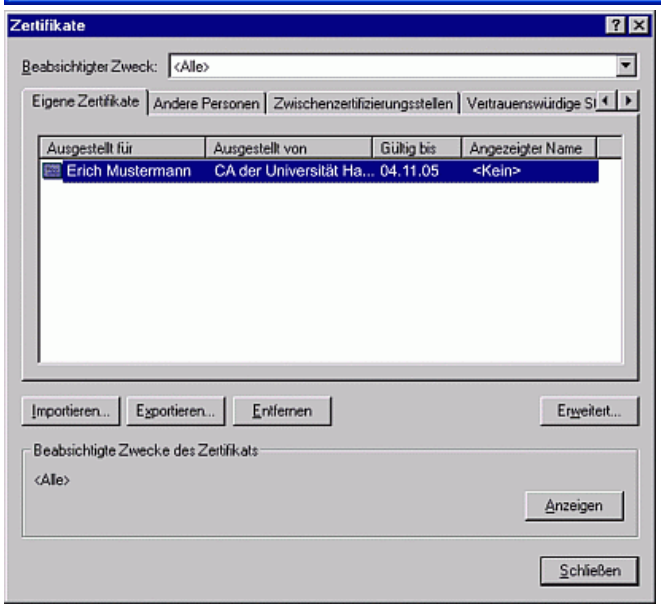
Das Zertifikat wurde erfolgreich importiert.

5 Sicherungskopie des privaten Schlüssels

Für die folgenden Schritte wird eine leere 3½" Diskette benötigt (oder ein anderer externer Datenträger).

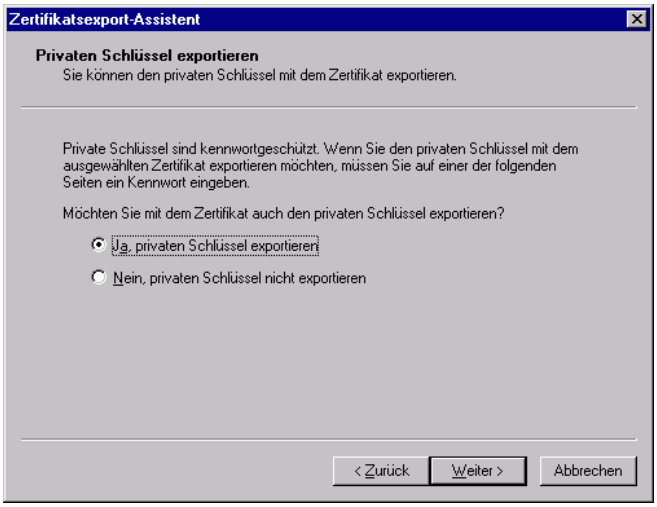


Unter **Extras-Internetoptionen** finden Sie den Reiter **Inhalte**. Klicken Sie hier bitte **Zertifikate** an.

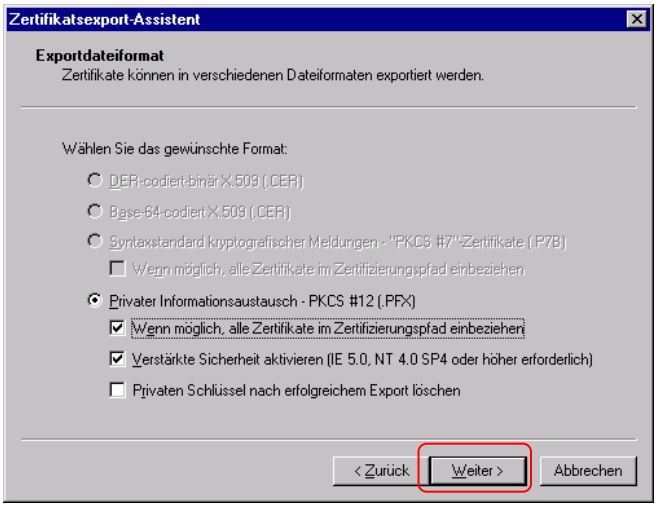


Unter **Eigene Zertifikate** sollte das eigene, von der Leibniz Universität Hannover ausgestellte Zertifikat vorhanden sein. Der rot markierte Schalter **Exportieren** wird erst nach der Auswahl des eigenen Zertifikates verfügbar.

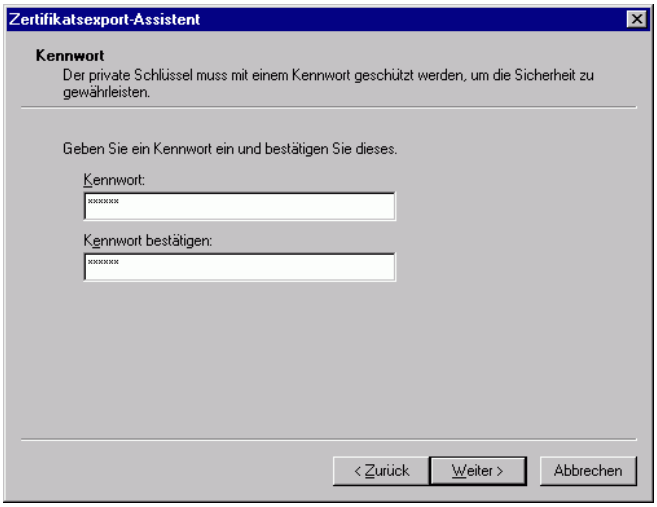
Es öffnet sich der Zertifikatsexport-Assistent. Wählen Sie **Weiter**.



