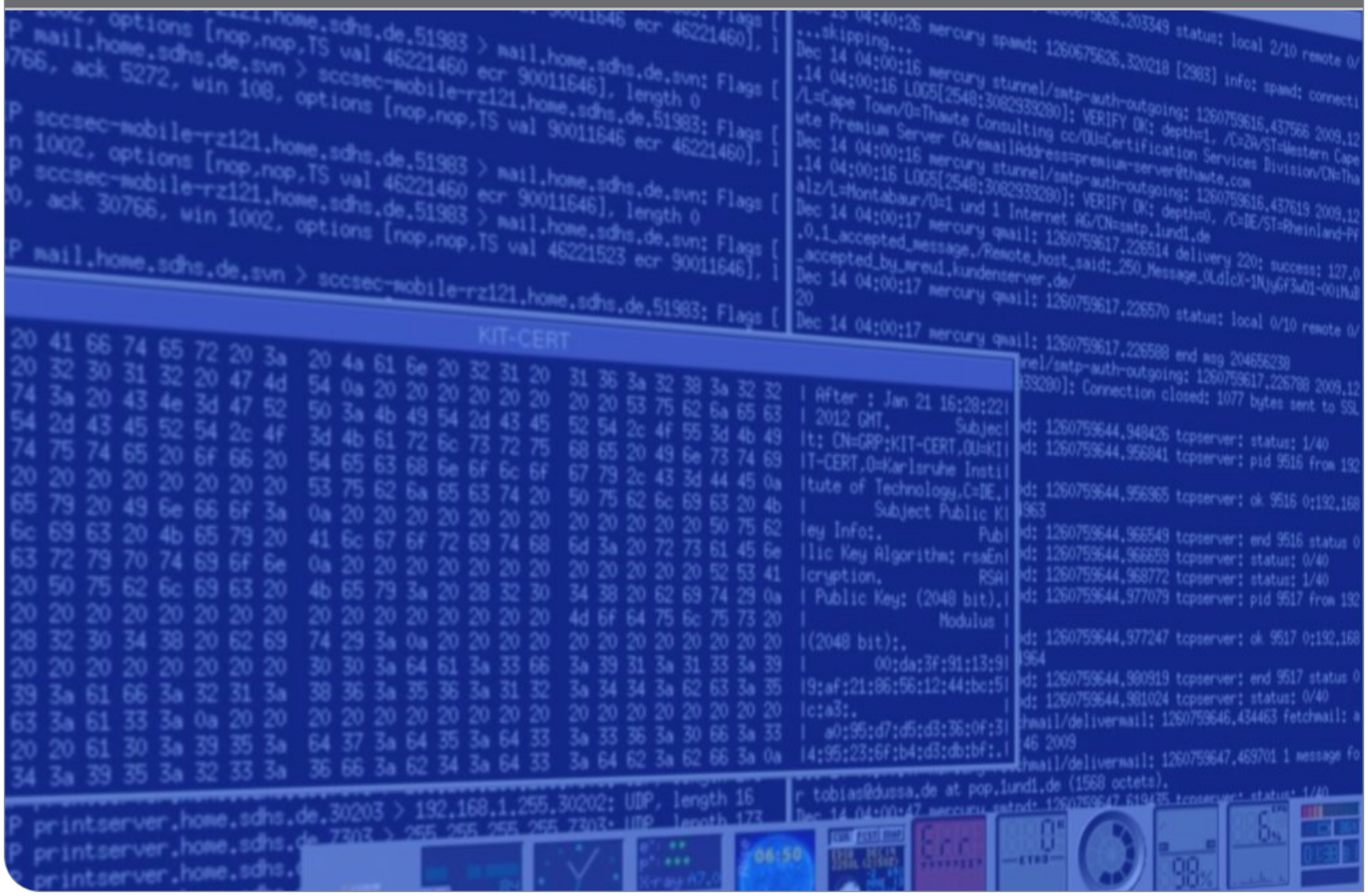
KIT Certification Authority

Anleitung zur Nutzung von S/MIME

Tobias Dussa · Heiko Reese

STEINBUCH CENTRE FOR COMPUTING



KIT – Universität des Landes Baden-Württemberg und
nationales Großforschungszentrum in der Helmholtz-Gemeinschaft

www.kit.edu

Kontakt

Karlsruhe Institute of Technology (KIT)
Certification Authority (CA)

