Benutzerhandbuch für die Beantragung und Verwendung von Zertifikaten mit Firefox /Thunderbird

Version 1.2 vom 15.09.2014

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!

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.

Im Folgenden soll den Benutzern der Zertifizierungsstelle der Universität Hamburg (UHH-CA) ein Leitfaden zur Zertifikatbeantragung und -verwendung mit Firefox / Thunderbird an die Hand gegeben werden.
Er enthält alle wichtigen Schritte, die zu einem gültigen Zertifikat innerhalb der Zertifizierungshierarchie des Deutschen Forschungsnetzes (DFN) führen.

Inhaltsverzeichnis

1 Einführung....2

1.1 Zertifizierungshierarchie....2

1.2 Das PKI-Portal des DFN....3

1.3 Die Zertifizierungsrichtlinien der Universität Hamburg....3

2 Import der CA-Zertifikate....5

2.1 Import der CA-Zertifikate in Firefox....5

2.2 Import der CA-Zertifikate in Thunderbird....9

3 Beantragen eines persönlichen Nutzer-Zertifikats....11

4 Aufsuchen des Rechenzentrums....13

5 Importieren des Zertifikats in den Browser / Mail Klienten....14

5.1 Importieren in Firefox....14

5.2 Importieren in Thunderbird....16

6 Sicherungskopie des privaten Schlüssels....18

7 Versenden einer signierten E-Mail....19

1 Einführung

1.1 Zertifizierungshierarchie

Für das Signieren und Verschlüsseln von E-Mail erhält jeder Benutzer 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 der 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.

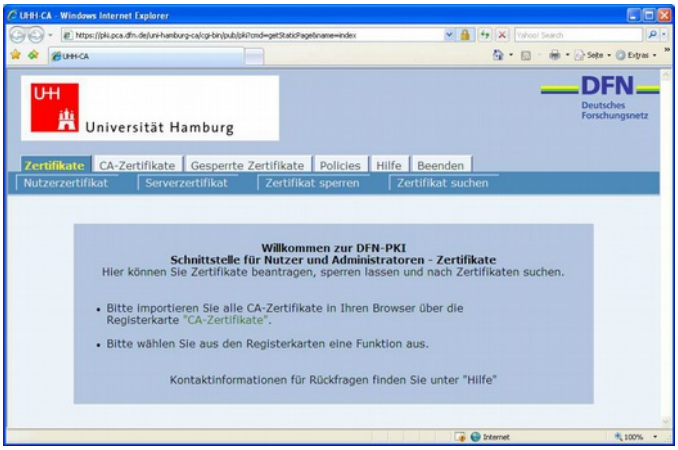
1.2 Das PKI-Portal des DFN

Das PKI-Portal des 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/de/services/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

1. ein Zertifikat beantragen,
2. ein Zertifikat zurückrufen und
3. Zertifikate suchen.

Desweiteren finden Sie hier

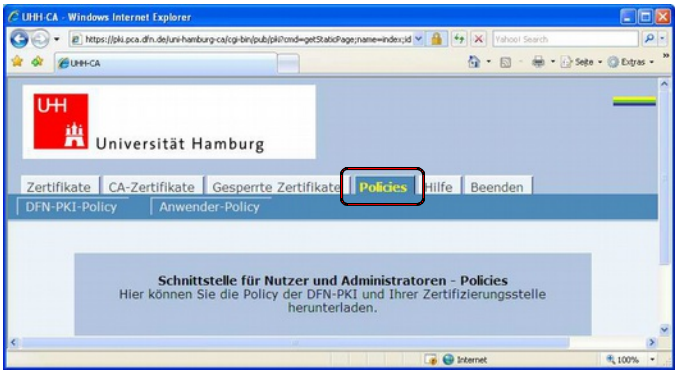
1. die Zertifizierungsrichtlinie,
2. die CA-Zertifikate und
3. die Zertifikat-Sperrlisten.

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.



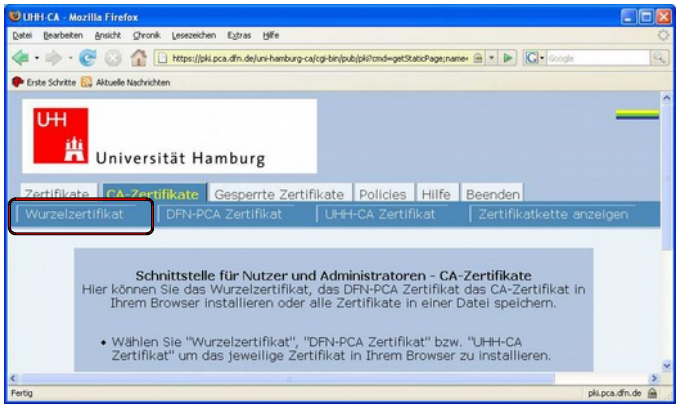
Mit Hilfe der Zertifizierungsrichtlinien ist es für jeden Teilnehmer möglich, eine Einschätzung über die Qualität der ausgestellten Zertifikate zu treffen. Sie beschreiben die Mindestanforderungen und Abläufe der Zertifizierung und sind Teil der Vereinbarung zwischen der CA und den Benutzern. Daher sollte 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 Ihren Browser (Firefox) und E-Mail Klienten (Thunderbird) wie unten beschrieben.

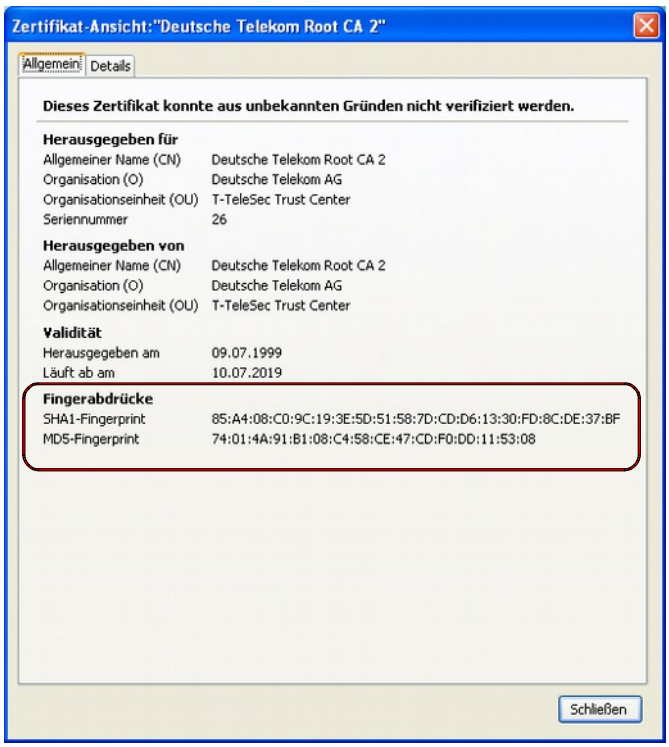
2.1 Import der CA-Zertifikate in Firefox

Weil es sich bei der Kombination Firefox/Thunderbird um zwei verschiedene Programme handelt, haben beide einen eigenen Zertifikatspeicher. Daher müssen die CA-Zertifikate in beide Programme eingebaut werden. Die Zertifikate werden zunächst per Mausklick in den Firefox Browser importiert. Dort wird ein Backup auf Diskette oder einen anderen externen Datenträger erstellt, anschließend werden die Zertifikate in Thunderbird importiert.