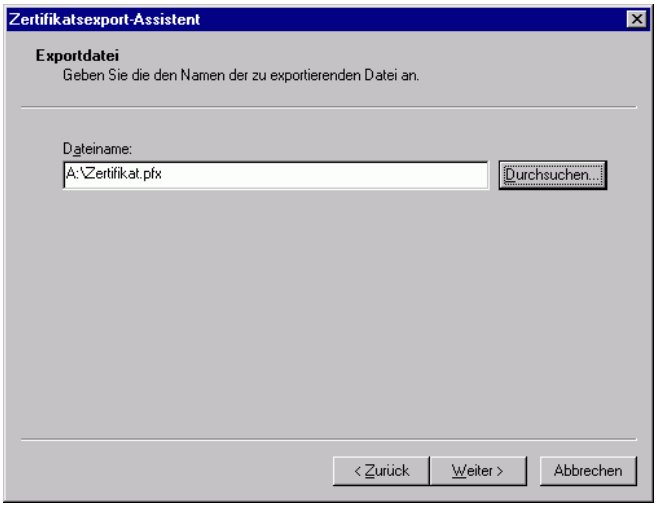
Bestätigen Sie mit **Ja**.



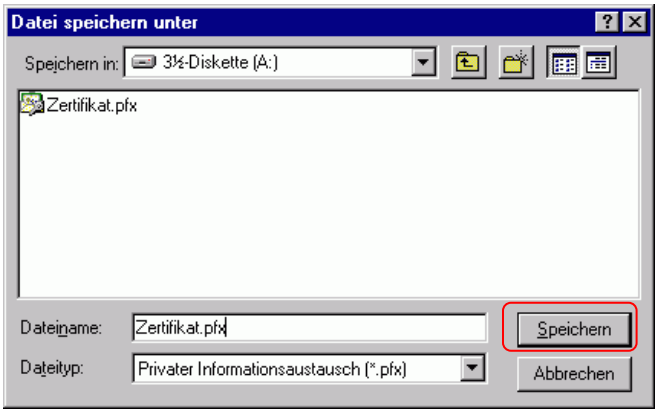
Setzen Sie bitte die beiden Haken.



Da ein Zugriff auf den geheimen Schlüssel stattfindet, geben Sie nun ein Kennwort ein und bestätigen Sie dieses noch einmal.



Drücken Sie **Durchsuchen**.



Wählen Sie das Floppylaufwerk bzw. einen anderen externen Datenträger, geben Sie einen Dateinamen ein und drücken Sie **Speichern**.

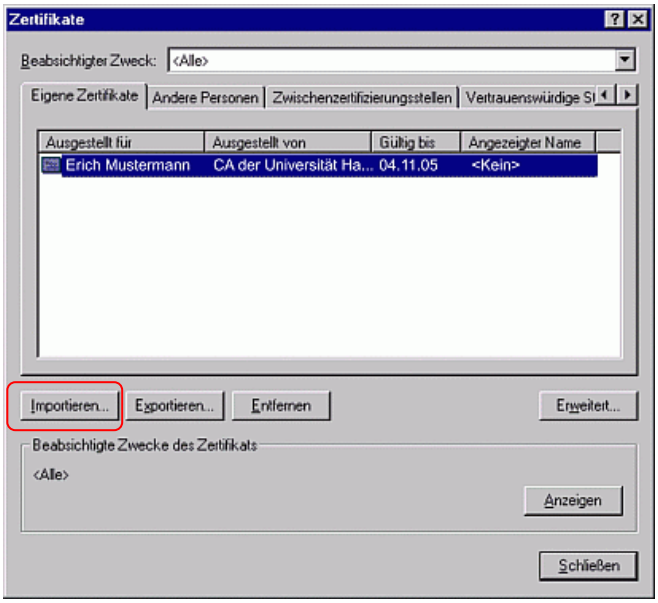
Wählen Sie **Fertig Stellen.**

Bestätigen Sie mit **OK.**

6 Wichtiger Hinweis zum Einstellen der Sicherheitsstufe

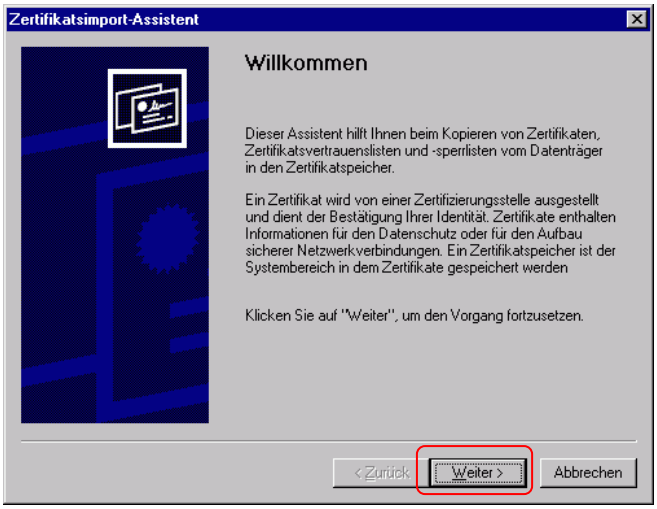
Für den Fall, dass Sie beim Erstellen des Zertifikatantrages für den privaten Schlüssel nicht die hohe Sicherheitstsufe eingestellt haben (wobei es Ihnen grundsätzlich freigestellt ist, ob Sie die hohe, mittlere oder niedrige Sicherheitsstufe wählen), wird beim Signieren einer E-Mail kein Passwort abgefragt.
Es besteht somit die Gefahr, dass ein Virus mit eigener SMTP-Engine (versendet eigenständig Mails an z.B. die Einträge im Adressbuch) nun möglicherweise auch signierte Mails verschicken kann.
Darum sollte unbedingt immer die hohe Sicherheitsstufe eingestellt werden, um zu gewährleisten, dass für signierte Mails immer ein Passwort abgefragt wird, sodass der oben beschriebene Fall nach Virusbefall, oder ähnlich gelagerter Missbrauch, verhindert wird.

So ändern Sie die Sicherheitsstufe für Ihren privaten Schlüssel:
Sie benötigen die Diskette, auf der Sie ihren privaten Schlüssel gespeichert haben.