Tobias Dussa
Leiter

Campus Süd
Zirkel 2
76131 Karlsruhe

Telefon: 0721 608-42479
Fax: 0721 608-9-42479
E-Mail: tobias.dussa@kit.edu

www.scc.kit.edu/dienste/kit-ca.php

Herausgeber

Karlsruhe Institute of Technology (KIT)
Certification Authority (CA)
Zirkel 2 | 76131 Karlsruhe

Telefon: 0721 608-45678
Fax: 0721 608-9-45678
E-Mail: ca@kit.edu

Stand 2012-09-24 (Revision 2323)

www.kit.edu

Inhaltsverzeichnis

Revisionshistorie

Version	Inkrafttreten	Autor(en)	Änderung
1	2010-07-20	Dussa, Tobias; Reese, Heiko	Initiale Revision.
2	2011-11-16	Dussa, Tobias	Empfohlener Chiffrealgorithmus wegen Windows-Kompatibilitätsproblemen von AES auf 3DES geändert.

1 Einleitung

Diese Anleitung soll Anwender dabei unterstützen, mit Hilfe von X.509-Zertifikaten kryptographisch gesicherte E-Mails zu veschicken und zu empfangen. Dabei werden die grundlegenden Verfahren sowie die nötigen Arbeitsschritte für die folgenden Mailprogramme beschrieben:

- Microsoft Outlook 2003
- Microsoft Outlook 2007
- Mozilla Thunderbird 3.0
- Mozilla Thunderbird 3.1

Die konkreten Anleitungen für Thunderbird basieren hierbei auf den Windows-Versionen von Thunderbird. Bei Nutzung von Thunderbird unter anderen Betriebssystemen bleiben zwar die wesentlichen gleich, können sich aber im Detail unterscheiden.

Es wird vorausgesetzt, dass bereits ein X.509-Nutzerzertifikat der KIT-CA oder der Uni-Karlsruhe-CA für die verwendete E-Mail-Adresse zur Verfügung steht. Entsprechende Zertifikate können unter dem URL `https://pki.pca.dfn.de/kit-ca/pub` beantragt werden; bitte beachten Sie auch die Benutzungsanleitung zur KIT-CA, die unter dem URL `https://www.scc.kit.edu/downloads/ism/benutzungsanleitung.pdf` verfügbar sind.

Im folgenden werden diese grundsätzlichen Arbeitsschritte beschrieben:

- Importieren des eigenen Nutzerzertifikats im Mailprogramm;
- Importieren von Nutzerzertifikaten anderer Anwender im Mailprogramm;
- Versenden gesicherter E-Mails und
- Empfangen gesicherter E-Mails.

2 Grundlagen von S/MIME

Der S/MIME-Standard erlaubt es, E-Mails auf zwei verschiedene Arten kryptographisch zu sichern. E-Mails können

- verschlüsselt und
- signiert

werden. Eine verschlüsselte E-Mails kann nur vom Empfänger gelesen werden und ist damit gegen unbefugte Kenntnisnahme gesicherte; das Signieren einer E-Mails schützt demgegenüber gegen das unbefugte Verändern des Inhalts und belegt zudem die Herkunft der Nachricht.

Um eine E-Mail verschlüsseln zu können, muss der Absender das X.509-Zertifikat des Empfängers kennen. Eine mit dem X.509-Zertifikat verschlüsselte E-Mail kann nur mit Hilfe des zugehörigen privaten Schlüssels dechiffriert werden; dieser ist nur dem Empfänger bekannt. Zum Signieren einer E-Mail wird hingegen der private Schlüssel verwendet. Hierbeit wird zunächst mittels einer Hashfunktion eine Prüfsumme über den Nachrichteninhalt erstellt, die dann mit dem privaten Schlüssel des Absenders chiffriert wird. Diese verschlüsselte Prüfsumme bildet die Signatur der E-Mail und wird an diese angehängt. Die Signatur wiederum kann nur mit Hilfe des X.509-Zertifikats des Absenders entschlüsselt werden; aus diesem Grund wird das X.509-Zertifikat (genauer gesagt, die gesamte Zertifikatkette) üblicherweise ebenfalls an die signierte E-Mail angehängt. Der Empfänger kann die Signatur mit Hilfe des X.509-Zertifikats des Absenders entschlüsseln und die darin enthaltene Prüfsumme mit der Prüfsumme vergleichen, die er selber über die Nachricht gebildet hat. Stimmen die Prüfsummen überein, so kann davon ausgegangen werden, dass die Nachricht vom Absender verfasst und unverändert übertragen wurde. Um sowohl gegen unbefugtes Mitlesen als auch gegen Verändern zu schützen, kann eine E-Mail zunächst signiert und dann mitsamt der Signatur verschlüsselt werden.

