Benutzerhandbuch für die Zertifizierung mit dem Internet Explorer

Version 1.0 vom 10.10.2007

Im Folgenden soll den Benutzern der Zertifizierungsinstanz der Universität Hamburg, der UHH-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.

Diese Anleitung beruht auf dem Benutzerhandbuch der UH-CA der Leibniz Universität Hannover, das der Universität Hamburg von Frau Gersbeck-Schierholz freundlicherweise zur Verfügung gestellt wurde. Vielen Dank!

Inhaltsverzeichnis

1 Zur Einführung

1.1 Zertifizierungshierarchie

Für das Signieren und Verschlüsseln von E-Mail kann jeder Universitätsangehörige (Studierende, Mitarbeiter) von der Zertifizierungsstelle der Universität Hamburg (UHH-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 UHH-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 Universität Hamburg.

1.2 Das PKI-Portal des DFN

Das PKI-Portal des DFN

Das PKI-Portal des Deutschen Forschungsnetzes (DFN) für die Universität Hamburg ist das öffentlich zugängliche Webinterface der UHH-CA. Es ist über den Link oben erreichbar. Alternativ erreichen Sie das PKI-Portal über die RRZ-Webseite

http://www.rrz.uni-hamburg.de/sicherheit/pki/beantragen-von-zertifikaten/persoenliche-zertifikate.html

Dort wählen Sie den Link „persönliches 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

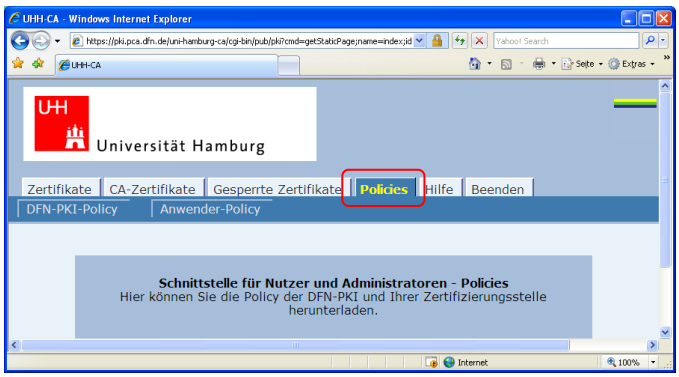
- die Zertifizierungsrichtlinie,
- die CA-Zertifikate und
- die Zertifikat-Sperrlisten.

1.3 Die Zertifizierungsrichtlinien der Universität Hamburg

Eine Zertifizierungsrichtlinie (Certification Policy, CP) definiert die Regeln, nach denen eine oder mehrere Zertifizierungsstellen arbeiten. Die in der Universität Hamburg angesiedelte Zertifizierungsstelle (UHH-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 Universität Hamburg angesiedelte Zertifizierungsstelle (UHH-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 UHH-CA in der DFN-PKI“ um eigene Spezifikationen erweitert.



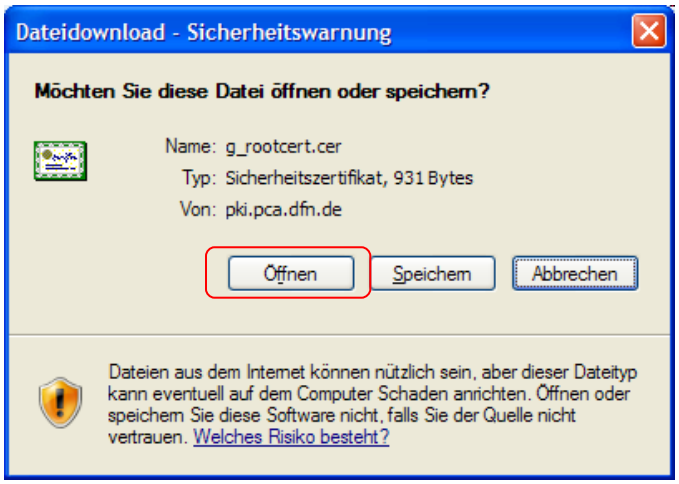
Mit Hilfe der Zertifizierungsrichtlinien ist es für jeden Teilnehmer möglich, eine Einschätzung über die Qualität der ausgestellten Zertifikate zu treffen. Sie beschreiben die Mindestanforderungen und Abläufe der Zertifizierung und sind Teil der Vereinbarung zwischen der CA und den Benutzern. Daher sollte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

2 Import der CA-Zertifikate

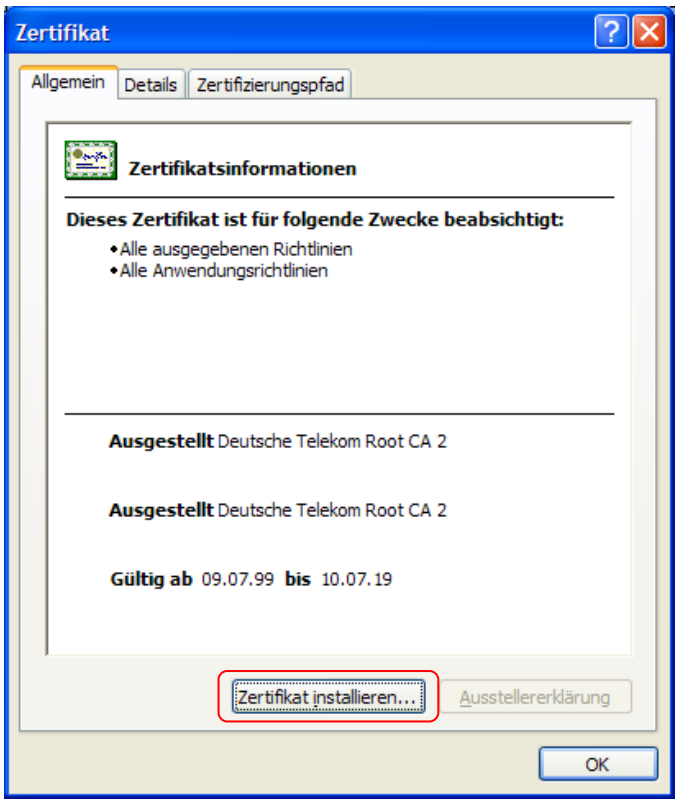
Bevor Sie Ihr persönliches Zertifikat beantragen, installieren Sie bitte per Mausklick die CA-Zertifikate der Zertifizierungshierarchie in Ihre Arbeitsumgebung wie unten beschrieben.

Klicken Sie als erstes unter dem Reiter **CA-Zertifikate** auf den Reiter **„Wurzelzertifikat“**. Dadurch wird das Wurzelzertifikat der Deutschen Telekom Root CA 2 in Ihren Browser importiert.

.