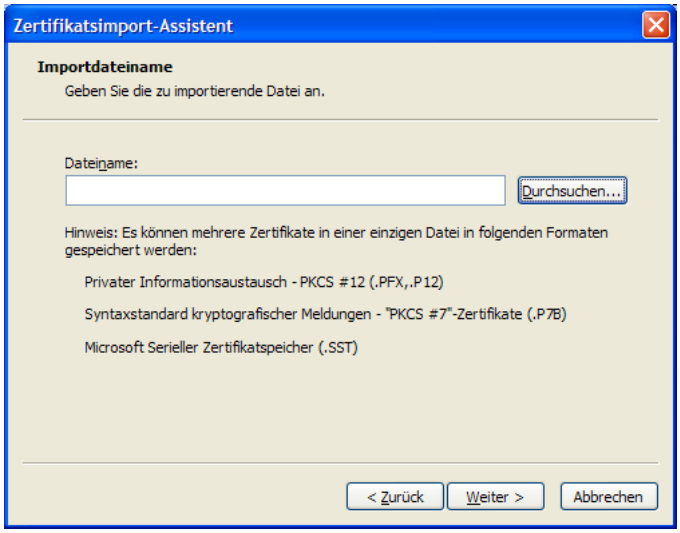


Wählen Sie im Menü des Internet Explorers unter **Extras** die **Internetoptionen**. Unter dem Reiter **Inhalte** wählen Sie den Button **Zertifikate.**

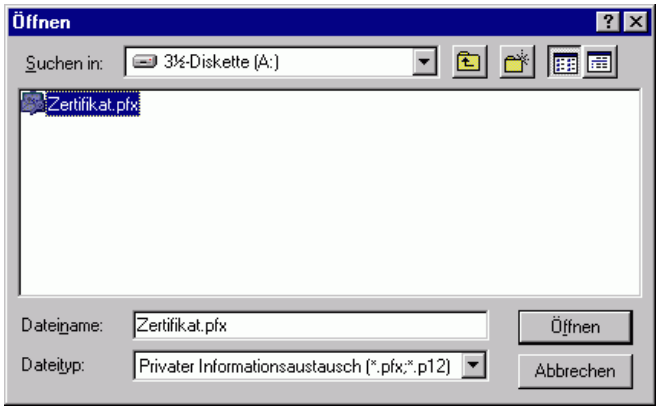
Unter **Eigene Zertifikate** sollte das eigene von der Leibniz Universität Hannover ausgestellte Zertifikat vorhanden sein. Der rot markierte Schalter **Importieren** wird erst nach der Auswahl des eigenen Zertifikates verfügbar.



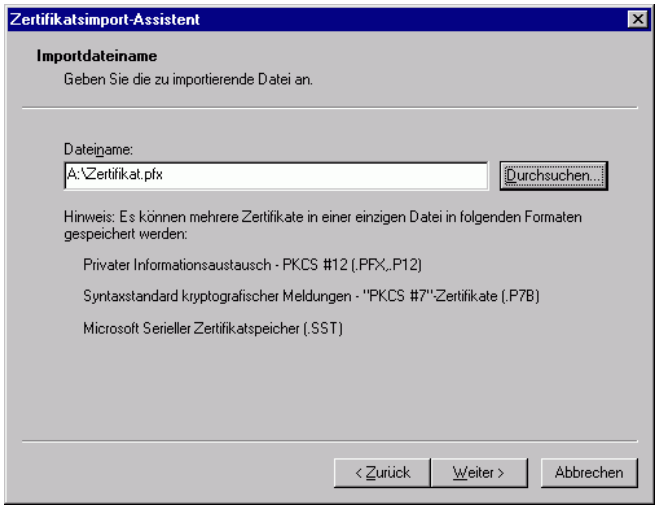
Es öffnet sich der Zertifikatsimport-Assistent. Drücken Sie **Weiter**.



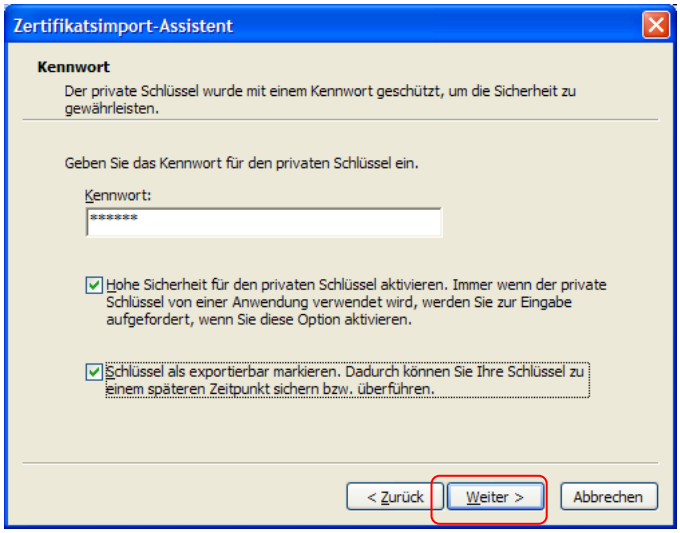
Wählen Sie **Durchsuchen**.



In Ihrem Floppylaufwerk sollte sich jetzt die Diskette mit Ihrem Zertifikat befinden. **Öffnen** Sie es.



Weiter

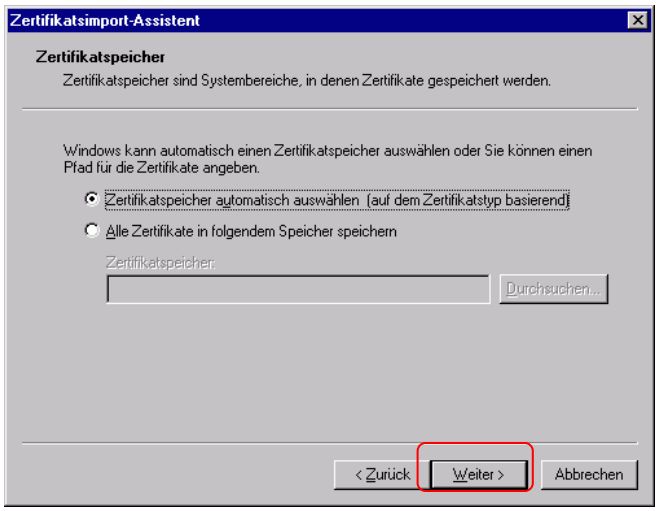


Setzen Sie das Häkchen für **Hohe Sicherheit und für Schlüssel als exportierbar markieren**. Geben Sie dann das **Kennwort** für Ihren privaten Schlüssel an, das Sie zuvor beim Exportieren benutzt haben.

