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

Im Folgenden soll den Benutzern der Zertifizierungsstelle der Leibniz Universität Hannover (UH-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.

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 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 der 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 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

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.

Sie finden hier auch

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

1.3 Die Zertifizierungsrichtlinien der Leibniz Universität Hannover

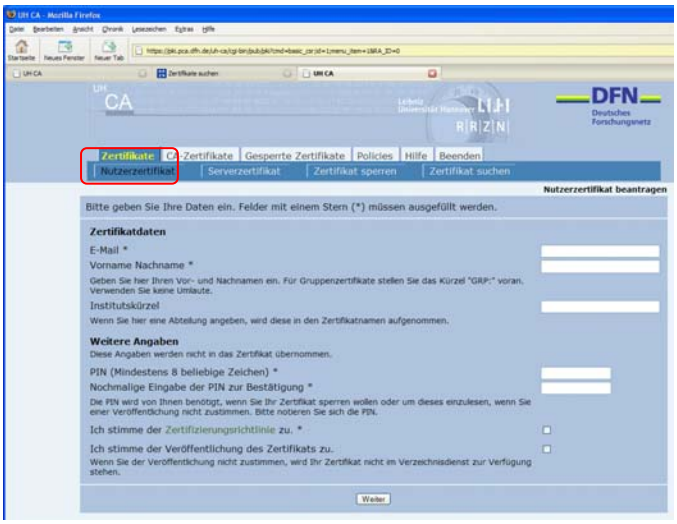
Eine Zertifizierungsrichtlinie (Certification Policy, CP) definiert die Regeln, nach denen eine oder mehrere Zertifizierungsstellen arbeiten. Die in der Leibniz Universität Hannover angesiedelte Zertifizierungsstelle (UH-CA) formuliert ihre Zertifizierungsrichtlinie in der Weise, dass die „Zertifizierungsrichtlinie 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, G03) 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

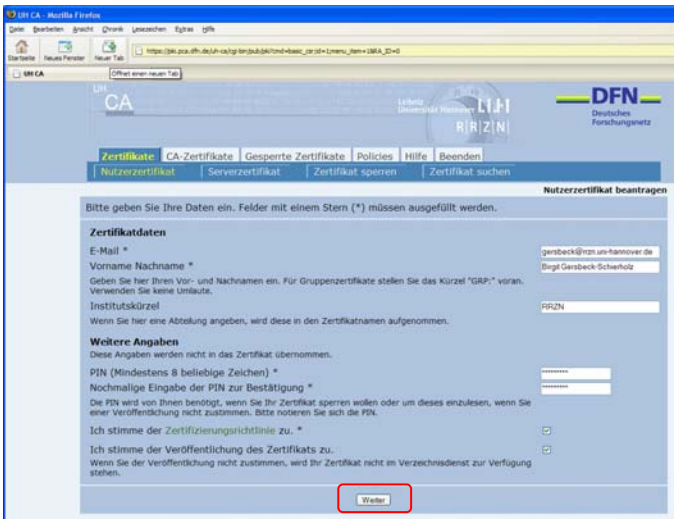
Für die Beantragung Ihres persönlichen Nutzer-Zertifikates, wählen Sie im PKI-Portal des DFN unter dem Reiter **Zertifkate** den Punkt **Nutzerzertifikat** aus, der zum folgenden Fenster führt.



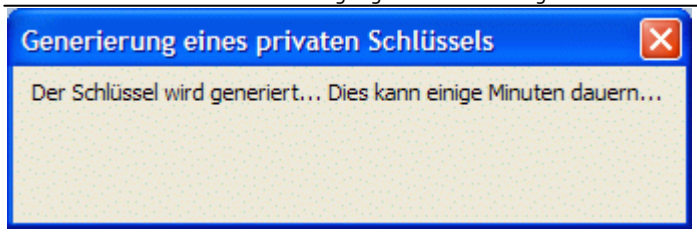
Füllen Sie bitte den Antrag mit Ihren Daten aus und wählen Sie **Weiter**.