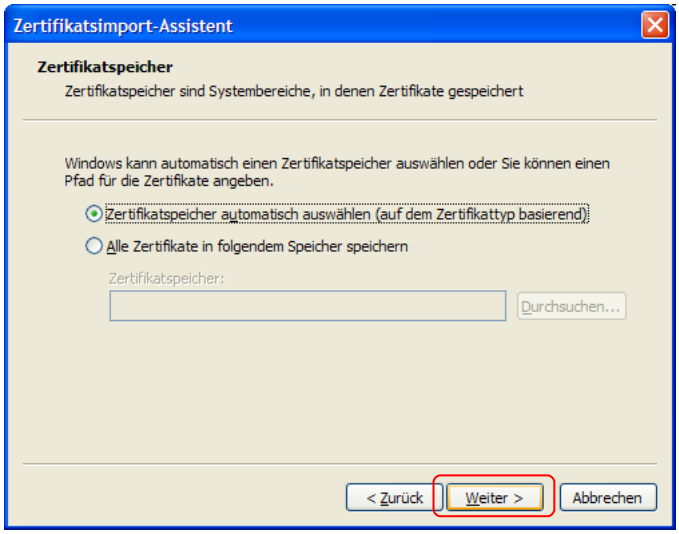


Es öffnet sich das nebenstehende Fenster. Wählen Sie **Öffnen**.

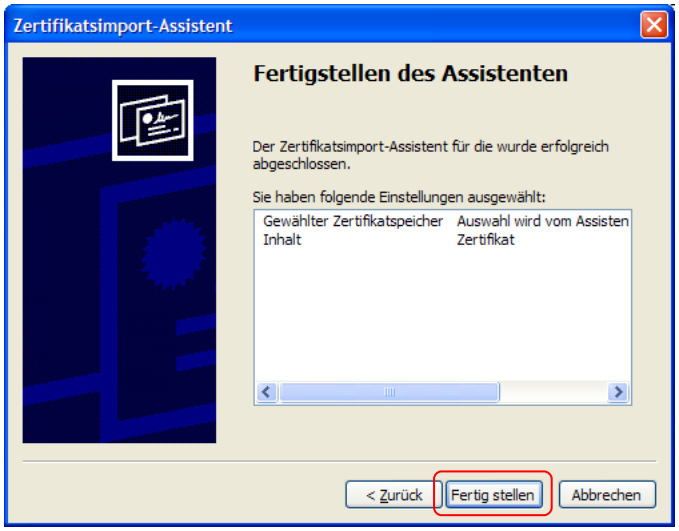


Wählen Sie **Zertifikat installieren**.

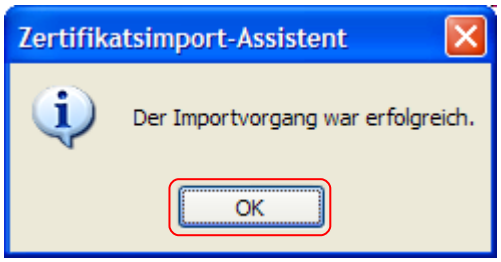
Das Zertifikat wird importiert. Wählen Sie **Weiter**.



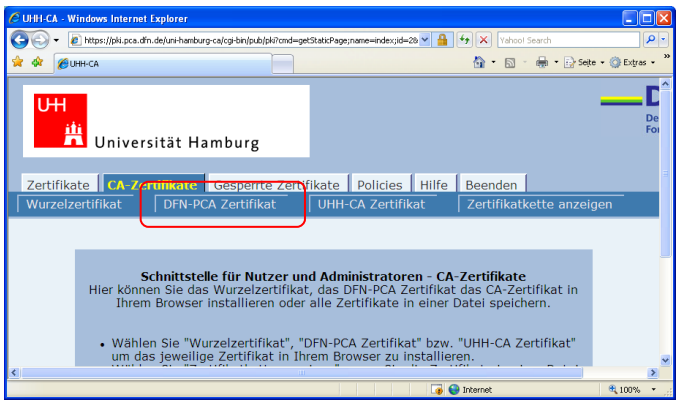
Wählen Sie Zertifikatspeicher automatisch wählen und dann **Weiter**.



Wählen Sie **Fertig stellen**.

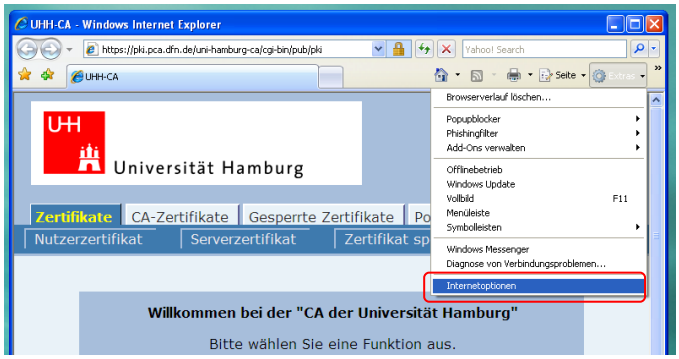


Bestätigen Sie mit **OK**.

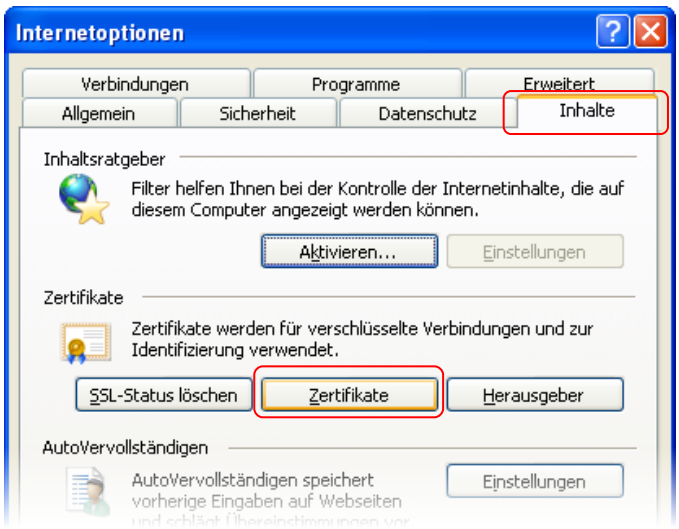


Klicken Sie dann im PKI-Portal auf den Reiter **„DFN-PCA Zertifikat“**. Dadurch wird das Zertifikat der DFN-Verein PCA Global in Ihren Browser importiert, nachdem Sie auch hier dem Installationsvorgang gefolgt sind wie oben für das Wurzelzertifikat im Detail beschrieben.

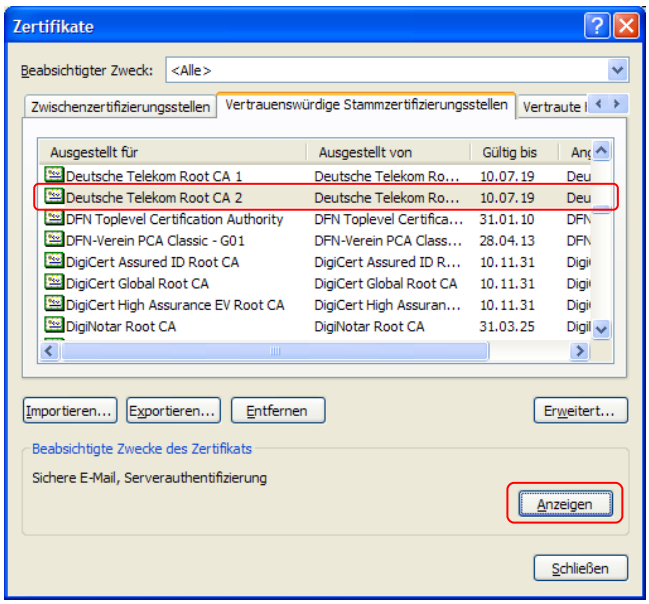
Verfahren Sie zuletzt ebenso mit dem Reiter **„UHH-CA Zertifikat“**. Dadurch wird das Zertifikat der CA der Universität Hamburg in Ihren Browser importiert, nachdem Sie auch hier dem Installationsvorgang gefolgt sind wie oben für das Wurzelzertifikat im Detail beschrieben.