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.

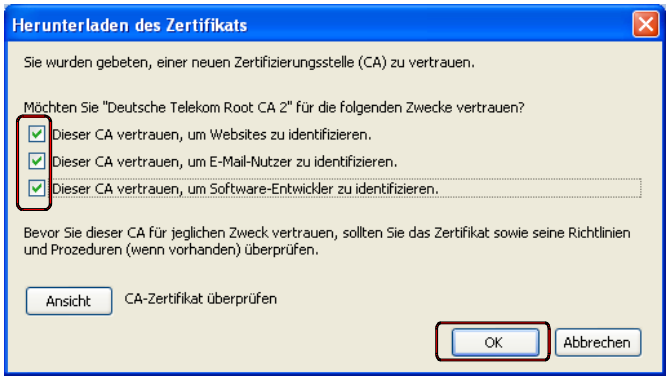
Zunächst aber öffnet sich das nebenstehende Fenster. Dort sollte als erstes der rot umrandete Button **Ansicht** betätigt werden, um den Inhalt des Zertifikates zu prüfen.



Da die CA-Zertifikate dem Browser nicht bekannt sind, werden sie auch noch nicht als vertrauenswürdig eingestuft.

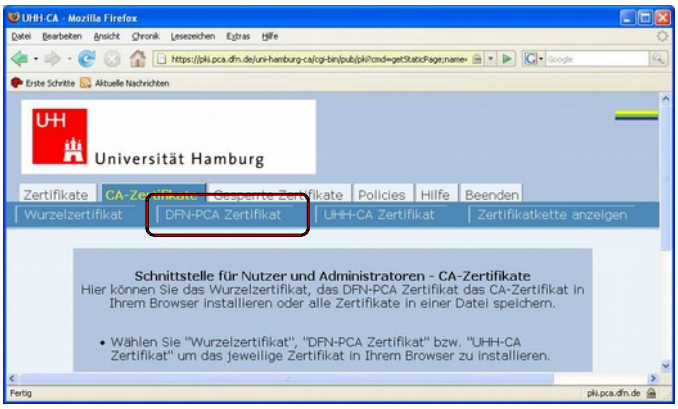
In diesem Fenster **Zertifikat Ansicht** sind die wichtigsten Informationen zu jedem Zertifikat enthalten: Unter **Herausgegeben für** wird der Inhaber des Zertifikates angezeigt, in diesem Fall die Deutsche Telekom Root CA 2. Unter **Herausgegeben von** derjenige, der das Zertifikat unterzeichnet hat, hier wieder die Deutsche Telekom Root CA 2, da es sich um ein selbstsigniertes Wurzelzertifikat handelt. Es folgt der Gültigkeitszeitraum, in dem das Zertifikat verwendet werden kann. Zuletzt werden die Prüfsummen (Fingerabdrücke) des Zertifikates angezeigt.

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

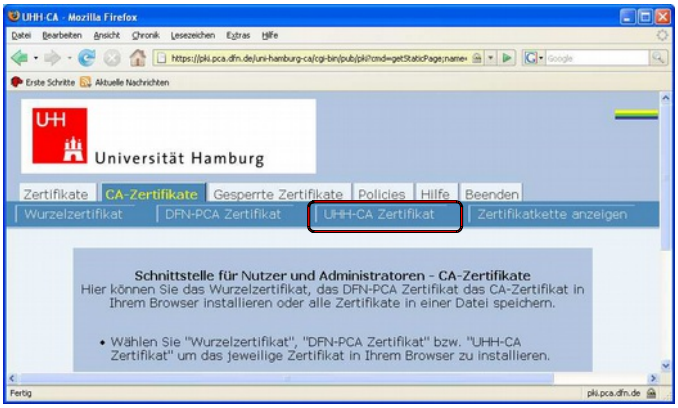


Nach dem Schließen des Anzeigefensters müssen jeweils die Zwecke des Zertifikates aktiviert werden, um es für die angegebenen Anwendungen als vertrauensvoll einzustufen.

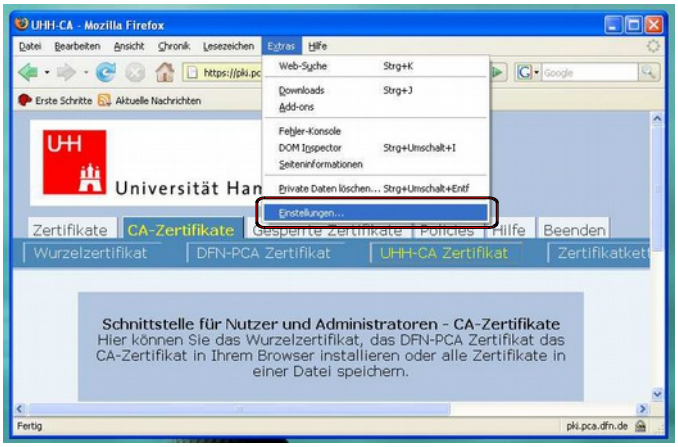
Bestätigen Sie danach mit **OK** und das Zertifikat wird in den Browser installiert.



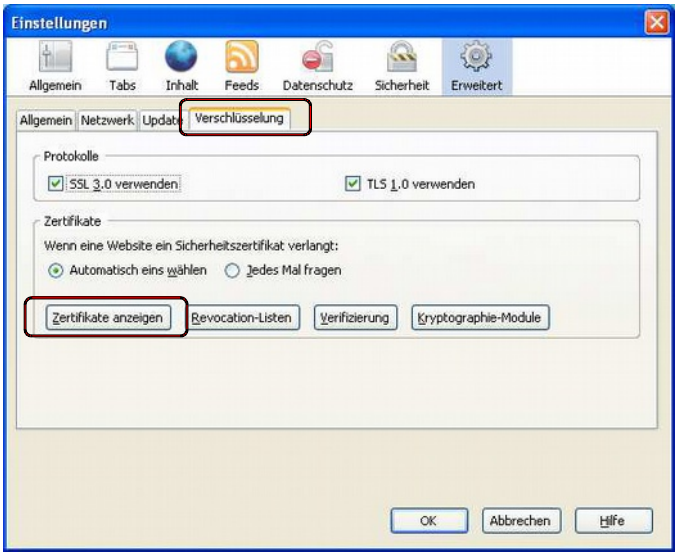
Klicken Sie dann auf den Reiter **„DFN-PCA Zertifikat“**. Dadurch wird das Zertifikat der DFN-Verein PCA Global in Ihren Browser importiert, nachdem Sie auch hier die Vertrauenswürdigkeit durch Aktivieren der Kontrollkästchen bestätigt haben.