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 **Institutskürzel** zusammen mit den festgelegten Einträgen O= Leibniz Universitaet Hannover 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. Bei Nichtzustimmung benötigen Sie eine Begründung. 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**.



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.

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.

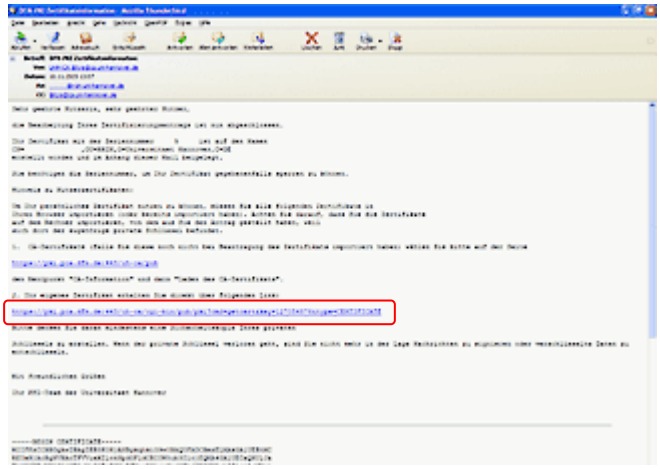
Prüfung und Beglaubigung des Zertifikatantrages:

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

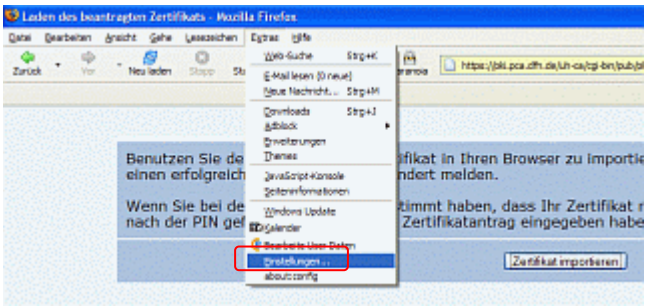
4 Das persönliche Zertifikat in den Browser/Mail Klienten importieren

4.1 Importieren in Firefox

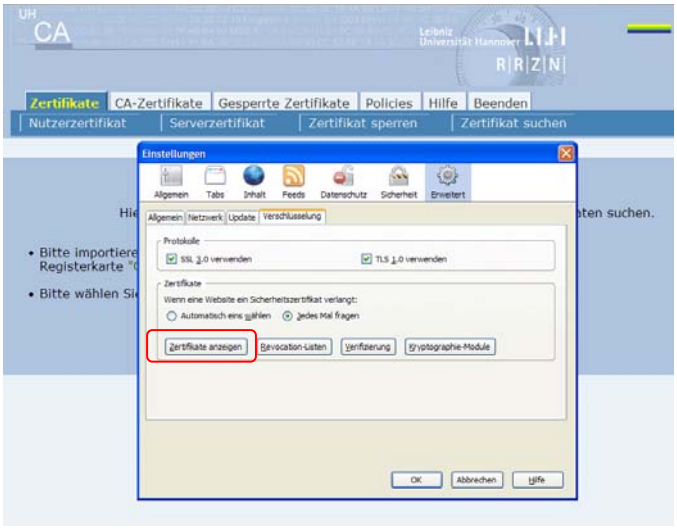
Nachdem die UH-CA Ihr Zertifikat erstellt hat, erhalten Sie eine E-Mail vom PKI-Team der Leibniz Universität Hannover...