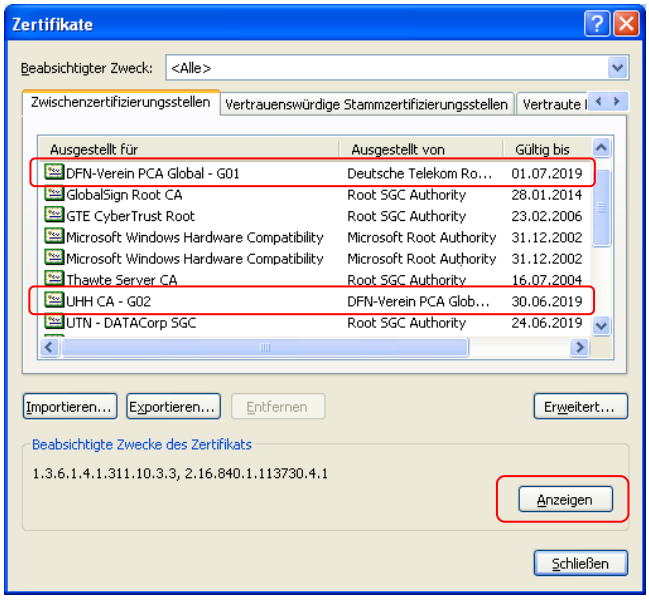
Nach der Installation der Zertifikate wird nun überprüft, ob diese richtig im Internet Explorer hinzugefügt wurden. Dazu öffnet man im Internet Explorer unter **Extras** die **Internetoptionen**.



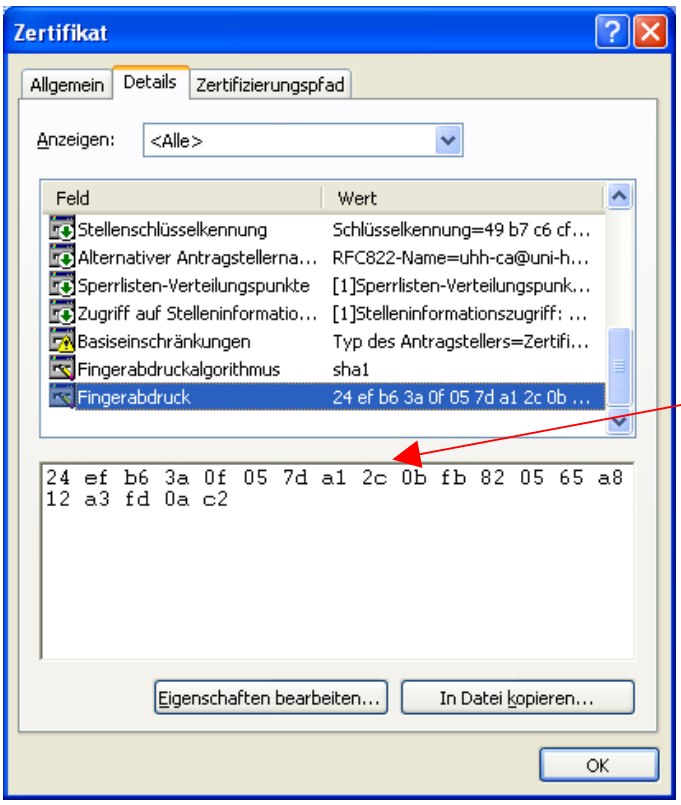
Wählen Sie unter dem Reiter **Inhalte** Zertifikate aus.



Unter dem Reiter **Vertrauenswürdige Stammzertifizierungsstellen** sollte das Zertifikat der **Deutschen Telekom Root CA 2** stehen.
Unter **Anzeigen** können Sie sich die Zertifikatsinformationen anzeigen lassen.



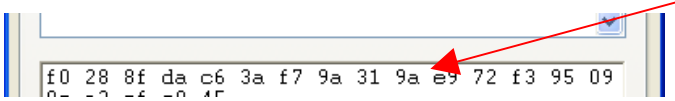
Unter dem Reiter **Zwischenzertifizierungsstellen** finden Sie das Zertifikat des **DFN-Verein PCA Global – G01** und das Zertifikat der **UHH CA – G02**
Mit dem Button **Anzeigen** können Sie sich die Zertifikatsinformationen ansehen.



Über **Anzeigen** -> **Details** erreichen Sie weitere Informationen zum Zertifikat wie z. B. den Fingerabdruck (fingerprint, Prüfsumme), ein charakeristisches Merkmal des Zertifikates.

Die angezeigten Fingerabdrücke der Zertifizierungsstellen sollten Sie mit den Angaben in diesem Dokument bzw. in einem anderen gedruckten Dokument der UHH CA - G02 abgleichen.

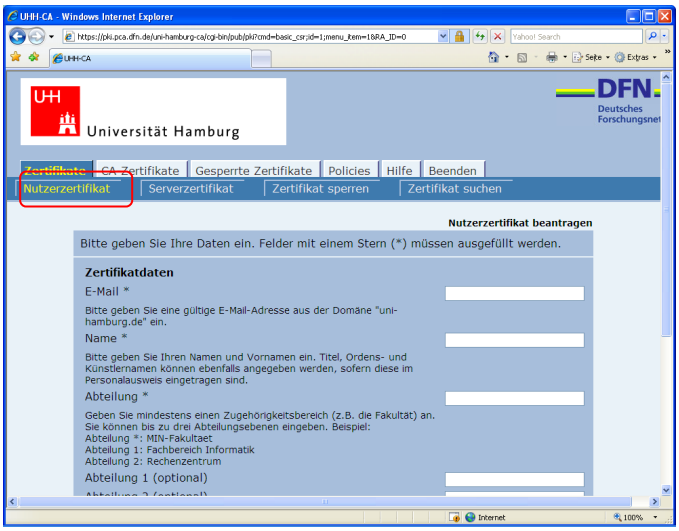
Fingerabdruck der UHH CA – G02



Fingerabdruck der DFN-Verein PCA Global – G01

3 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.