Um eine E-Mail an einen oder mehrere Empfänger verschlüsseln zu können, ist es also notwendig, die X.509-Zertifikate aller Empfänger zu kennen; um eine E-Mail signieren zu können, benötigt der Absender ein eigenes X.509-Zertifikat.

3 Herunterladen und Importieren der Zertifikatkette

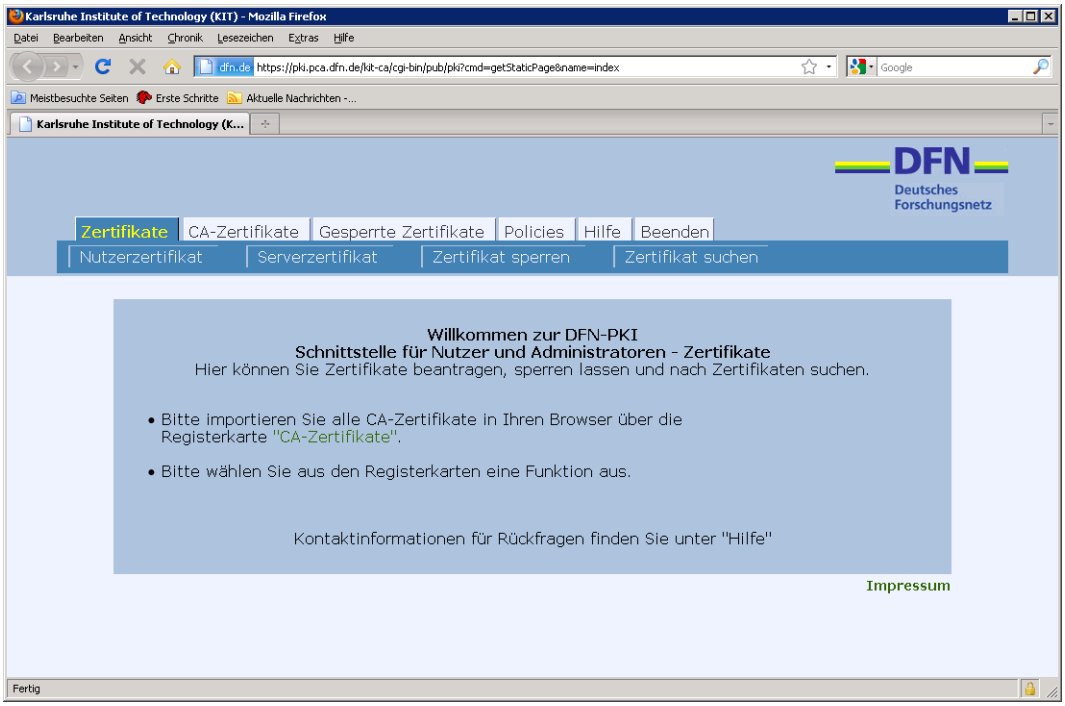
Sowohl für das Verschlüsseln als auch für das Signieren von E-Mails ist es notwendig, die vollständige Zertifikatkette vorliegen zu haben, um die Gültigkeit eines Nutzerzertifikats prüfen zu können. Zum Prüfen eines Zertifikats ist das Zertifikat der ausstellenden Zertifizierungsstelle notwendig. Die offiziellen Zertifikate von KIT-Mitarbeitern sind in der Regel von der KIT-CA ausgestellt; ältere Zertifikate sind dagegen von der UNIKA-CA ausgestellt worden. Zum Prüfen ist also entweder das Zertifikat der KIT-CA oder das der UNIKA-CA notwendig, je nachdem, welche Zertifizierungsstelle das konkret vorliegende Zertifikat ausgestellt hat. Die Zertifikate beider Zertifizierungsstellen wurden von der DFN-CA ausgestellt, deren Zertifikat wiederum von der Deutschen Telekom ausgestellt wurde. Das Zertifikat der Deutschen Telekom wurde nicht von einer weiteren Zertifizierungsstelle ausgestellt und bildet damit das letzte Glied dieser Zertifikatkette. Es kann daher nicht automatisch geprüft werden; dies ist auch nicht notwendig, da es bei aktuellen Versionen von Windows, Firefox, Opera, Thunderbird und Java bereits mitgeliefert wird. Um ein Nutzerzertifikat vollständig zu prüfen, müssen alle genannten Zwischenzertifikate vorliegen. Es ist daher notwendig, die folgenden Zertifikate dem Mailprogramm bekanntzumachen:

- KIT-CA,
- UNIKA-CA,
- DFN-CA und
- CA der Deutschen Telekom.