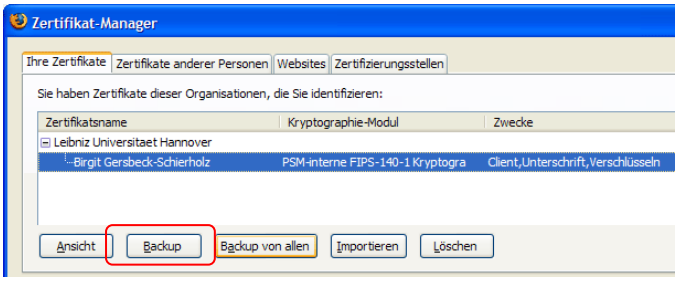
... mit der Information, dass Sie Ihr Zertifikat nun abholen können. Es reicht ein Mausklick auf den markierten Link, um Ihr persönliches Zertifikat in Ihren Browser Firefox zu integrieren.
Ihr Zertifikat ist außerdem noch als PEM-Datei als Anlage der E-Mail beigefügt (in diesem Format müssen die Sie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



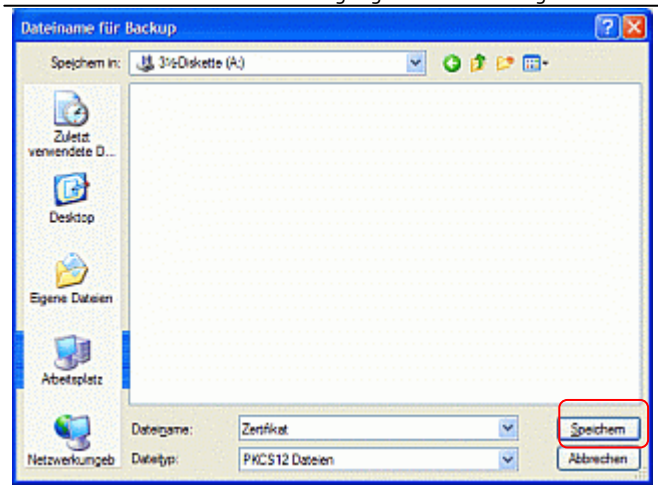
Nachdem Sie das Zertifikat in Firefox importieren **haben**, sollten Sie ein Backup für Thunderbird machen, denn hier wollen Sie es ja hauptsächlich für das Signieren und Verschlüsseln von E-Mail benutzen. Gehen Sie bitte im Programm Firefox, Menü **Extras,** auf **Einstellungen.**



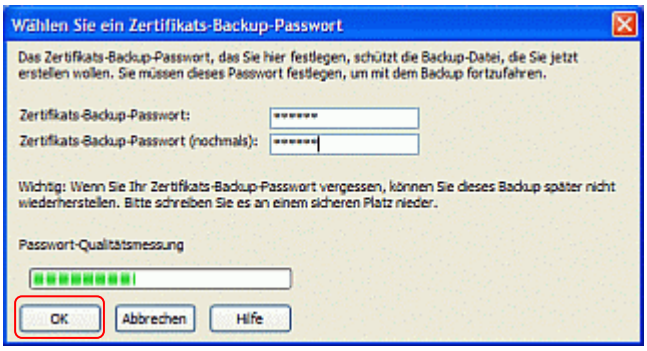
Drücken Sie den Button **Zertifikate anzeigen**.



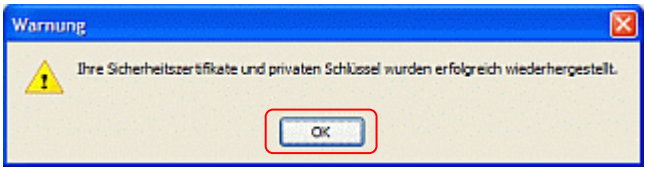
Unter dem Reiter **Ihre Zertifikate** sollte Ihr eigenes Zertifikat angezeigt werden.
Sichern Sie Ihr Zertifikat auf Diskette, indem Sie es markieren und **Backup** anwählen.



Geben Sie einen Dateinamen an und speichen Sie die PKCS12 Datei auf Diskette oder einen anderen externen Datenspeicher.