Dieses Kennwort ist nicht zu verwechseln mit dem Kennwort für die hohe Sicherheitsstufe für Ihr Zertifikat.

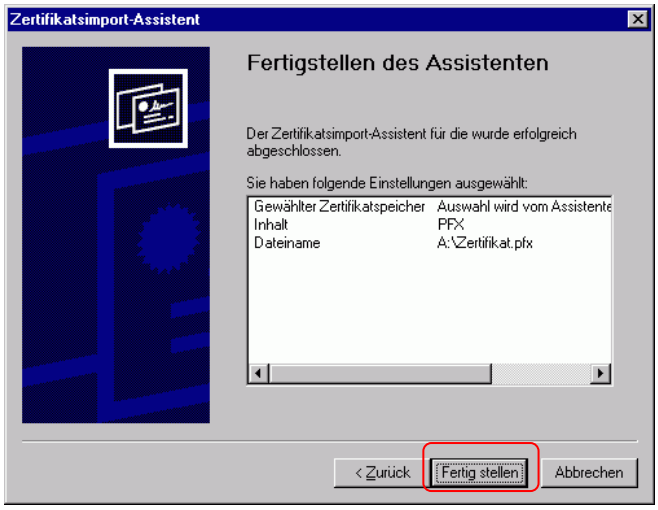
Mit diesem Kennwort hatten Sie Ihren privaten Schlüssel auf der Diskette vor missbräuchlichen Zugriff geschützt.

Drücken Sie **Weiter**.



Wählen Sie **Zertifikatsspeicher automatisch auswählen.**

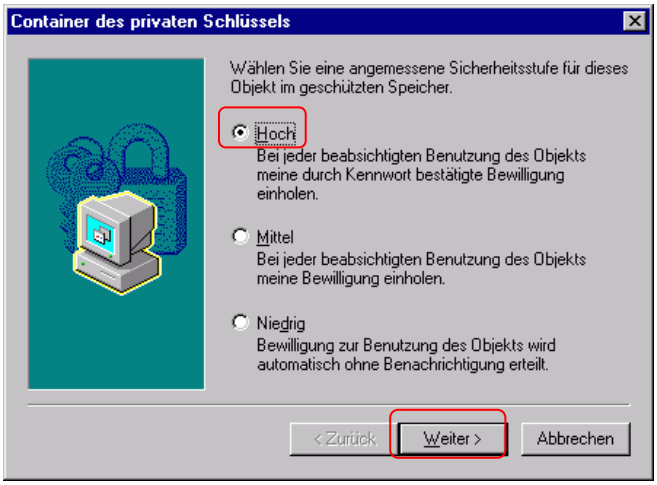
Weiter



Wählen Sie **Fertig Stellen.**

Jetzt können und sollen Sie die Sicherheitsstufe ändern.

Hier sollten Sie die **Sicherheitsstufe einstellen** wählen.



Wählen Sie jetzt **Hoch**.

Sie werden nun zur Eingabe eines **Kennwortes** aufgefordert. Damit wird der Kryptospeicher auf Ihrem Computer , der die eigenen Zertifikate beinhaltet, geschützt. Überlegen Sie sich ein Kennwort und bestätigen Sie dieses noch einmal. Dieses Kennwort wird bei jeder zu signierenden Mail abgefragt werden.

Drücken Sie **Fertig Stellen**.

Die Sicherheitsstufe wurde geändert.

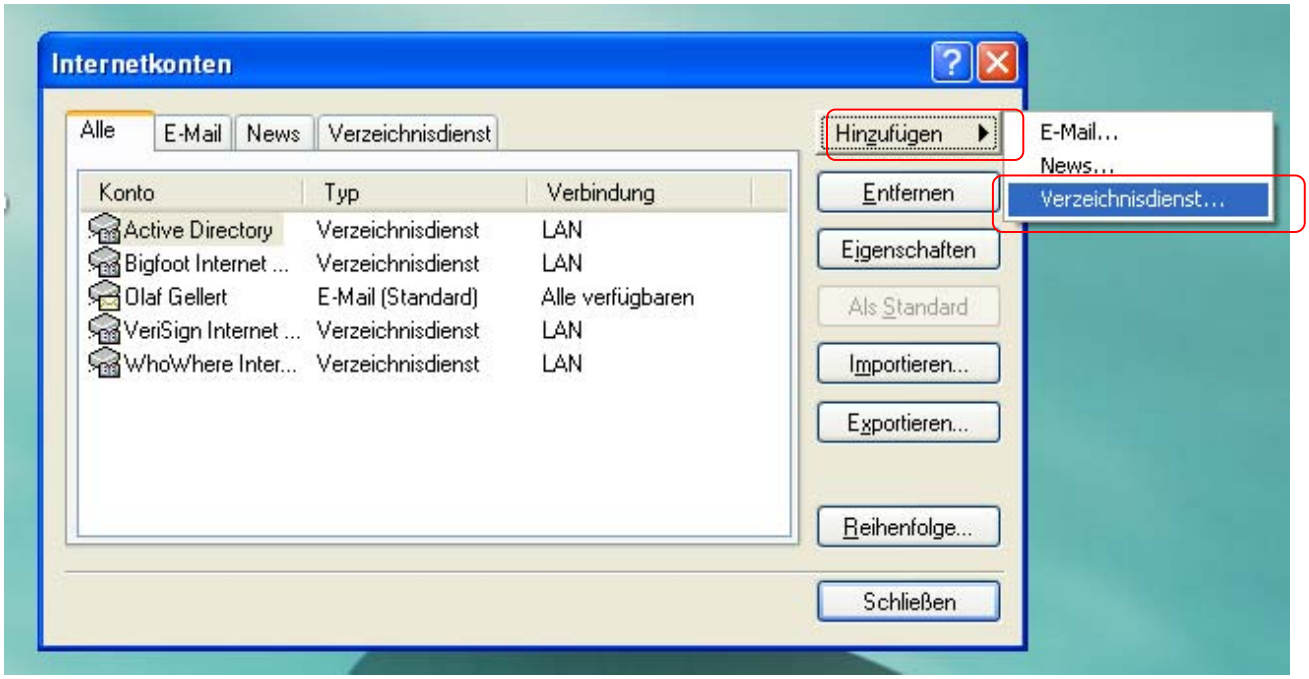
Bestätigen Sie mit **OK**.