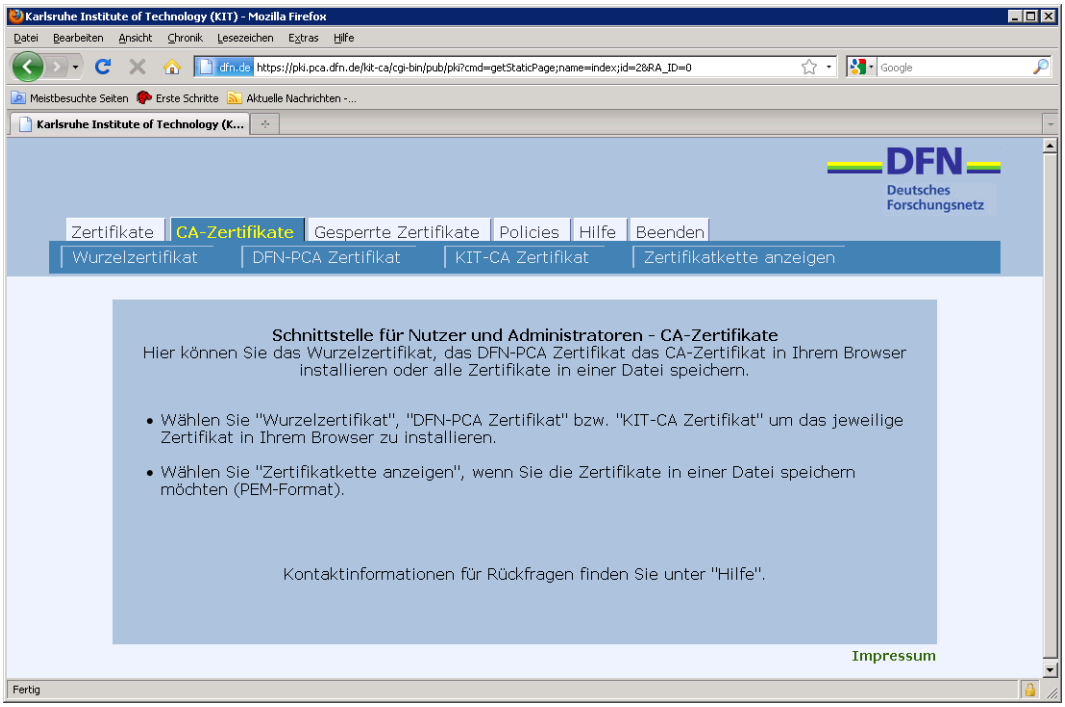
3.1 Herunterladen der Zertifikate der DFN-CA, der KIT-CA und der UNIKA-CA

Um die benötigten CA-Zertifikate herunterzuladen, gehen Sie wie folgt vor. Für das DFN-CA-Zertifikat sind unten jeweils Bildschirmfotos vorhanden, die beispielhaft mit dem Mozilla Firefox erstellt wurden. Für die anderen CA-Zertifikate wurden keine Bildschirmfotos erstellt, da das Vorgehen dasselbe ist.