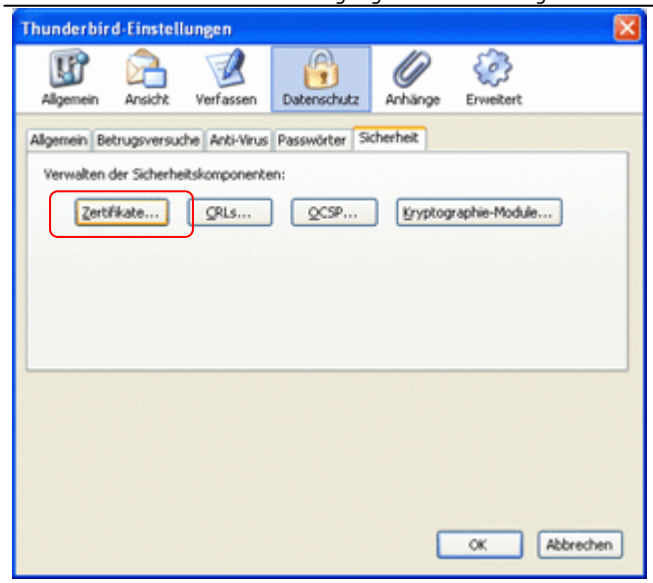
Geben Sie ein **Passwort** für die Backup Datei und und bestätigen Sie dieses nocheinmal. Mit **OK** schließen sie den Dialog.



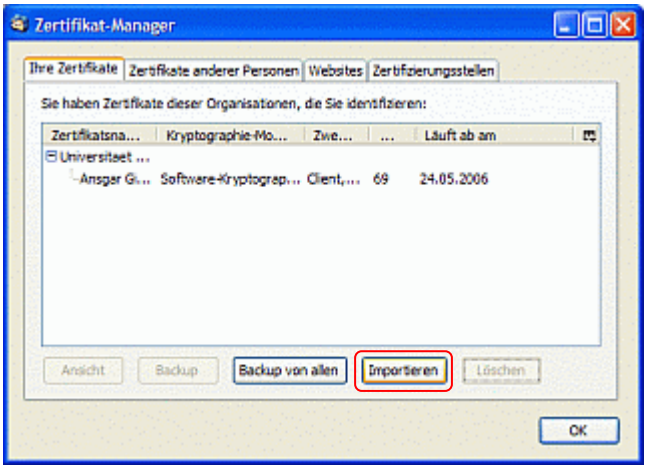
Bestätigen Sie mit **OK**.

4.2 Importieren in Thunderbird

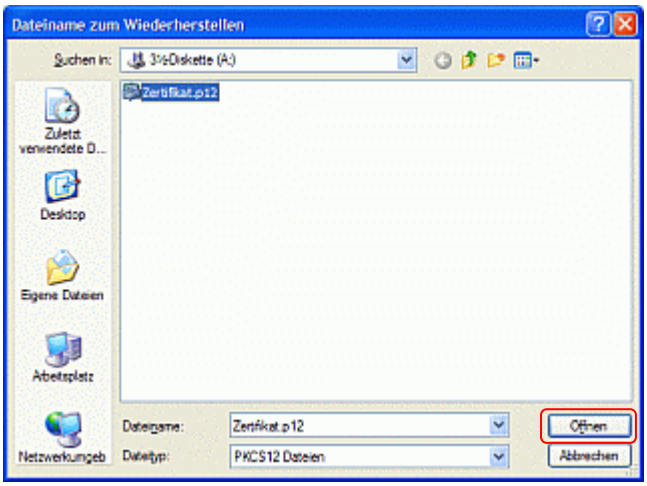
Um Ihr persönliches Zertifikat in den Zertifikatspeicher von Thunderbird zu importieren, öffnen Sie das Programm und wählen unter **Extras** den Punkt **Einstellungen**.



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



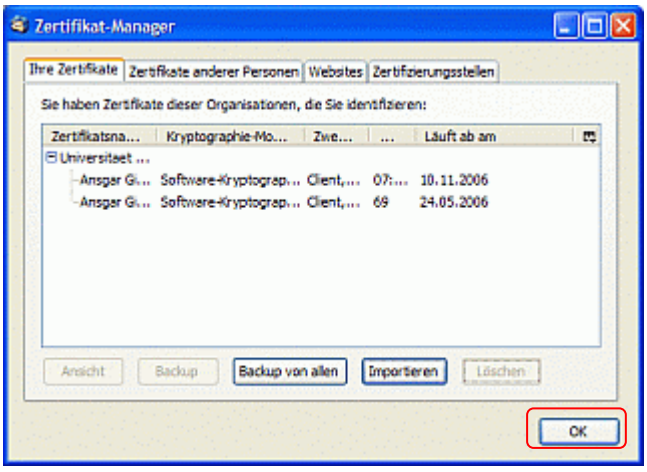
Unter dem Reiter Ihre Zertifikate drücken Sie den Button **Importieren**.