OK

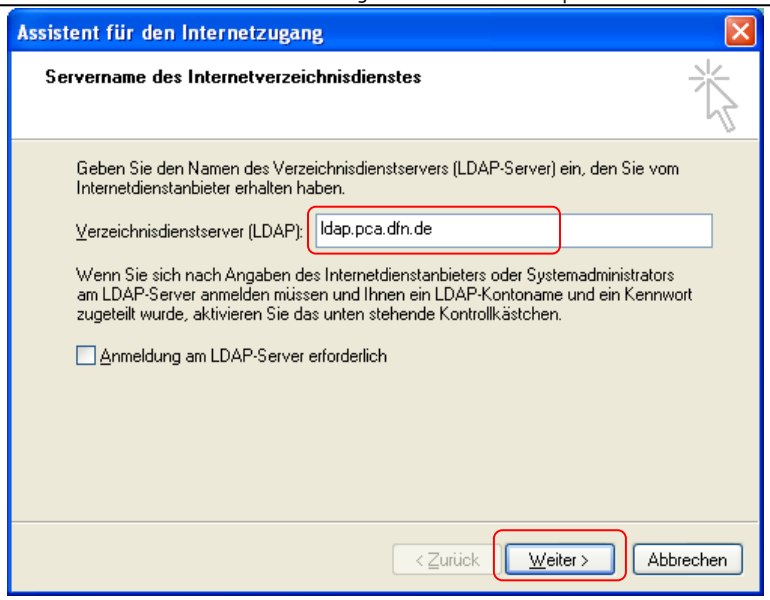
7 LDAP Verzeichnisdienst konfigurieren

Eine nützliche Angelegenheit ist die Verwendung eines LDAP-Verzeichnisdienstes im Mail-Programm. Der Verzeichnisdienst ermöglicht die Suche von Empfängeradressen und -zertifikaten, mit denen zuvor noch nicht kommuniziert wurde. Auf diese Weise kann man verschlüsselte Mails an zuvor unbekannte Kommunikationspartner senden.

Wählen Sie zunächst im Menü **Extras** den Eintrag **Konten** aus. In dem erscheinenden Fenster klicken sie oben rechts den Button **Hinzufügen** an und wählen in dem Menü den Eintrag **Verzeichnisdienst**.



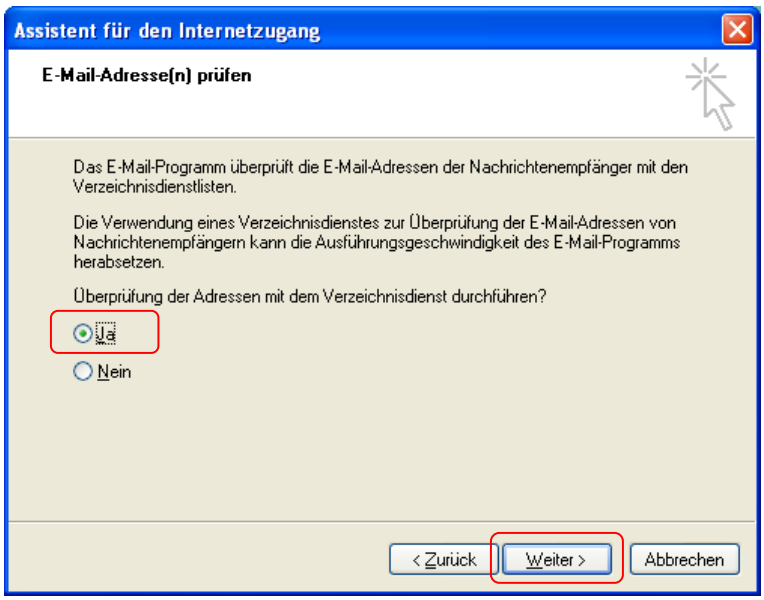
Nun fragt Outlook Express der Reihe nach die notwendigen Parameter für den LDAP-Server ab:



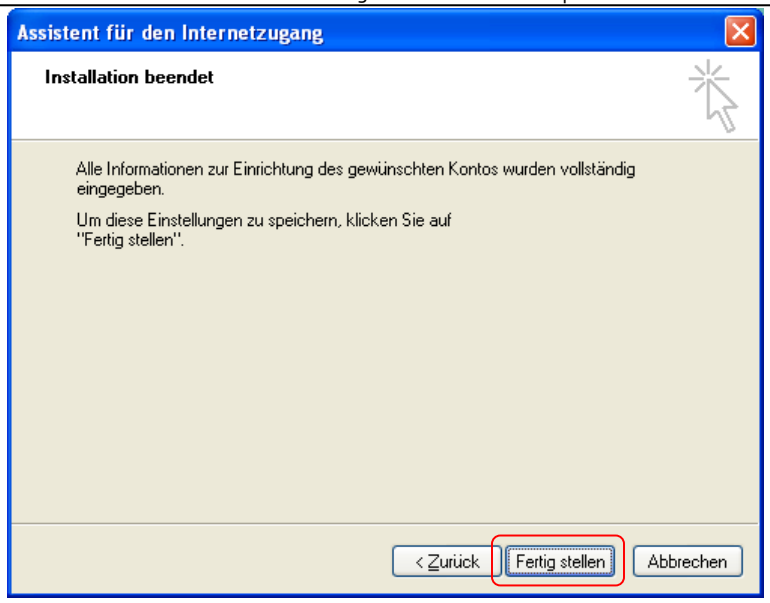
Zunächst erfragt Outlook den Namen des Verzeichnisdienst-Servers. Hier muss

ldap.pca.dfn.de

eingegeben werden. Eine Anmeldung am LDAP-Server ist nicht erforderlich.