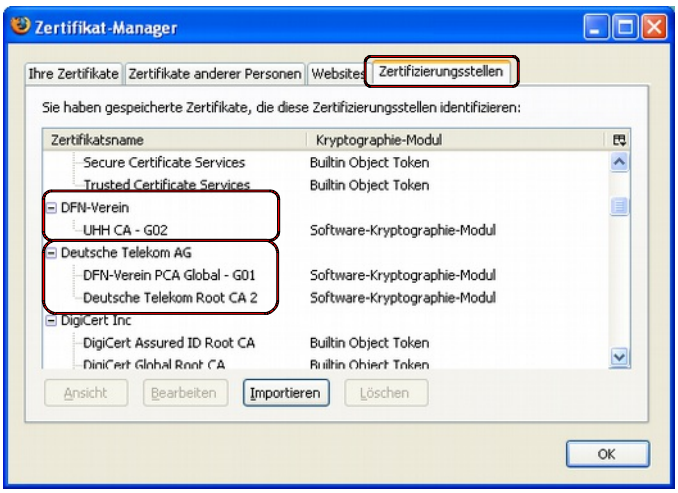
Zuletzt klicken Sie auf den Reiter **„UHH-CA Zertifikat“**. Dadurch wird das Zertifikat der CA der Universität Hamburg in Ihren Browser importiert, nachdem Sie auch hier die Vertrauenswürdigkeit durch Aktivieren der Kontrollkästchen bestätigt haben.



Zur Überprüfung, ob die CA-Zertifikate korrekt importiert worden sind, wählen Sie im Firefox-Menü unter **Extras** den Punkt **Einstellungen**.



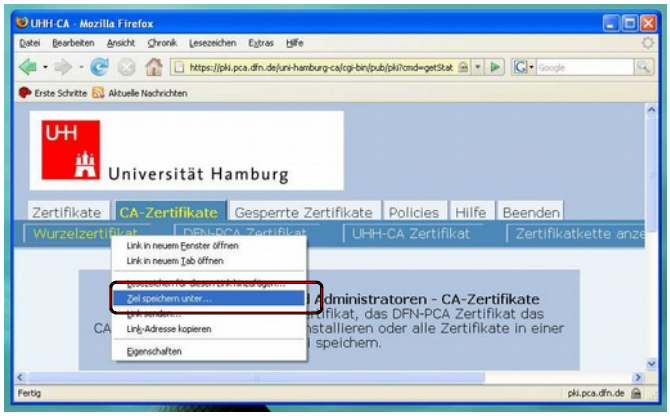
Hier öffnet man unter **Erweitert, Reiter Verschlüsselung,** den Button **Zertifikate anzeigen** mit dessen Hilfe man in den Zertifikats-Manager gelangt.



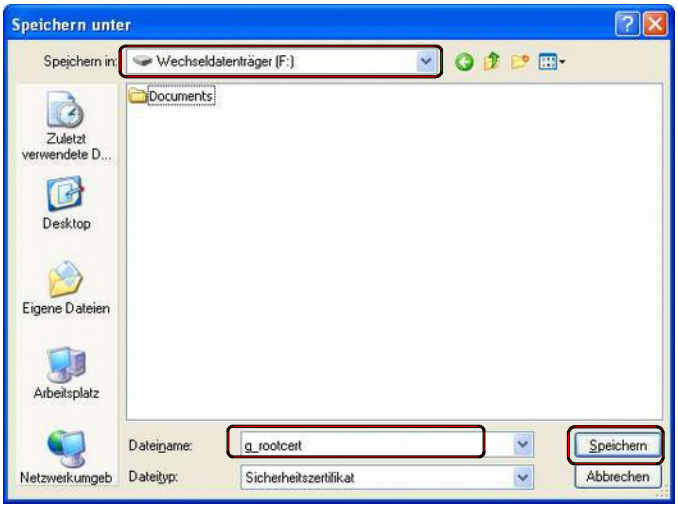
Wählen Sie den Reiter **Zertifizierungsstellen** aus.
Hier sollte sich jetzt unter der Überschrift **Deutsche Telekom AG** das Zertifikat der **Deutschen Telekom Root CA 2** und der **DFN-Verein PCA Global-G01** befinden und darüber unter der Überschrift **DFN-Verein** das Zertifikat der **UHH CA – G02**.

Damit sind die CA-Zertifikate der Zertifizierungshierarchie in Firefox installiert.

Um die CA-Zertifikate auch in Thunderbird verfügbar zu machen, müssen sie zunächst auf der Festplatte oder einem externen Datenträger zwischengespeichert werden. Da Sie aber Ihr eigenes Zertifikat unbedingt auf einem externen Datenspeicher zur Aufbewahrung sichern sollten, bietet es sich an, die CA-Zertifikate ebenfalls auf diesem externen Datenträger (z.B. auf Diskette, CD oder USB-Stick) zu speichern:



Klicken Sie auf im PKI-Portal (Reiter CA-Zertifikate) das **Wurzelzertifikat** mit der rechten Maustaste an und wählen Sie **Ziel speichern unter…** .



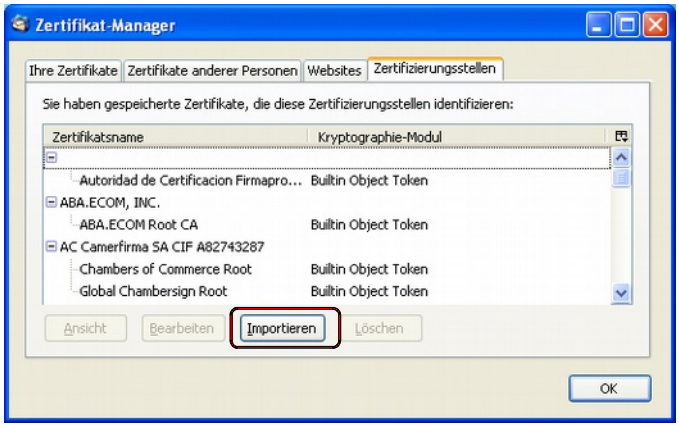
Legen Sie eine Diskette in das Laufwerk und **speichern** Sie dort das Zertifikat oder speichern Sie es auf einem anderen externen Datenträger.