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

Geben Sie das von Ihnen vergebene **Passwort** an und wählen Sie **OK**.

Bestätigen Sie mit **OK**.



Ihr eigenes Zertifikat wurde in den Zertifikatspeicher von Thunderbird importiert.

5 Sicherungskopie des privaten Schlüssels

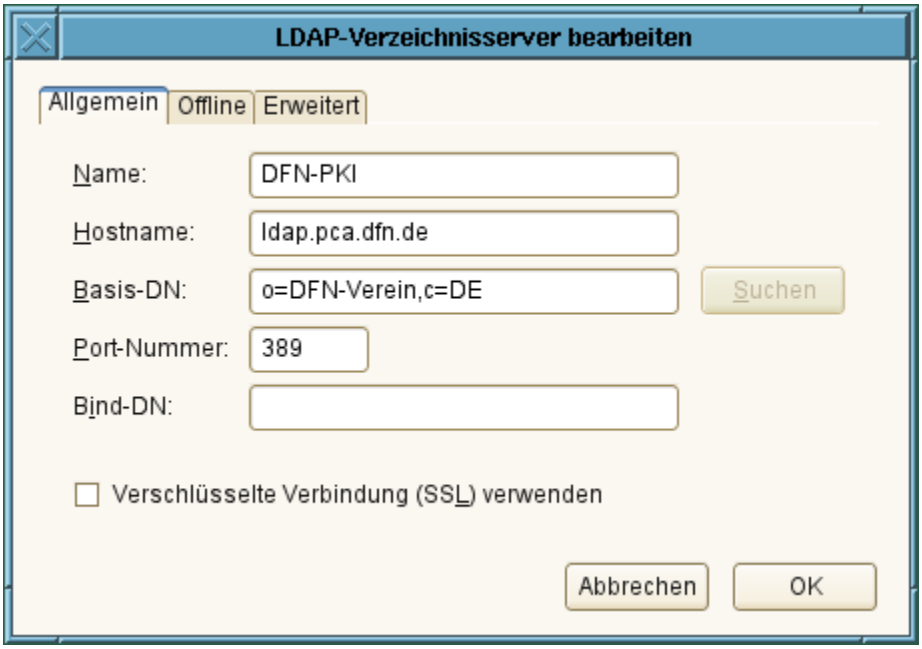
Verwahren Sie die Diskette bzw. Ihren externen Datenträger mit den Zertifikaten an einem sicheren Ort!

Die Datei, welches 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 SecurityEnvironment). Hierbei handelt es sich um einen Passwort geschützten, sicheren Bereich. So steht Ihnen komfortabel und sicher die Signier- und Verschlüsselungsfunktionalität von Mozilla Thunderbird jeder Zeit zur Verfügung.

6 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.

Im Thunderbird wird der LDAP-Verzeichnisdienst am einfachsten über das Adressbuch eingerichtet. Öffnen Sie das **Adressbuch** über das Adressbuch-Symbol. Gehen Sie im Menü unter **Datei** zu **Neu** und wählen dort **LDAP-Verzeichnis** aus. Es öffnet sich ein Fenster mit den Einstellungen für den LDAP-Verzeichnisdienst:



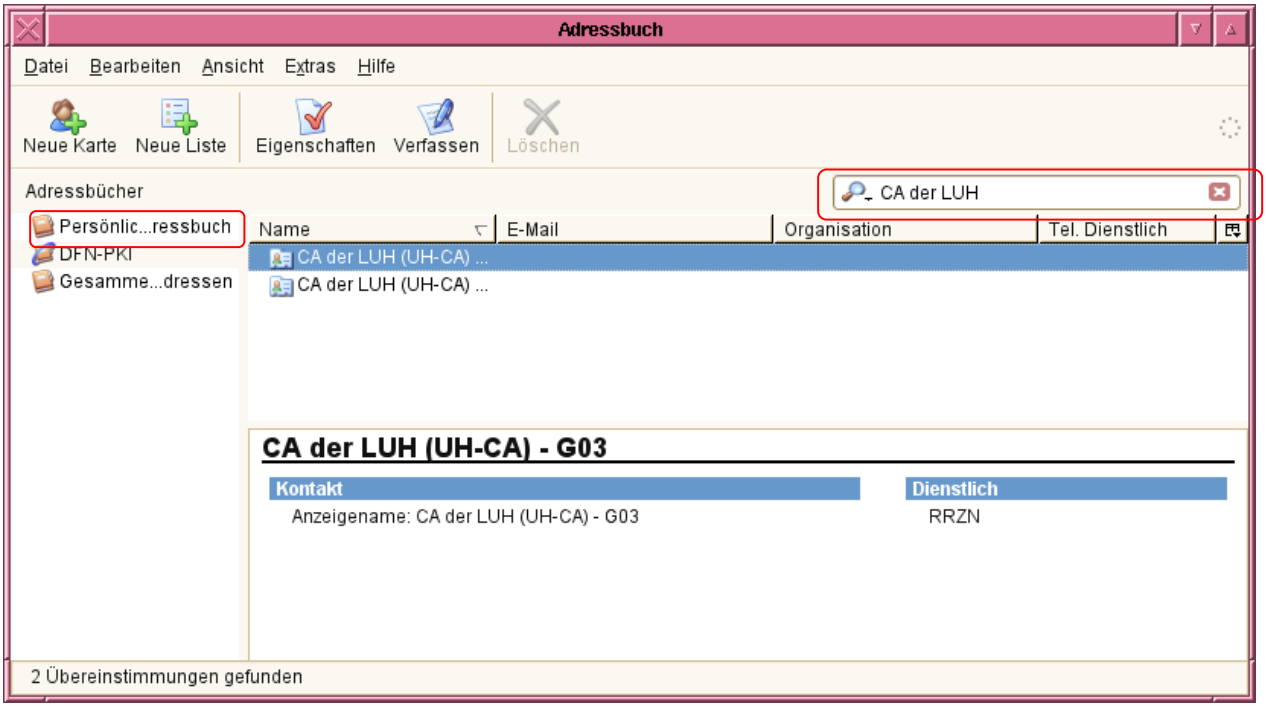
Geben Sie die folgenden Angaben ein:

Name:	DFN-PKI
Hostname:	ldap.pca.dfn.de
Basis-DN:	o=DFN-Verein,c=DE
Port-Nummer:	389