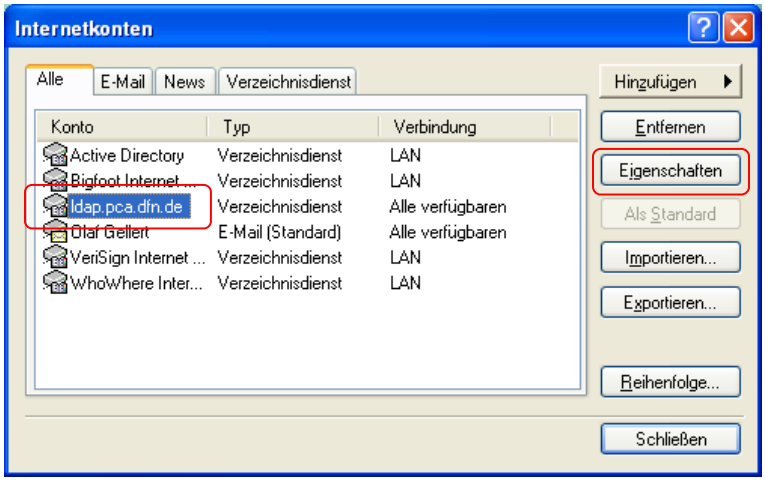


Outlook Express kann bereits beim Eintippen eine Empfängers vom LDAP-Server die möglichen Empfängeradressen abfragen und zum Vervollständigen anbieten. Diese Option wird durch anklicken von Ja gewählt.

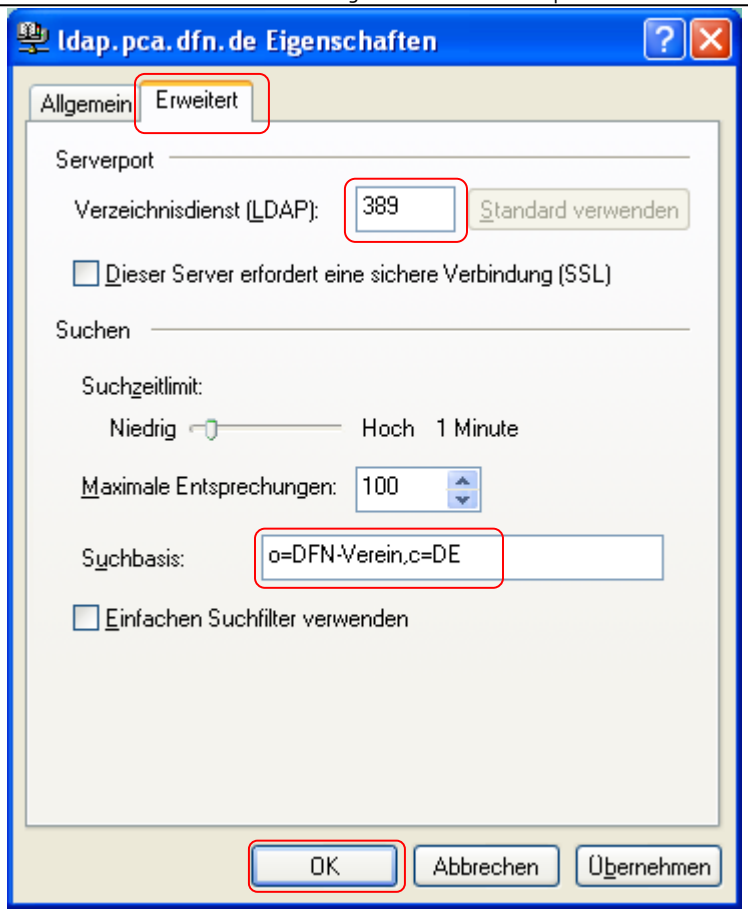


Outlook Express schließt den Konfigurationsvorgang damit erfolgreich ab.

Es müssen jedoch im nächsten Schritt noch einige weitere Einstellungen vorgenommen werden.



Im noch offenen Fenster Konten wählt man den soeben eingerichteten LDAP-Verzeichnisdienst aus und klickt dann rechts auf Eigenschaften.



In einem Fenster erscheinen die bisherigen Angaben zum LDAP-Verzeichnisdienst. Hier wählt man oben zunächst die Karteikarte Erweitert aus.

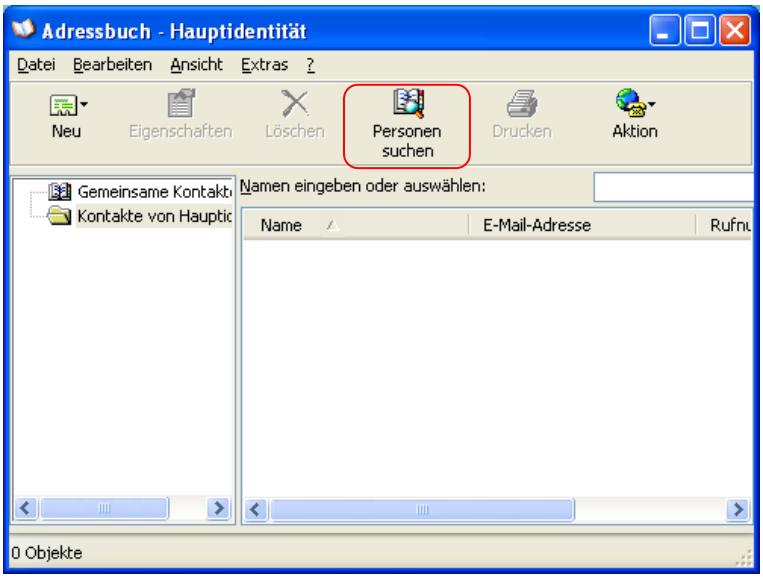
Der Serverport muss nicht verändert werden, er sollte 389 lauten.