Verfahren Sie ebenso mit dem DFN-PCA Zertikat und dem UHH-CA Zertifikat!

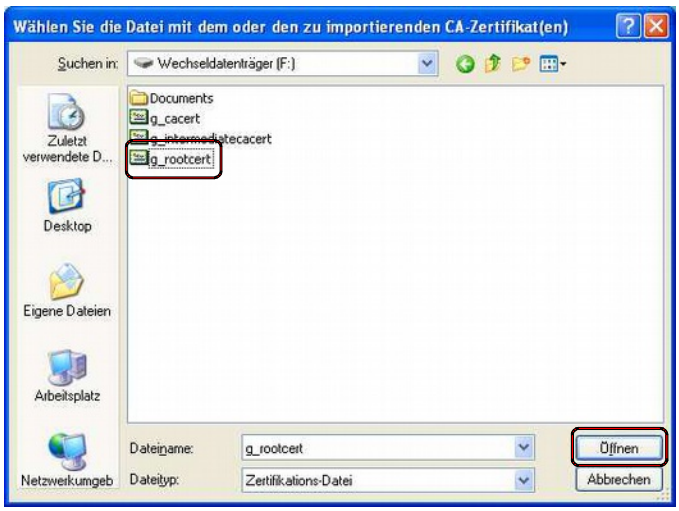
2.2 Import der CA-Zertifikate in Thunderbird

Jetzt installieren Sie die CA-Zertifikate in Ihren Mail Klienten Thunderbird. Öffnen Sie das Programm und gehen Sie im Menü unter **Extras** zu **Einstellungen**. Es öffnet sich folgendes Fenster:

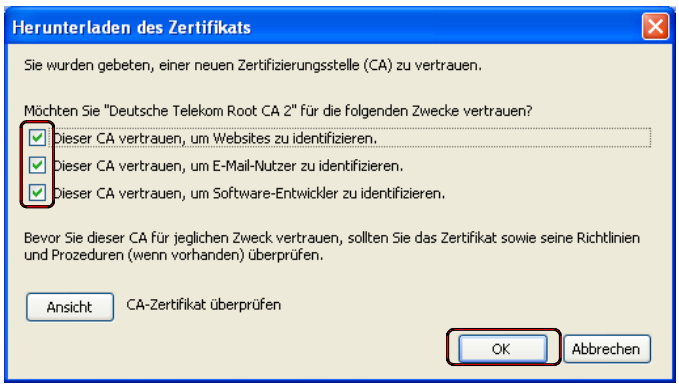
Dort klicken Sie unter **Erweitert** im Reiter **Zertifikate** auf den Button **Zertifikate** (je nach Thunderbird Version kann sich dieser auch unter **Datenschutz** im Reiter **Sicherheit** befinden).



Sie gelangen in den Zertifikat Manager. Unter dem Reiter **Zertifizierungsstellen** wählen Sie **Importieren**.



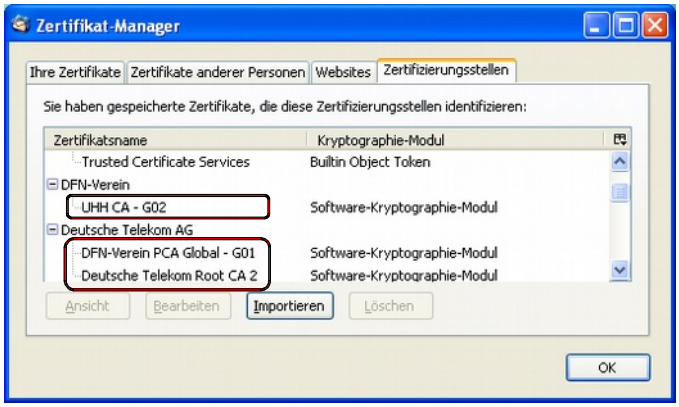
Markieren Sie das zuvor gespeicherte Wurzelzertifikat **g_rootcert.crt** und gehen Sie auf **Öffnen**.



Vertrauen Sie der Zertifizierungsstelle, indem Sie die drei Haken setzen. Drücken Sie **OK**. Das Zertifikat wird in Thunderbird importiert.

Wiederholen Sie den Vorgang mit den beiden anderen CA-Zertifikaten **g_intermediatecacert.crt** und **g_cacert_crt!**

Anschließend…



…finden Sie die CA-Zertifikate im Zertifikat-Manager von Thunderbird unter dem Reiter Zertifizierungsstellen.

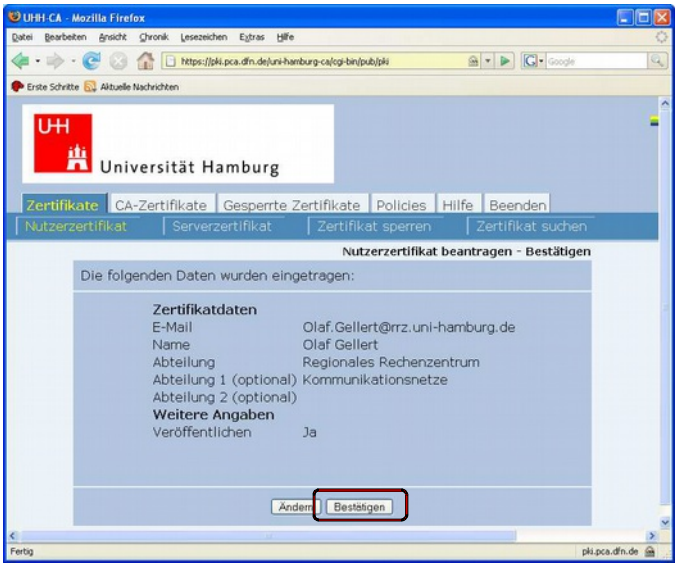
3 Beantragen eines persönlichen Nutzer-Zertifikats

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

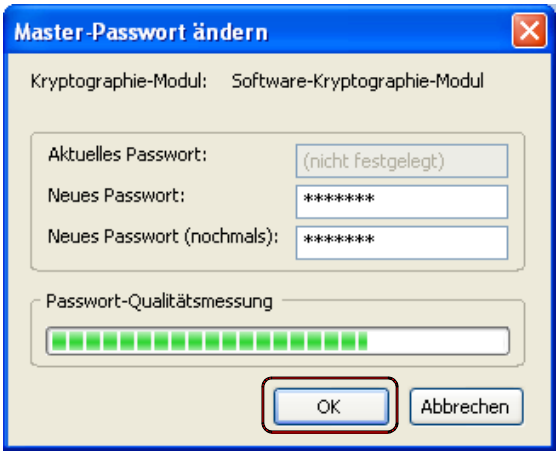
Füllen Sie bitte den Antrag mit Ihren Daten aus und wählen Sie **Weiter**.