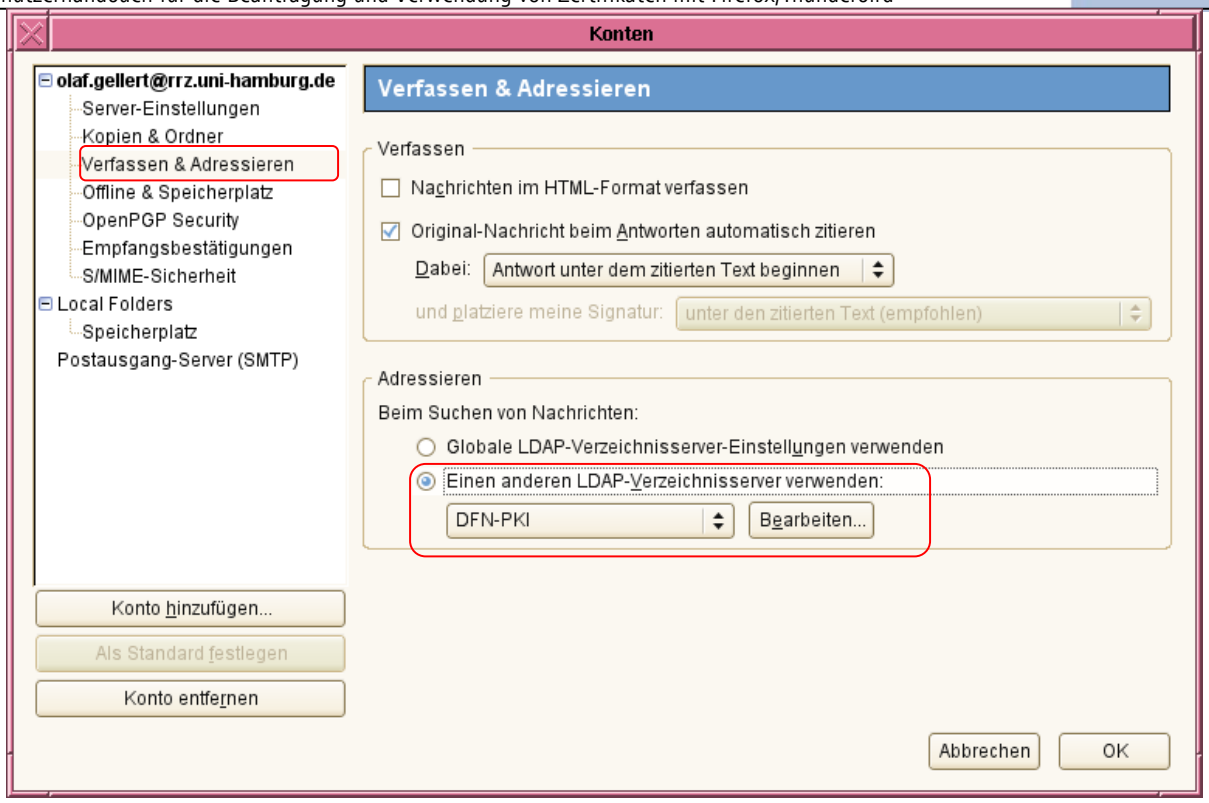
Danach klicken Sie auf **OK**. Zum Testen des LDAP-Servers können Sie im Adressbuch-Fenster aus der Liste der Adressbücher den Eintrag DFN-PKI anwählen und oben rechts in der Suchmaske z.B. einen Namen oder eine Email-Adresse eingeben. Thunderbird such nach dem Eintrag im LDAP-Server und liefert die gefundenen

Ergebnisse zurück. Geben Sie hier z.B. "CA der LUH" an, so werden Ihnen (neben einigen anderen) die Einträge der UH-CA angezeigt.