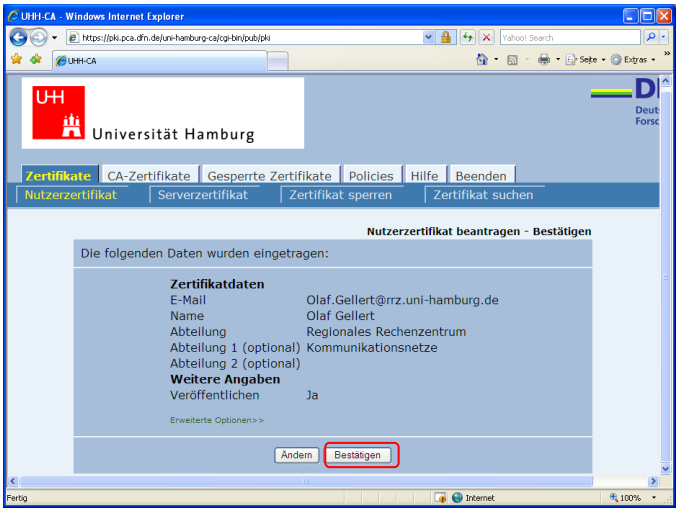


Füllen Sie den Antrag mit Ihren Daten aus und wählen Sie **Weiter**.

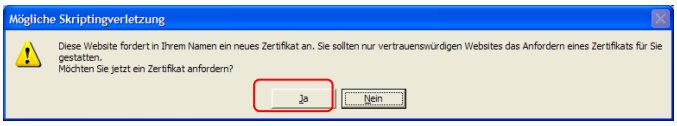
Unter **Zertifikatdaten** werden die Daten erfasst, die in das Zertifikat mit aufgenommen werden. Jedes Zertifikat beinhaltet u.a. einen eindeutigen Namen (Distinguished Name, DN). Dieser wird von den Feldern **E-Mail, Name** und **Abteilung** zusammen mit den festgelegten Einträgen O=Universitaet Hamburg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

Geben Sie auch eine PIN ein und bestätigen Sie diese noch einmal, stimmen Sie der Zertifizierungsrichtlinie zu und stimmen Sie bitte unbedingt auch einer Veröffentlichung Ihres Zertifikates zu. 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 der Veröffentlichung ihres Zertifikats zugestimmt haben.

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



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



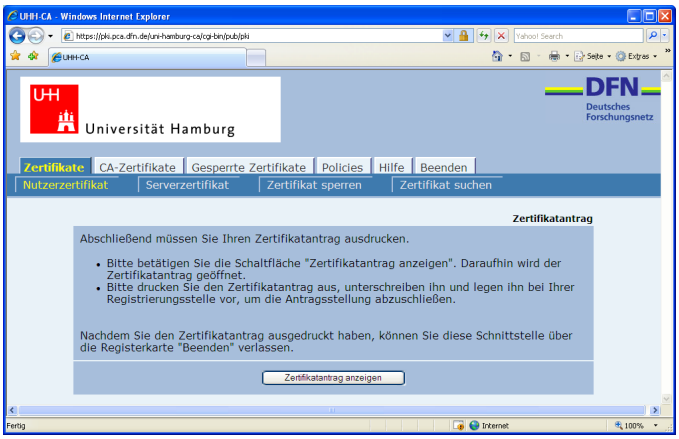
Bestätigen Sie mit **JA**.

Im Dialog „Ein neuer RSA-Austauschschlüssel wird erstellt“ sollte zunächst die Sicherheitsstufe eingestellt werden: Automatisch wird eine mittlere Sicherheitsstufe gewählt. Über den 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 **Schlüssel-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.

4 Aufsuchen des Rechenzentrums

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

Herr Olaf Gellert
Regionales Rechenzentrum der Universität Hamburg
Schlüterstraße 70
20146 Hamburg
Telefon: 040 - 42838 4694
Terminabsprachen sind für den Vertretungsfall auch unter -3095 und -3050 möglich!

Folgendes ist mitzubringen:

1. Der vollständig ausgefüllte Zertifikatantrag,
2. der Personalausweis oder Pass,
3. ein Dokument, das die Zugehörigkeit zur Universität bestätigt (z.B. gültiger Studierendenausweis).

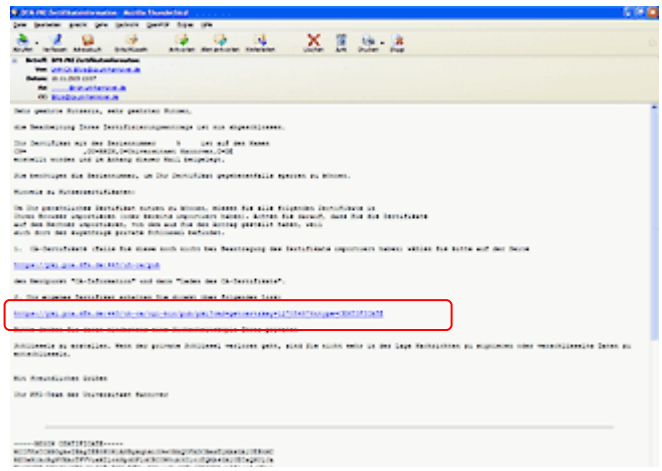
Wenn Sie den Mitarbeitern persönlich bekannt sind, kann auf das Dokument über die Zugehörigkeit (3.) verzichtet werden.

Prüfung und Beglaubigung des Zertifikatantrages:

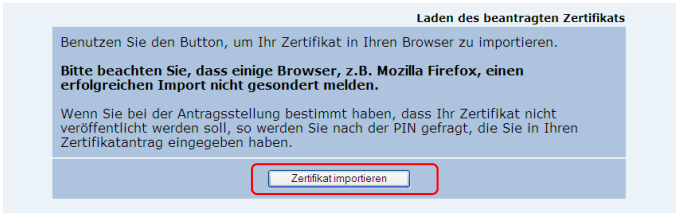
Nach Kontrolle des Zertifikatantrages wird dieser beglaubigt von der RA an die CA weitergeleitet. Dort wird das Zertifikat erstellt und Sie erhalten umgehend eine Benachrichtigung per E-Mail.

5 Antwort E-Mail und Zertifikat in den Browser importieren

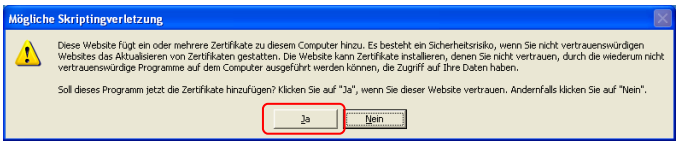
Nachdem die UHH CA Ihr Zertifikat erstellt hat, erhalten Sie eine Mail vom PKI-Team der Universität Hamburg…



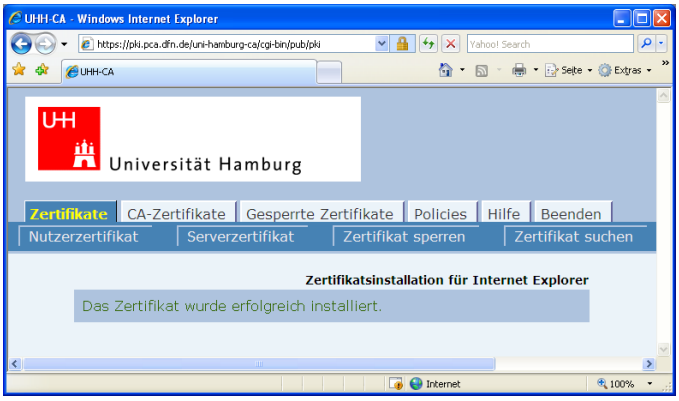
… mit der Information, dass Sie Ihr Zertifikat nun abholen können. Es reicht ein Mausklick auf den markierten Link, um Ihr persönliches Zertifikat in Ihren Browser zu integrieren.
Ihr Zertifikat ist außerdem noch als PEM-Datei als Anlage der E-Mail beigefügt (in diesem Format müssen Sie es aber nicht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



Sie werden nun aufgefordert, das Zertifikat zu importieren.