Die Suchbasis auf dem LDAP-Server muss eingegeben werden. Hier sollte

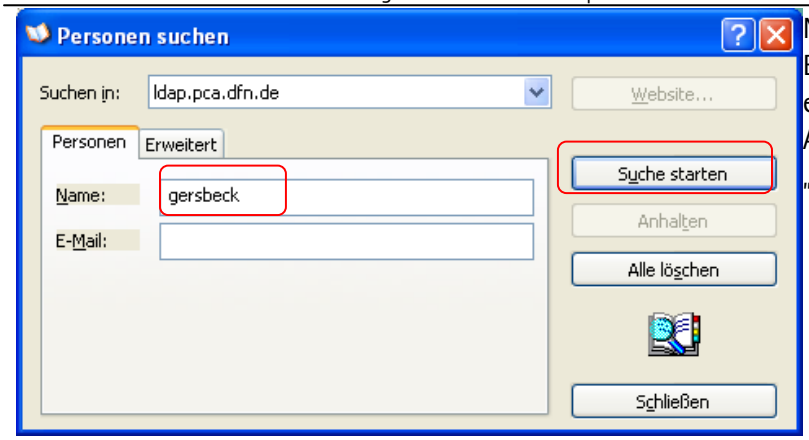
o=DFN-Verein,c=DE

eingetragen werden. Damit wird der gesamte Server nach Einträgen gesucht, d.h. man findet auch die Adressen anderer Universitäten und Forschungseinrichtungen.

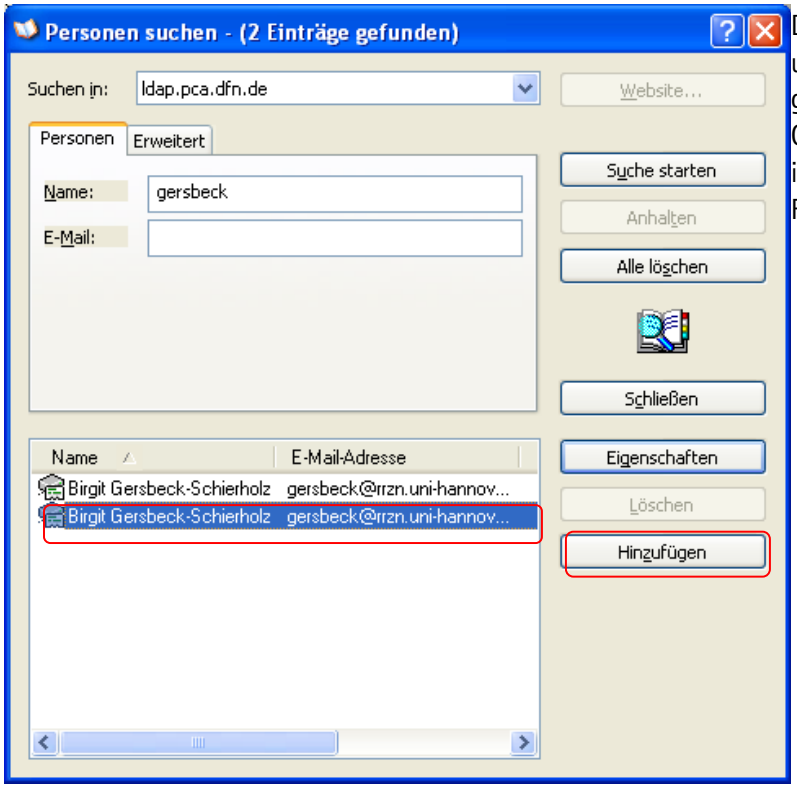
Die Konfiguration des LDAP-Servers ist damit vollständig. Zum Testen kann man im Hauptfenster von Outlook Express das Adressbuch aufrufen:



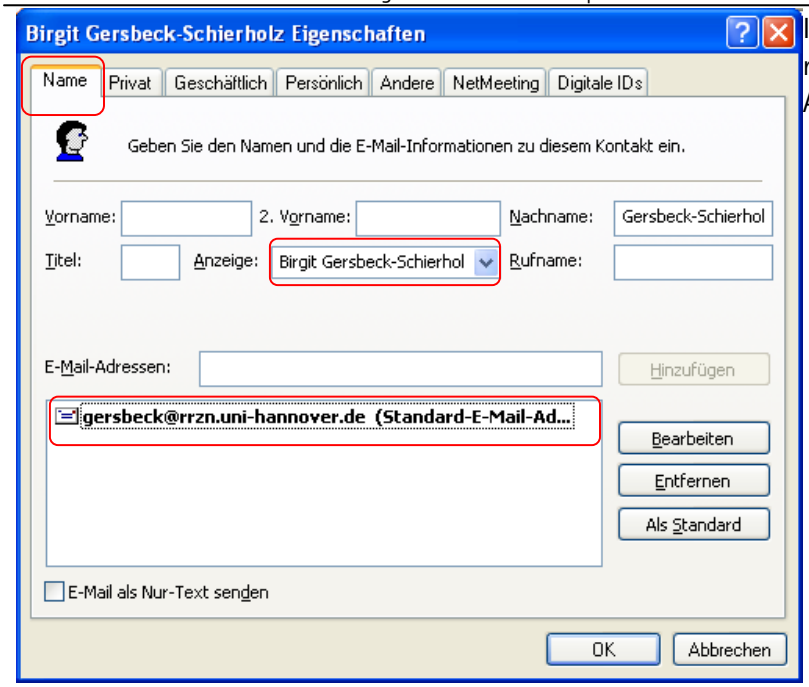
Im Adressbuch wählt man die Funktion Personen suchen.