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 Ihr Zertifikat veröffentlicht haben zugestimmt haben.

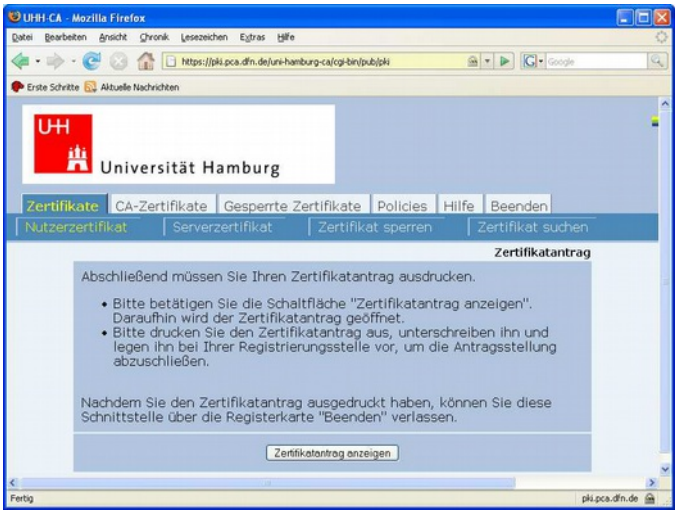


Wenn alle Angaben korrekt sind, bestätigen Sie mit **Bestätigen**.



Wenn Sie noch keine Zertifikate in Firefox verwalten, müssen Sie ein Master-Passwort für den internen Schlüsselspeicher wählen. Dieses wird später jeweils vor dem Verwenden oder Exportieren eines privaten Schlüssels abgefragt. Weiter geht es mit **Ok**.

Firefox 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.



Anschließend werden Sie 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 im RRZ (UHH-RA) auf.

Regionales Rechenzentrum der Universität Hamburg
Schlüterstraße 70
20146 Hamburg

Hr. J. Baftijari
Raum 417
Telefon: 040 - 42838 4625

Hr. R. Kurtz
Raum 408
Telefon: 040 - 42838 7977

Terminabsprachen sind für den Vertretungsfall auch unter -3097 (Herr Dr. C. Benecke).

Folgendes ist mitzubringen

1. Der vollständig ausgefüllte Zertifikatantrag,
2. der 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.

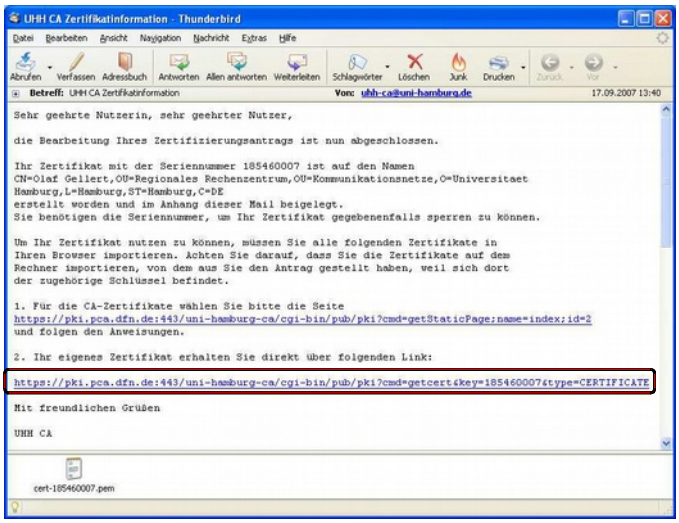
Prüfung und Beglaubigung des Zertifikatantrages

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.

5 Importieren des Zertifikats in den Browser / E-Mail Klienten

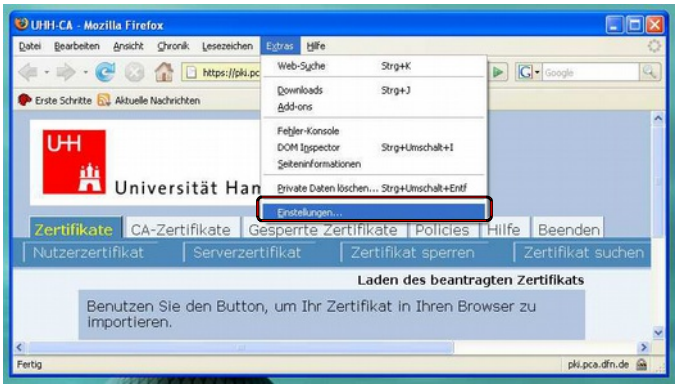
5.1 Importieren in Firefox

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

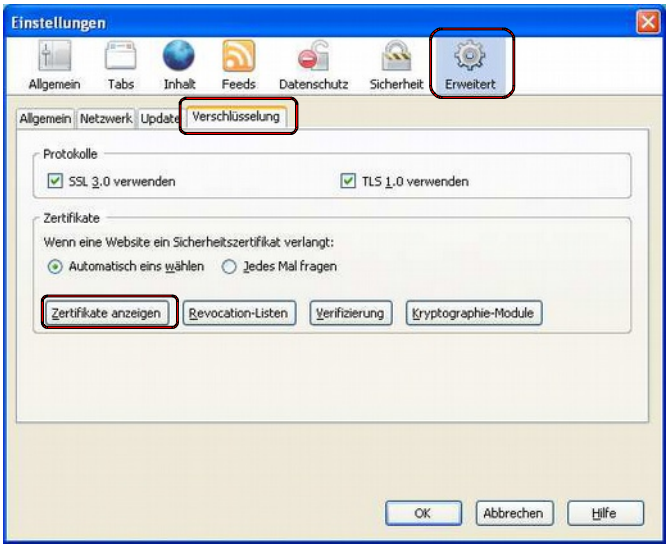


… mit der Information, dass Sie Ihr Zertifikat nun abholen können. Es reicht ein Mausklick auf den markierten Link, um Ihr persönliches Zertifikat in Ihren Browser zu integrieren.