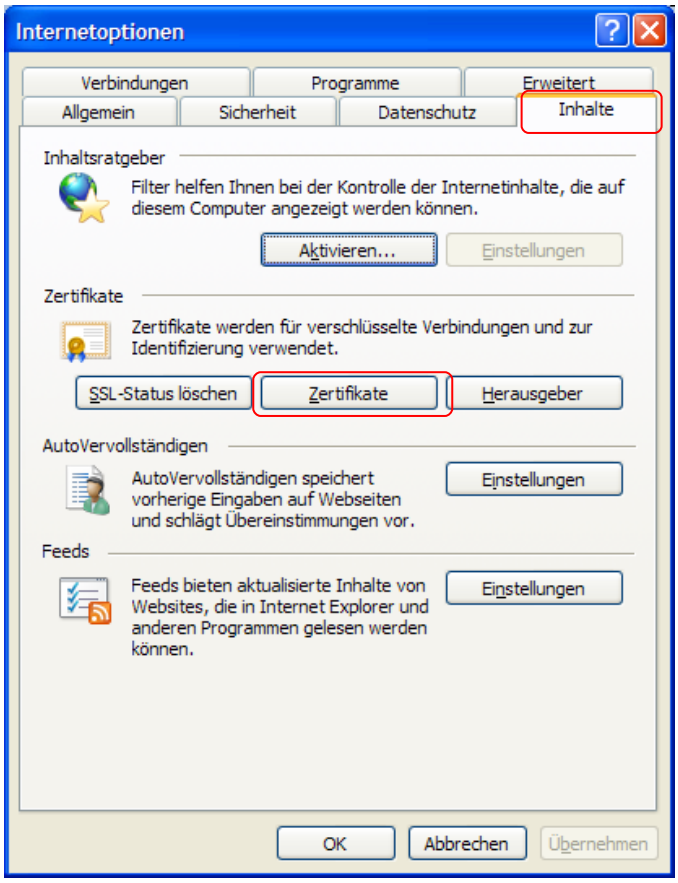
Bestätigen Sie mit JA.



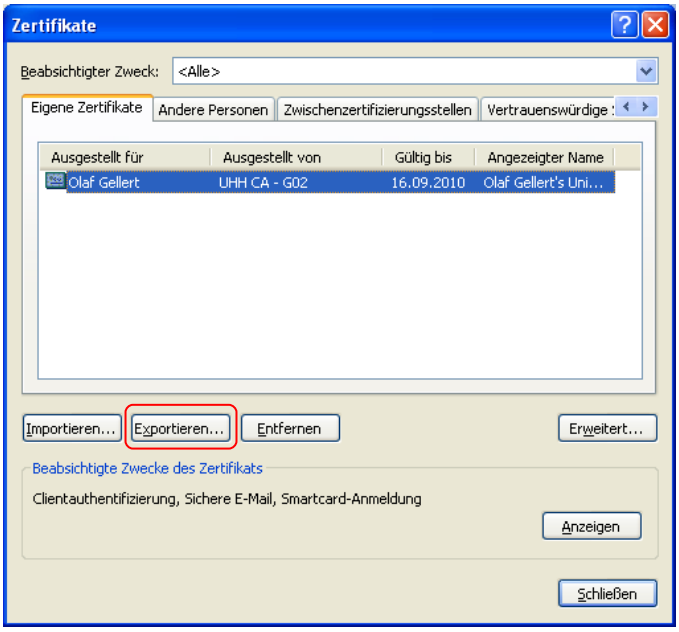
Das Zertifikat wurde erfolgreich importiert.

6 Sicherungskopie des privaten Schlüssels

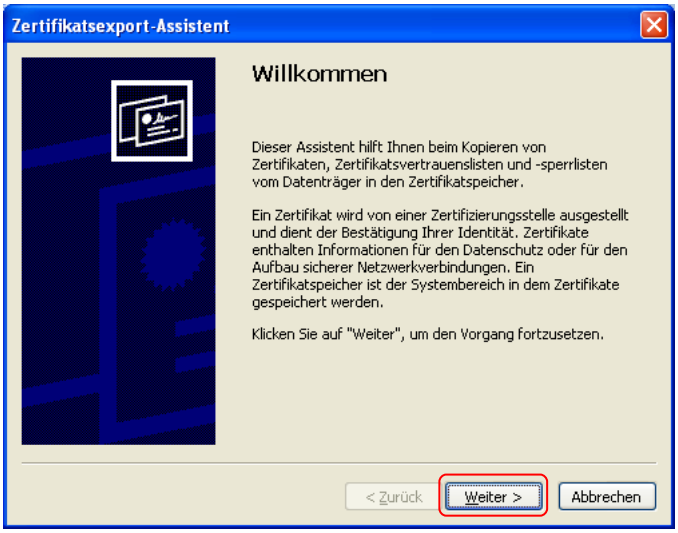
Für die folgenden Schritte wird ein USB-Stick oder eine leere Diskette benötigt (oder ein anderer externer Datenträger).



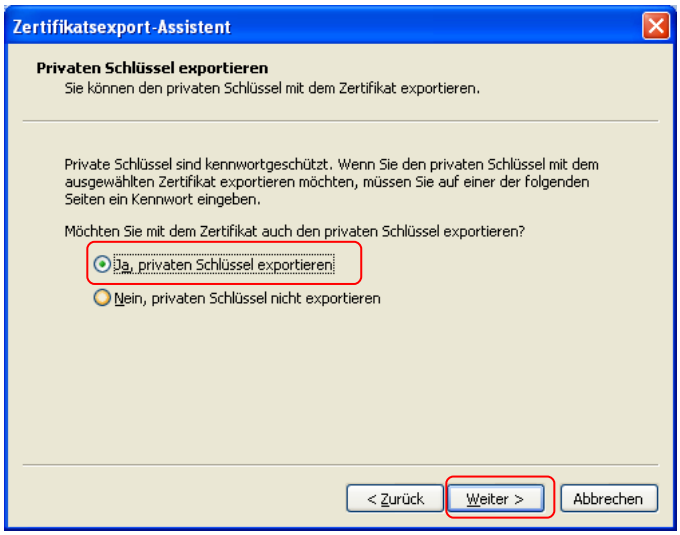
Unter **Extras-Internetoptionen** finden Sie den Reiter **Inhalte**. Klicken Sie hier bitte **Zertifikate** an.