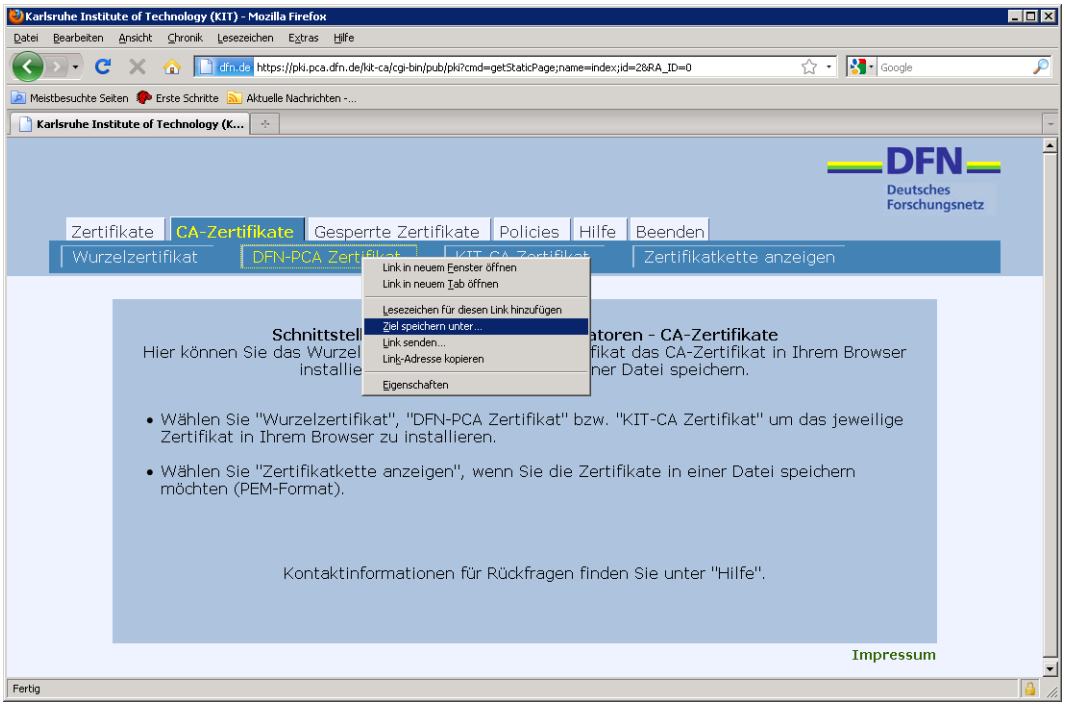
1. Öffnen Sie mit einem Webbrowser die Webseite der KIT-CA (`https://pki.pca.dfn.de/kit-ca/pub`.


Karlsruhe Institute of Technology (KIT) - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki?cmd=getStaticPage&name=index
Meistbesuchte Seiten Erste Schritte Aktuelle Nachrichten -...
Karlsruhe Institute of Technology (K...
DFN
Deutsches Forschungsnetz
Zertifikate CA-Zertifikate Gesperrte Zertifikate Policies Hilfe Beenden
Nutzerzertifikat Serverzertifikat Zertifikat sperren Zertifikat suchen
Willkommen zur DFN-PKI
Schnittstelle für Nutzer und Administratoren - Zertifikate
Hier können Sie Zertifikate beantragen, sperren lassen und nach Zertifikaten suchen.
• Bitte importieren Sie alle CA-Zertifikate in Ihren Browser über die Registerkarte "CA-Zertifikate".
• Bitte wählen Sie aus den Registerkarten eine Funktion aus.
Kontaktinformationen für Rückfragen finden Sie unter "Hilfe"
Impressum
Fertig

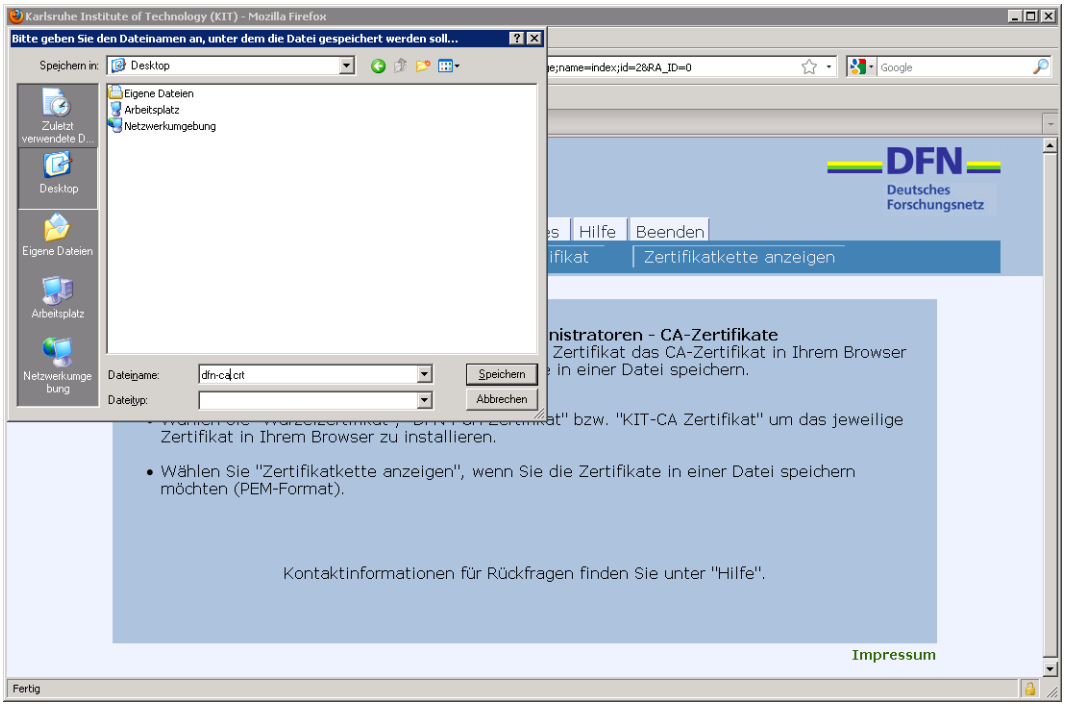
2. Klicken Sie auf den Reiter »CA-Zertifikate«.