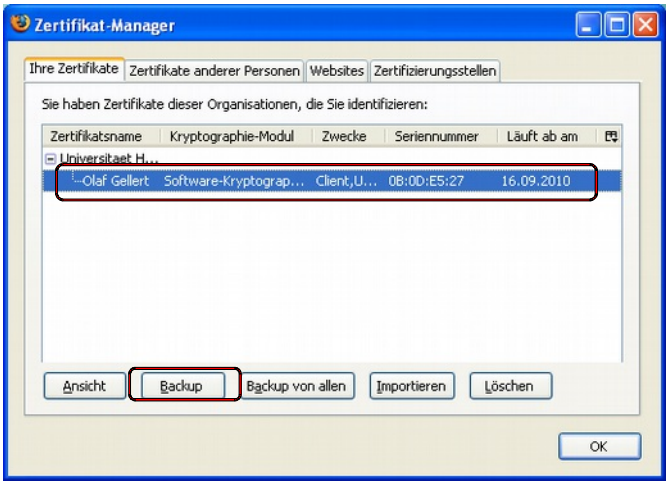
Ihr Zertifikat ist außerdem noch als PEM-Datei als Anlage der E-Mail beigefügt (in diesem Format müssen die Sie es aber nicht nutzen).



Nachdem Sie das Zertifikat in Firefox importieren haben, sollten Sie ein Backup für Thunderbird machen, denn hier wollen Sie es ja hauptsächlich für das Signieren und Verschlüsseln von E-Mail benutzen. Gehen Sie bitte im Programm Firefox, Menü **Extras,** auf **Einstellungen.**

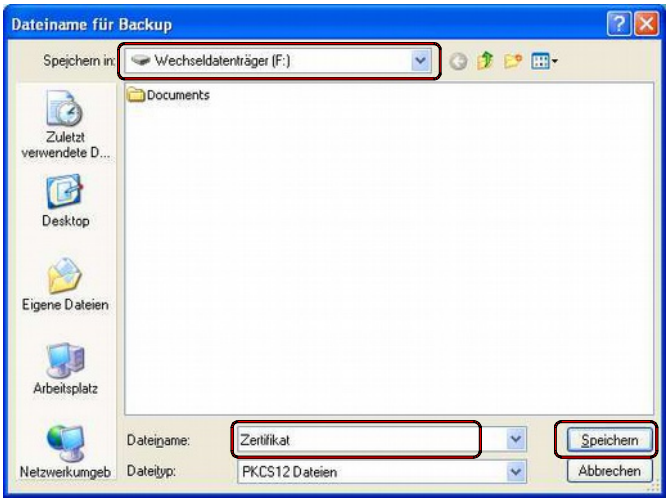


Wählen Sie unter **Erweitert** den Reiter **Verschlüsselung**. Drücken Sie den Button **Zertifikate anzeigen**.



Unter dem Reiter **Ihre Zertifikate** sollte Ihr eigenes Zertifikat angezeigt werden.

Sichern Sie Ihr Zertifikat z. B. auf einem USB-Stick, indem Sie es markieren und **Backup** auswählen.



Geben Sie einen Dateinamen an und speichern Sie die PKCS12 Datei auf dem USB-Stick oder einem anderen externen Datenspeicher.

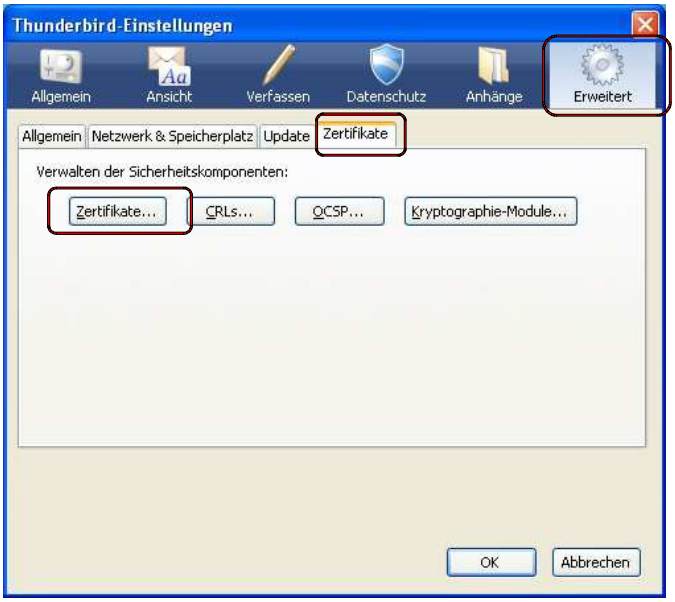
Firefox fragt Sie noch einmal nach dem Master-Passwort für den Zertifikatspeicher. Bestätigen Sie danach mit **OK**.

Geben Sie ein **Backup-Passwort** für die Backup Datei ein und bestätigen Sie dieses noch einmal. Mit **OK** schließen sie den Dialog.

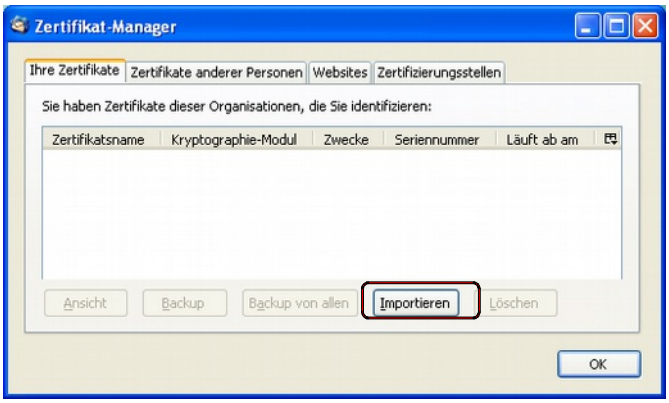
Bestätigen Sie mit **OK**.

5.2 Importieren in Thunderbird

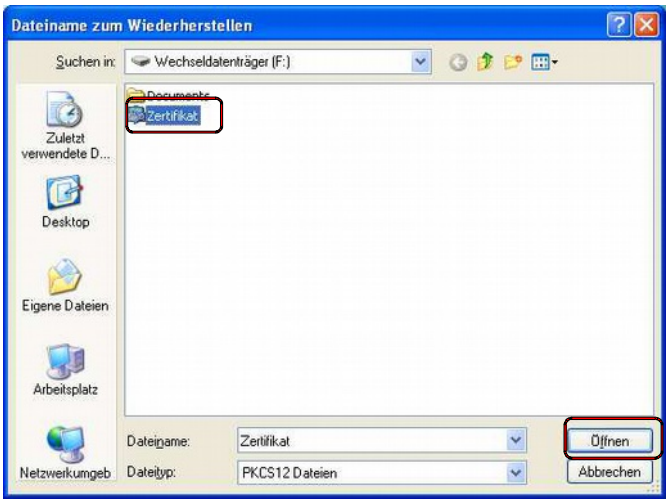
Um Ihr persönliches Zertifikat in den Zertifikatspeicher von Thunderbird zu importieren, öffnen Sie das Programm und wählen unter **Extras** den Punkt **Einstellungen**.