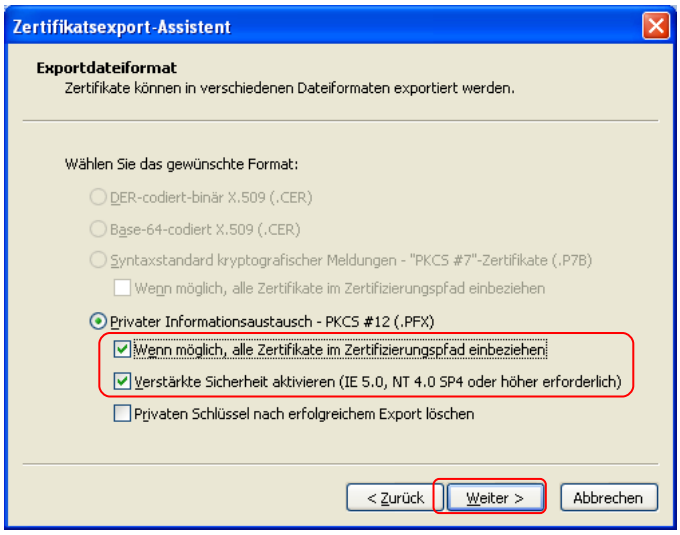
Unter **Eigene Zertifikate** sollte das eigene, von der UHH CA ausgestellte Zertifikat vorhanden sein. Wählen Sie Ihr neues Zertifikat von der UHH-CA aus und klicken Sie auf **Exportieren**.



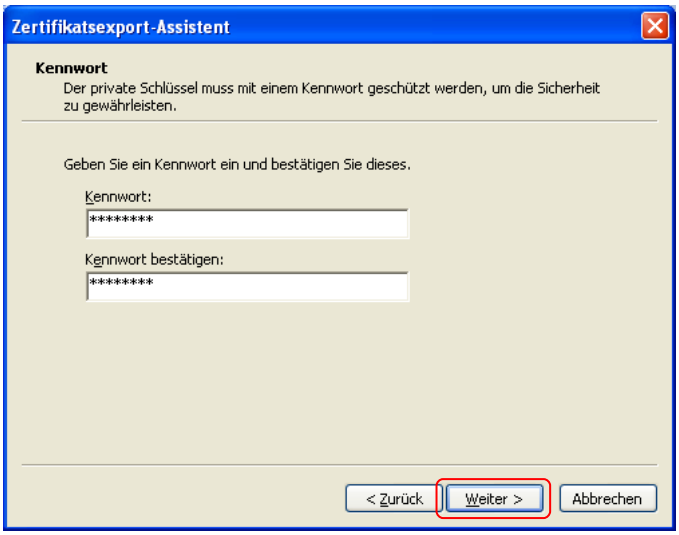
Es öffnet sich der Zertifikatsexport-Assistent. Wählen Sie **Weiter**.



Wählen Sie „**Ja**“ und bestätigen Sie mit **Weiter**.

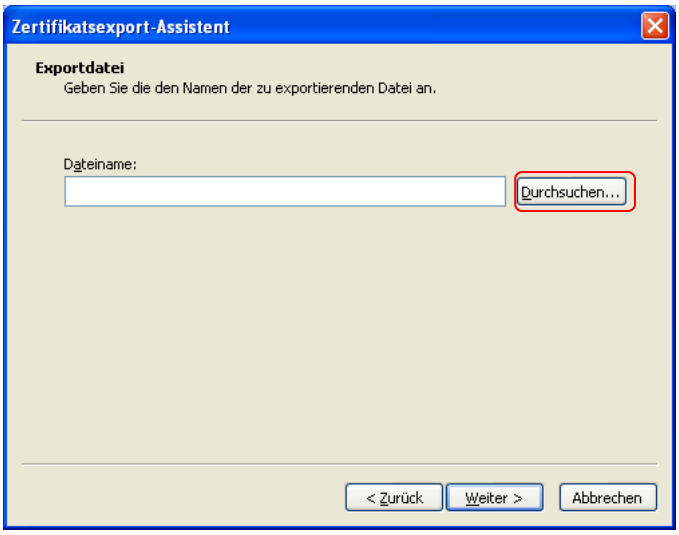


Setzen Sie bitte die beiden Haken. Bestätigen Sie mit **Weiter**.

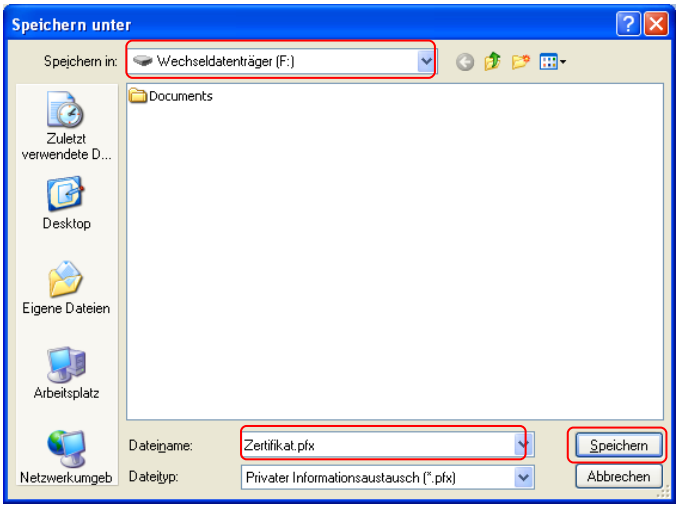


Da in dem Backup auch der private Schlüssel abgelegt wird, muss das Backup mit einem Kennwort gesichert werden. Geben Sie nun ein Backup-Kennwort ein und bestätigen Sie dieses noch einmal.

Das Kennwort ist frei wählbar. Sie müssen es unbedingt aufbewahren bzw. sich daran erinnern, wenn Sie Ihr Zertifikat später in einen anderen Browser oder E-Mail-Client importieren möchten.



Drücken Sie **Durchsuchen**.



Wählen Sie den Wechseldatenträger (USB-Stick) oder das Floppylaufwerk bzw. einen anderen externen Datenträger, geben Sie einen Dateinamen ein und drücken Sie **Speichern**. Sie gelangen zurück zum vorigen Dialog, den Sie mit **Weiter** fortsetzen.

Wählen Sie **Fertig Stellen**.

Wenn Sie die hohe Sicherheitsstufe für Ihren Schlüssel gewählt haben, erscheint eine Kennwort-Abfrage. Geben Sie das Schlüssel-Kennwort für den Schlüssel ein und bestätigen Sie mit **OK**.

Bestätigen Sie mit **OK**.