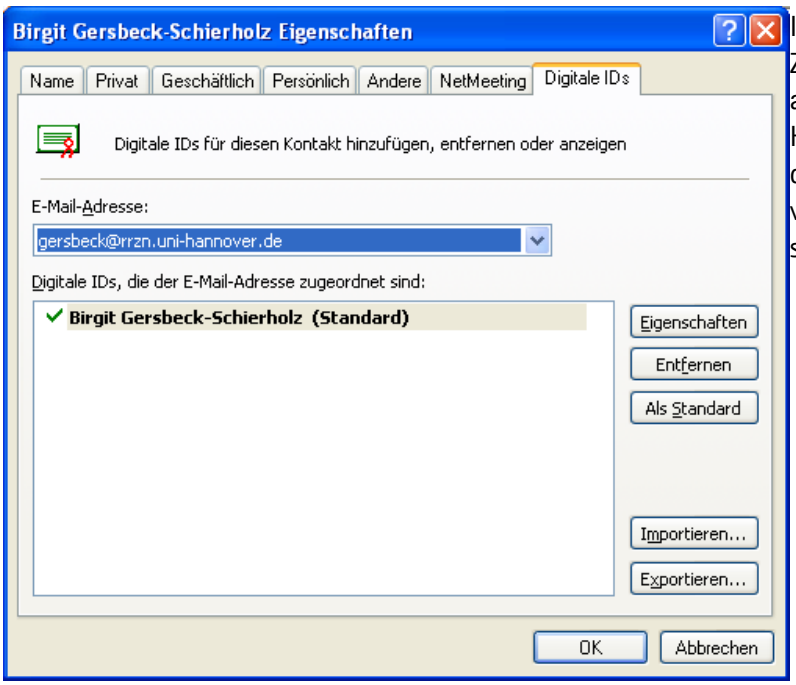
Nun können Sie Teile des Namens oder der Emailadresse der gesuchten Person eingeben und eine entsprechende LDAP-Anfrage wird gestartet, wenn Sie auf „Suche starten" klicken.



Die Ergebnisse der Suchanfrage werden unten im Fenster angezeigt. Einen gefundenen Kontakt können Sie den Outlook Express Kontakten hinzufügen, indem Sie den Kontakt anklicken und die Funktion „Hinzufügen" anwählen.

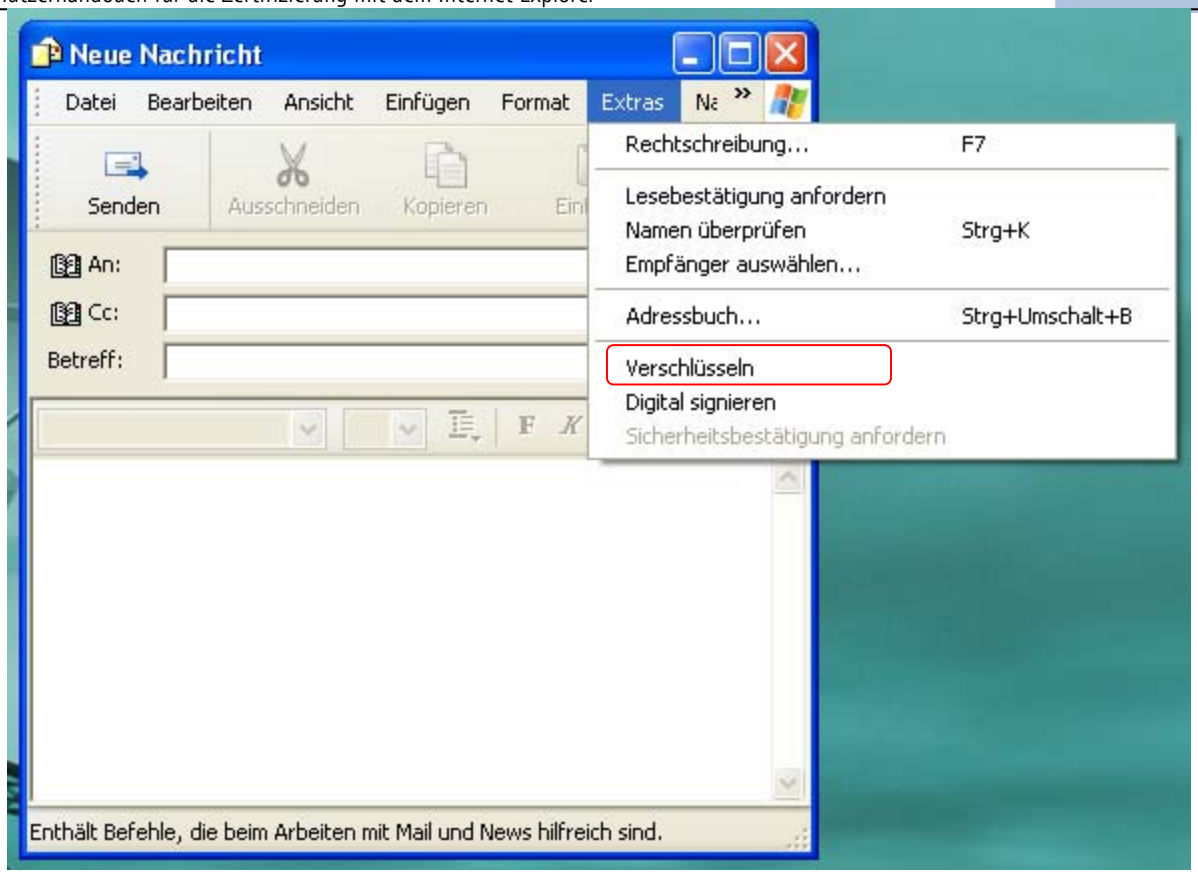


In der angezeigten Karteikarte „Name" wird nun bereits der Name und die Email-Adresse der gefundenen Person angezeigt.



In der Karteikarte „Digitale IDs" wird das Zertifikat der gefundenen Person angezeigt. Ist der Eintrag mit einem grünen Haken versehen, so konnte Outlook Express das Zertifikat validieren und Sie können verschlüsselte Emails an die Person schicken.

Beim Erstellen einer neuen Mail können Sie im Menü Extras nun Verschlüsselung für diese Mail wählen.



Bei Outlook Express muss ein im LDAP gefundene Mailempfänger zu den Kontakten hinzugefügt werden, bevor man verschlüsselte Emails verschicken kann. Benötigen Sie ein Zertifikat eines Empfängers, das nicht im LDAP-Server vorhanden ist, so können Sie sich vom Empfänger zunächst eine signierte Email schicken lassen. Outlook Express importiert beim Aufruf der Email automatisch die enthaltenen Schlüssel, so dass Sie nun auch verschlüsselte Mails an diesen Empfänger senden können.