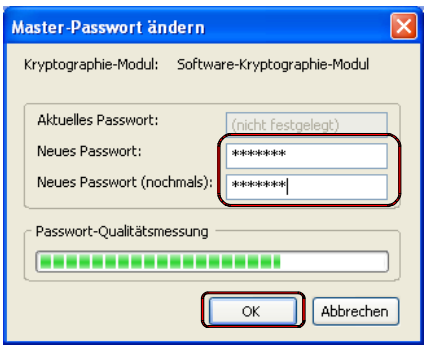
Wählen Sie unter **Erweitert** den Button **Zertifikate**.



Unter dem Reiter Ihre Zertifikate drücken Sie den Button **Importieren**.



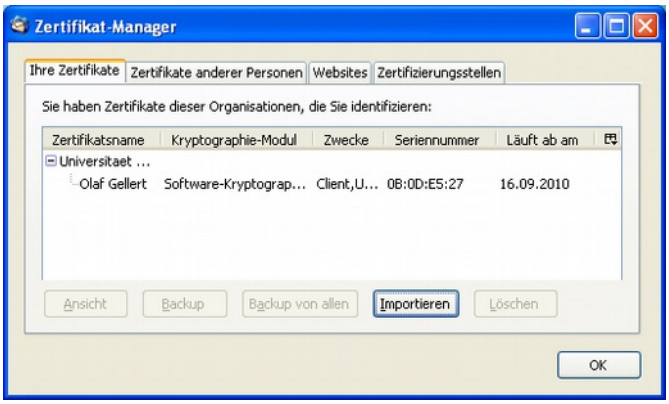
Wählen Sie das von Ihnen gespeicherte Zertifikat und gehen Sie auf **Öffnen**.



Wenn Sie noch keine Zertifikate in Thunderbird benutzt haben, werden Sie aufgefordert, ein Master-Passwort für den Zertifikatspeicher von Thunderbird zu wählen. Dieses wird später für den Zugriff auf den Schlüssel beim Signieren und Entschlüsseln von Mails abgefragt. Nach zweimaliger Eingabe des Passworts bestätigen Sie mit **OK**.

Geben Sie das von Ihnen beim Exportieren auf Firefox vergebene **Backup-Passwort** an und wählen Sie **OK**.

Bestätigen Sie mit **OK**.



Ihr eigenes Zertifikat wurde in den Zertifikatspeicher von Thunderbird importiert.

6 Sicherungskopie des privaten Schlüssels

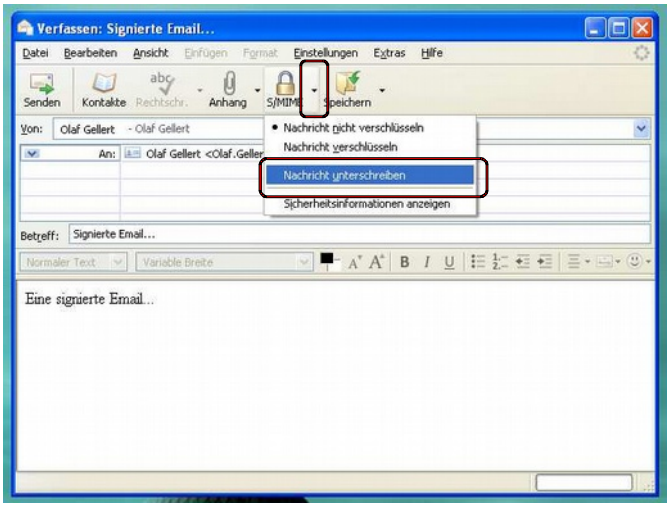
Verwahren Sie den externen Datenträger mit den Zertifikaten an einem sicheren Ort!

Die Datei, welche Sie dort vorhalten, beinhaltet nicht nur Ihr Zertifikat, sondern auch Ihren privaten Schlüssel. Der private Schlüssel wird zusammen mit dem Zertifikat vom System für das Signieren von E-Mail und für das Entschlüsseln von an Sie verschlüsselt gesendete Mails eingesetzt. Er muss deshalb geschützt werden! Bei Missbrauch durch Dritte ist das Zertifikat hinfällig! Mit einer Kopie des Schlüssels kann der Angreifer eine falsche Identität vortäuschen und vertrauliche Daten entschlüsseln.

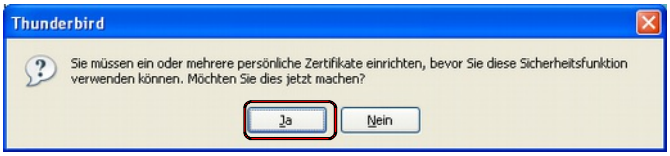
Ihre Anwendungen Firefox und Thunderbird speichern außerdem den privaten Schlüssel in einer Software-PSE (Private Security Environment). Hierbei handelt es sich um einen passwortgeschützten, sicheren Bereich. So steht Ihnen komfortabel und sicher die Signier- und Verschlüsselungsfunktionalität von Mozilla Thunderbird jederzeit zur Verfügung.

7 Versenden einer signierten E-Mail

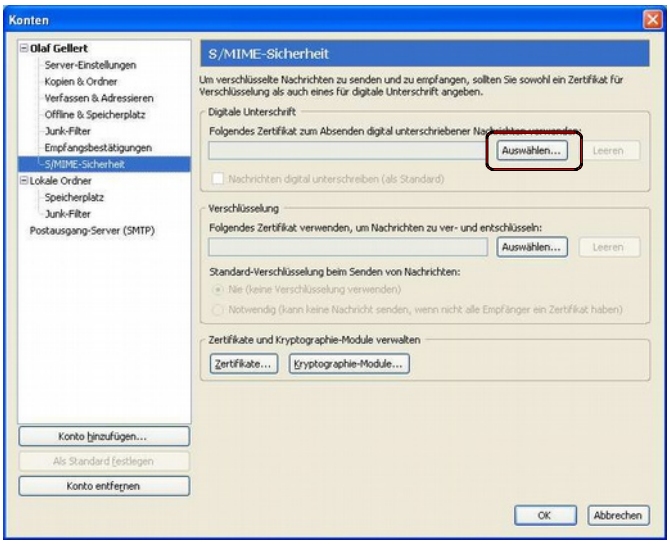
Mit Ihrem Zertifikat können Sie nun E-Mails, die Sie versenden, digital signieren. Damit kann der Empfänger sicher sein, dass es sich wirklich um eine E-Mail von Ihnen handelt. Das Ver- und Entschlüsseln von E-Mails wird in der Anleitung zum Einrichten des LDAP-Verzeichnisdienstes beschrieben. Zum Signieren einer E-Mail erstellen Sie diese wie gewohnt mit Thunderbird. Vor dem Absenden...