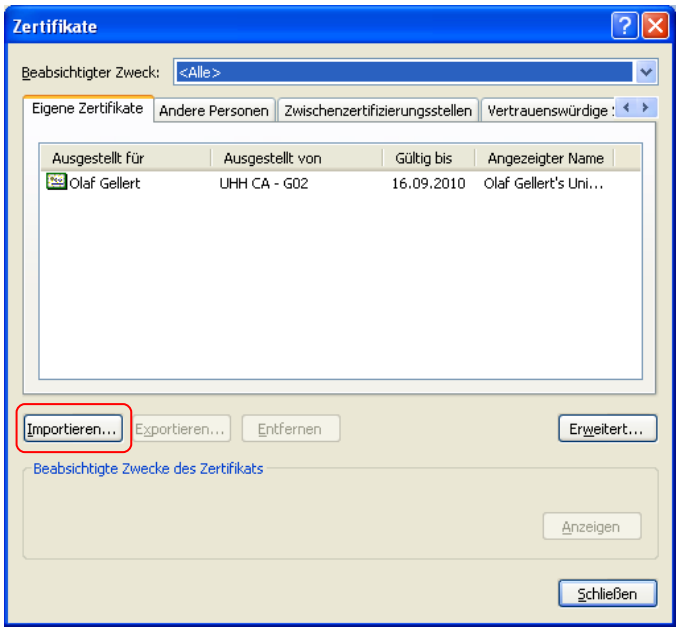
7 Wichtiger Hinweis zum Einstellen der Sicherheitsstufe

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 Kennwort 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.

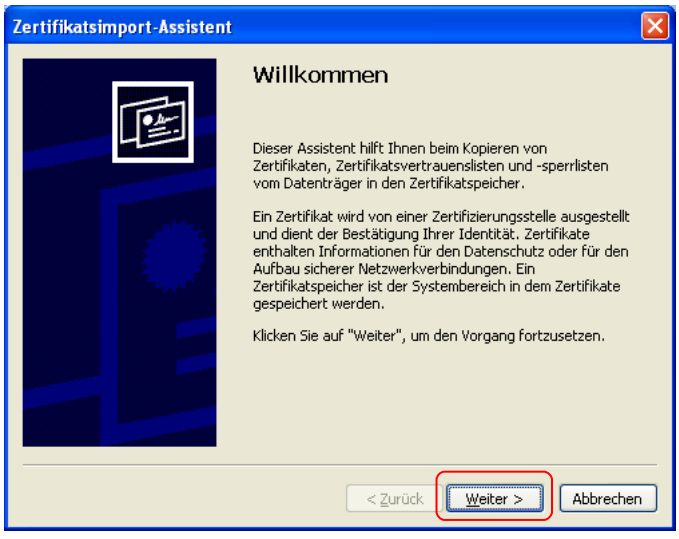
Darum sollte unbedingt immer die hohe Sicherheitsstufe eingestellt werden, um zu gewährleisten, dass für signierte Mails immer ein Kennwort abgefragt wird, so dass der oben beschriebene Fall nach Virusbefall, oder ähnlich gelagerter Missbrauch, verhindert wird.

So ändern Sie die Sicherheitsstufe für Ihren privaten Schlüssel: Windows hat keinen Mechanismus vorgesehen, um die Sicherheitsstufe zu verändern. Zum Ändern der Sicherheitsstufe wird der Schlüssel einfach erneut von der Sicherheitskopie importiert. Sie benötigen den USB-Stick oder die Diskette, auf der Sie ihren privaten Schlüssel gespeichert haben.

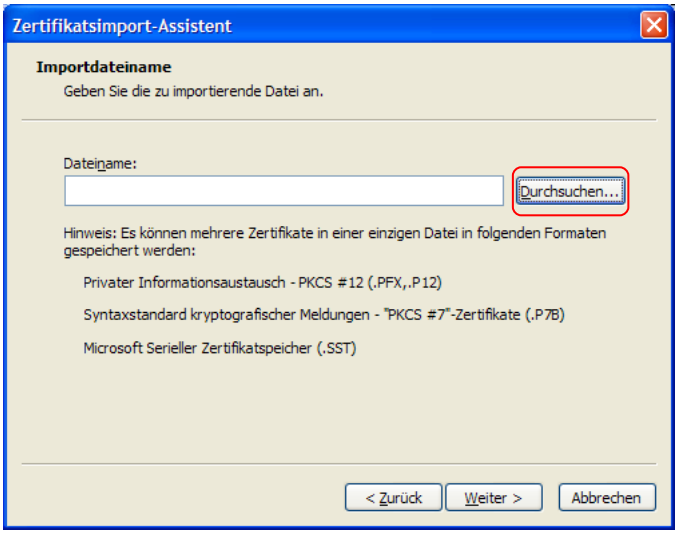


Wählen Sie im Menü des Internet Explorers unter **Extras** die **Internetoptionen**. Unter dem Reiter **Inhalte** wählen Sie den Button **Zertifikate.**

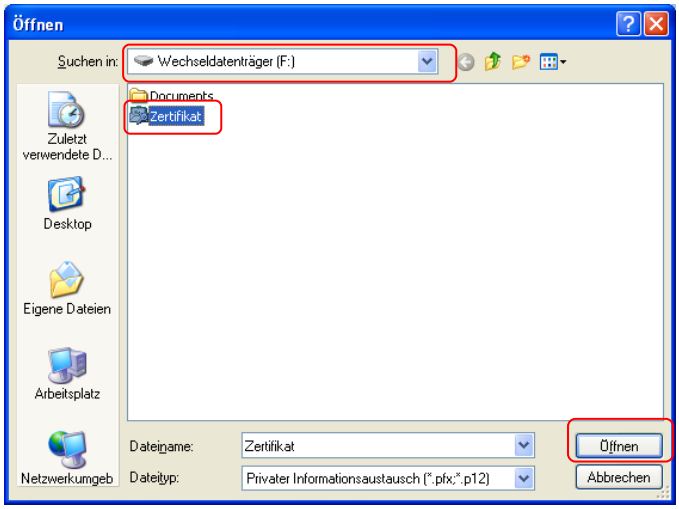
Unter **Eigene Zertifikate** sollte das eigene von der Universität Hamburg ausgestellte Zertifikat vorhanden sein. Der rot markierte Schalter **Importieren** wird erst nach der Auswahl des eigenen Zertifikates verfügbar.



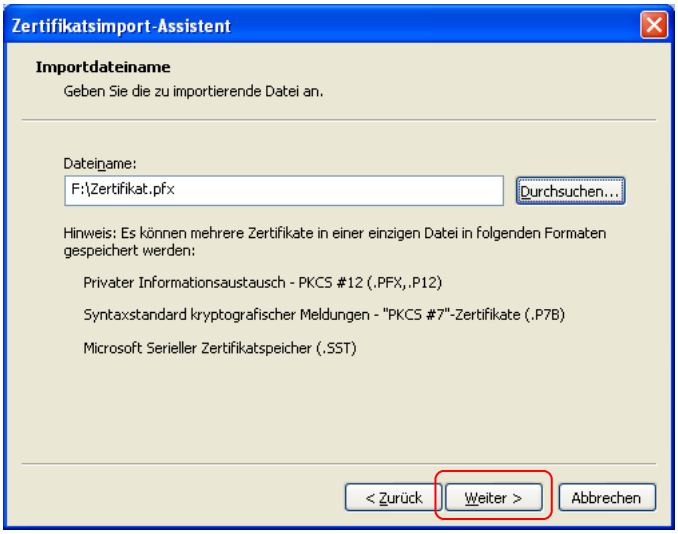
Es öffnet sich der Zertifikatsimport-Assistent.
Drücken Sie **Weiter**.