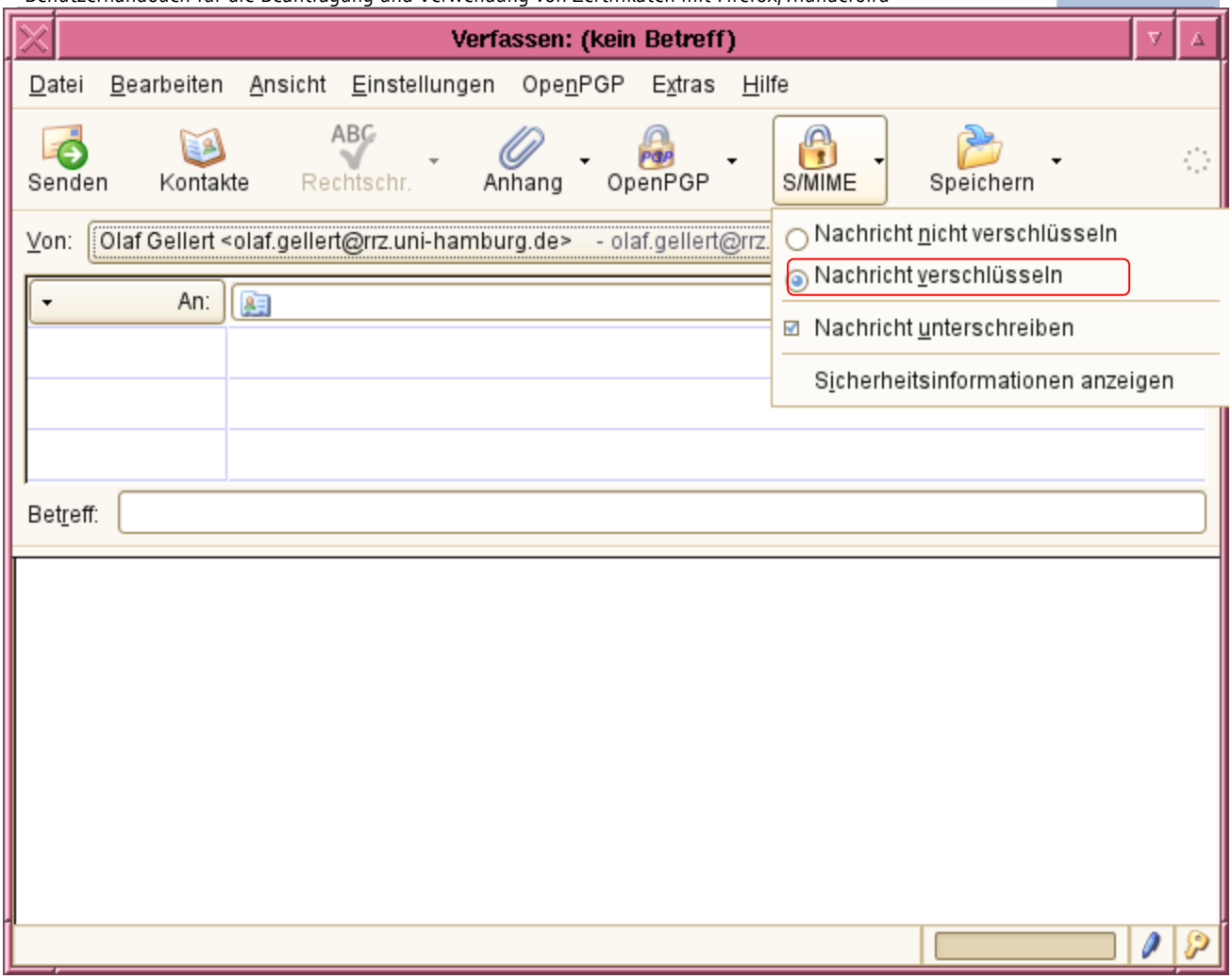
Ein Klick auf einen Eintrag in dieser Liste zeigt den vollständigen Kontakt an:



Zurück im Hauptfenster von Thunderbird muss noch im Menü **Bearbeiten** der Eintrag **Konten** ausgewählt werden. In dem Fenster wählen Sie links Ihren Mail-Account aus und wählen die Option "**Verfassen & Adressieren**". Rechts unten klicken Sie nun auf "Einen anderen LDAP-Verzeichnisserver verwenden" und wählen in der Liste den Eintrag "**DFN-PKI**". Über den OK-Button verlassen Sie die Einstellungen wieder.



Nun können beim Versenden von Mails die Empfänger auf dem LDAP-Server gesucht werden. Beim Eintippen einer Empfängeradresse werden bereits Ergänzungsvorschläge gemacht. Wird im **S/MIME** Menü die Option "**Nachricht verschlüsseln**" angewählt, so wird beim Versenden der Mail das notwendige Zertifikat des Empfängers vom LDAP-Server geholt und die Nachricht an diesen verschlüsselt.



Das automatische Holen von Zertifikaten funktioniert jedoch zunächst nur für die Empfänger mit Zertifikaten der eigenen CA. Soll an Empfänger anderer Einrichtungen im DFN verschlüsselt werden, so muss erst das zugehörige CA-Zertifikat importiert werden. Die CA-Zertifikate im DFN können sie von den Informationsseiten der CAs unter https://info.pca.dfn.de/ jeweils importieren. 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. Thunderbird importiert beim Aufruf der Email automatisch die enthaltenen Schlüssel, so dass Sie nun auch verschlüsselte Mails an diesen Empfänger senden können.