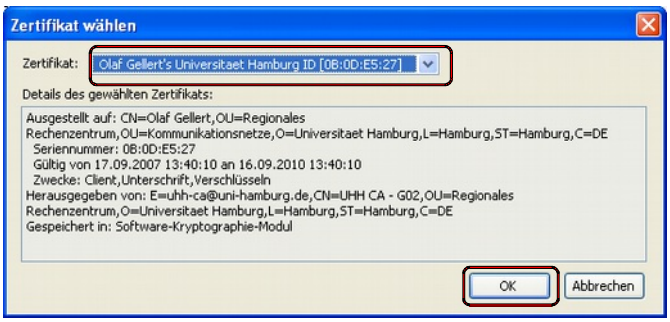
... klicken Sie auf den kleinen Pfeil nach unten im Button **SMIME.** In dem erscheinenden Menü wählen Sie den Eintrag **Nachricht unterschreiben**.



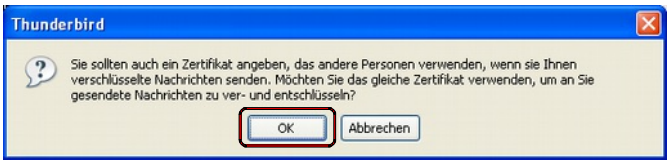
Wenn Sie noch keine signierten E-Mails verschickt haben, fragt Thunderbird, ob Sie Ihr Zertifikat einrichten wollen. Wählen Sie **Ja**.



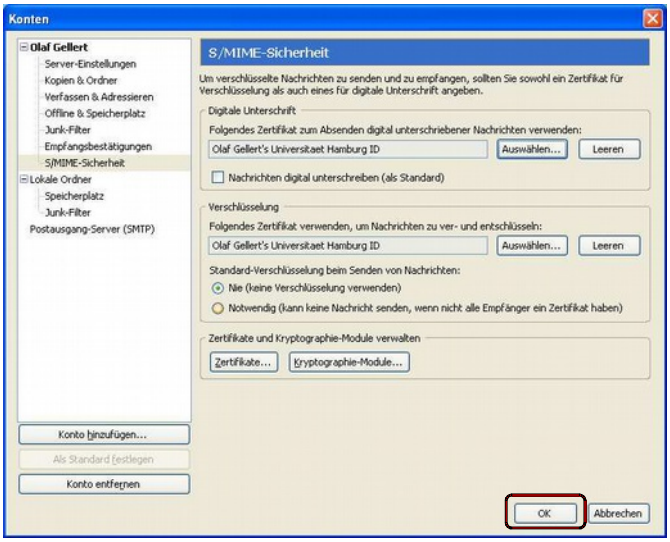
Im Dialogfeld wählen Sie unter **Digitale Unterschrift** den Button **Auswählen**.



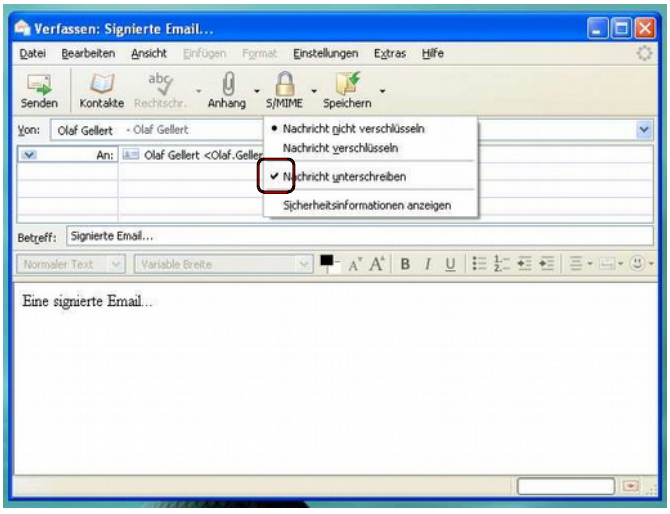
Wählen Sie Ihr Zertifikat an und bestätigen mit **OK**.



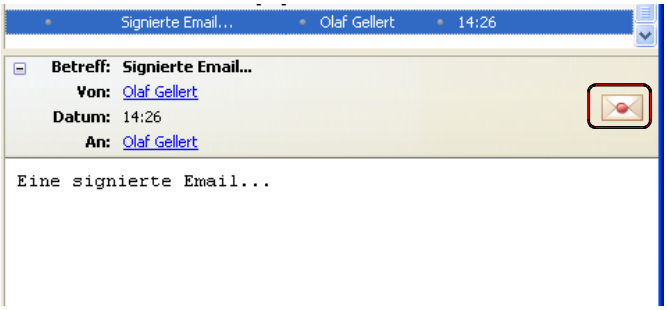
Ihr Zertifikat sollte auch für die Verschlüsselung von E-Mails eingesetzt werden. Wählen Sie **OK**.



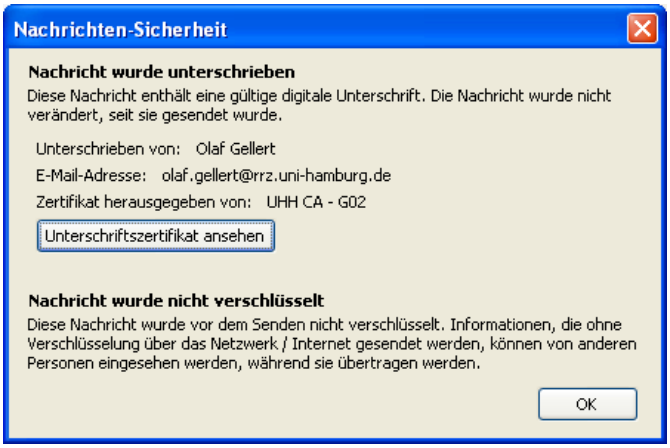
Das Zertifikat ist nun für digitale Unterschrift und Verschlüsselung ausgewählt Bestätigen Sie mit **OK**.



Wenn Sie erneut das Menü des Buttons SMIME aufrufen, sehen Sie ein Häkchen bei „**Nachricht unterschreiben**“. Beim Senden der Mail wird diese signiert.



Wenn Sie eine signierte E-Mail empfangen, wird Ihnen dies symbolisch in der Kopfzeile der E-Mail angezeigt. Wenn Sie das Symbol anklicken...



... wird der genaue Status der Signatur angezeigt.