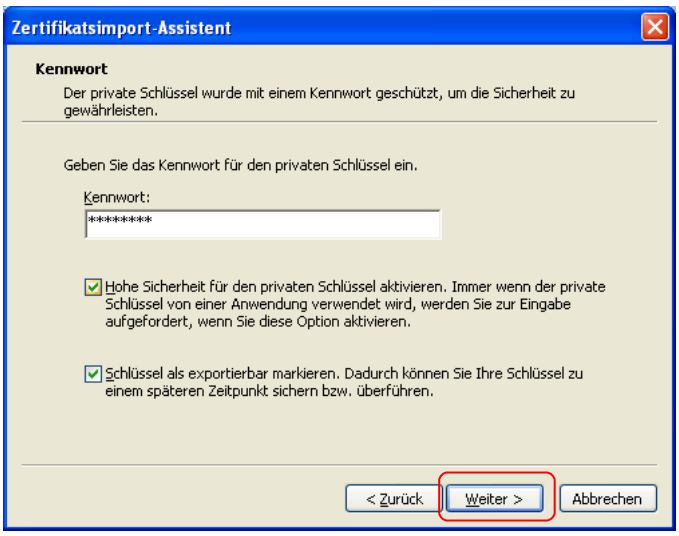
Wählen Sie **Durchsuchen**.



Wählen Sie unter „**Suchen in:**“ den Datenträger mit Ihrem Zertifikat (USB-Stick oder Diskette). Wählen Sie Ihr Zertifikat an und klicken Sie auf **Öffnen**.



Wählen Sie „**Weiter“.**

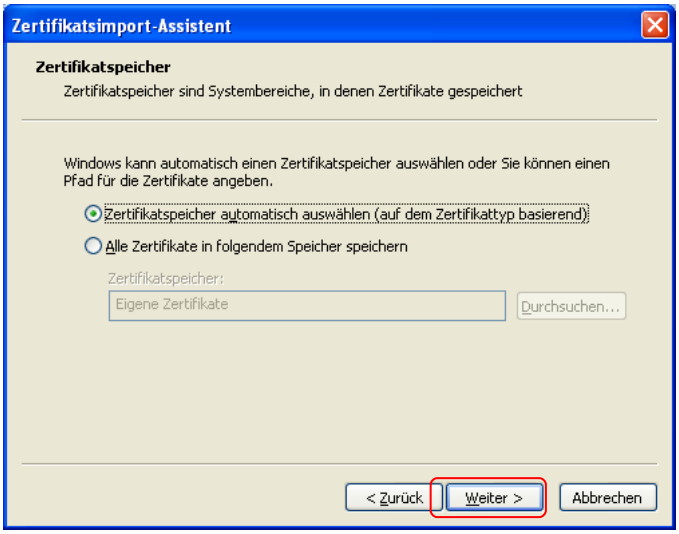


Setzen Sie das Häkchen für **Hohe Sicherheit und für Schlüssel als exportierbar markieren**. Geben Sie dann das **Backup-Kennwort** für Ihren privaten Schlüssel an, das Sie zuvor beim Exportieren benutzt haben.

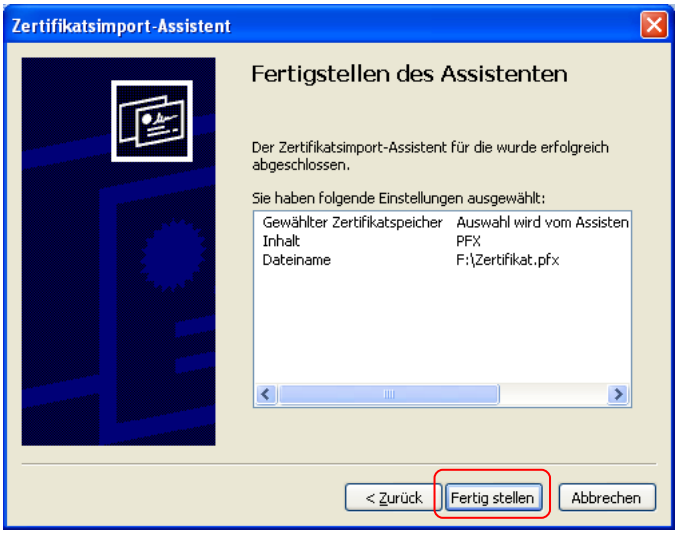
Dieses Kennwort ist nicht zu verwechseln mit dem Schlüssel-Kennwort für die hohe Sicherheitsstufe für Ihr Zertifikat.

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

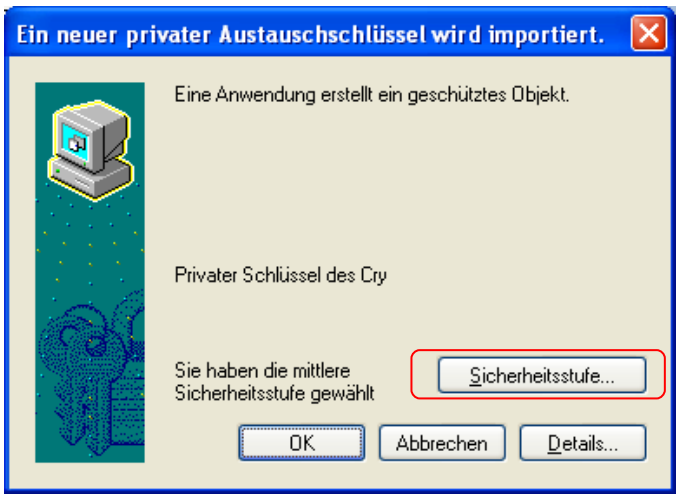
Drücken Sie **Weiter**.



Wählen Sie **Zertifikatsspeicher automatisch auswählen**.
Weiter



Wählen Sie **Fertig Stellen**.



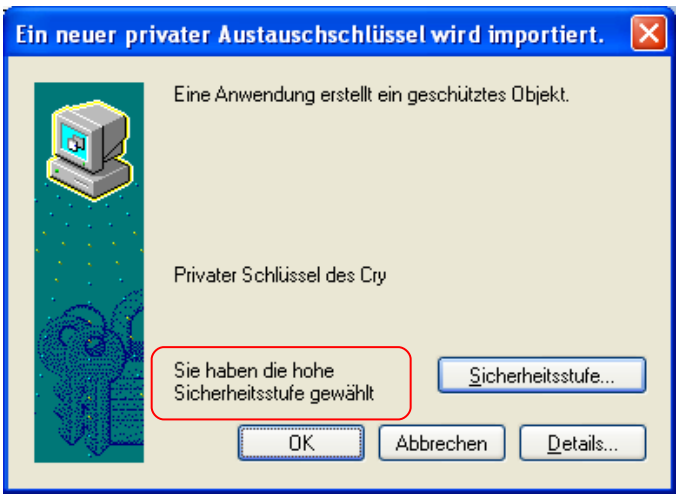
Jetzt können und sollen Sie die Sicherheitsstufe ändern.

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

Wählen Sie jetzt **Hoch**.

Sie werden nun zur Eingabe eines **Schlüssel-Kennwortes** aufgefordert. Damit wird der Kryptospeicher auf Ihrem Computer, der das eigene Zertifikat und den zugehörigen privaten Schlüssel 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