3. Klicken Sie mit der rechten Maustaste auf die Schaltfläche »DFN-PCA-Zertifikat« und speichern Sie das Linkziel auf Ihrem Desktop oder in einem anderen Ordner.



Der vorgeschlagene Dateiname lautet `intermediatecacert.crt`; ändern Sie diesen der Übersichtlichkeit halber in `dfn-ca.crt`.



4. Klicken Sie mit der rechten Maustaste auf die Schaltfläche »KIT-CA-Zertifikat« und speichern Sie das Linkziel. Der vorgeschlagene Dateiname lautet `cacert.crt`; ändern Sie diesen in `kit-ca.crt`.

5. Öffnen Sie mit einem Webbrowser die Webseite der UNIKA-CA (`https://pki.pca.dfn.de/uni-karlsruhe-ca/pub`).

6. Klicken Sie auf den Reiter »CA-Zertifikate«.

7. Klicken Sie mit der rechten Maustaste auf die Schaltfläche »UNIKA-CA-Zertifikat« und speichern Sie das Linkziel. Der vorgeschlagene Dateiname lautet `cacert.crt`; ändern Sie diesen in `unika-ca.crt`.

8. Klicken Sie mit der rechten Maustaste auf die Schaltfläche »Wurzelzertifikat« und speichern Sie das Linkziel. Der vorgeschlagene Dateiname lautet `rootcert.crt`; ändern Sie diesen in `dtag-ca.crt`.

3.2 Importieren der CA-Zertifikate

In den folgenden Abschnitten wird beschrieben, wie Sie die heruntergeladenen CA-Zertifikate in Ihrem System installieren können.

3.2.1 Microsoft Outlook 2003 und 2007

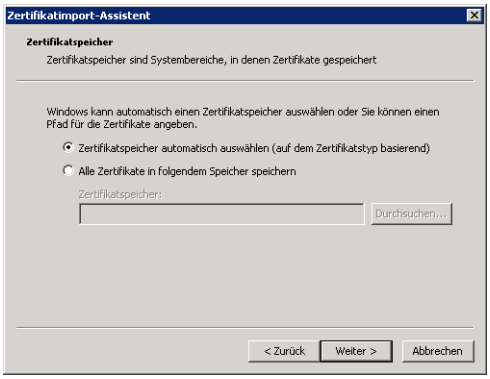
Microsoft Outlook 2003 greift auf den Zertifikatspeicher von Windows zurück. Um die CA-Zertifikate für Outlook verfügbar zu machen, müssen sie daher in den Zertifikatspeicher importiert werden. Hierfür gehen Sie wie folgt vor; die in den Abbildungen gezeigten Bildschirmfotos zeigen beispielhaft den Vorgang für das Zertifikat der DFN-CA.

1. Klicken Sie mit der rechten Maustaste auf das Symbol der Datei mit dem zu installierenden Zertifikat und wählen Sie »Zertifikat installieren« aus.

2. Aktuelle Windows-Versionen zeigen daraufhin einen Warndialog an und erwarten eine Bestätigung, dass die Zertifikatdatei tatsächlich geöffnet werden soll, obwohl sie einen »unbekannten Herausgeber« hat. Bestätigen Sie durch einen Klick auf die Schaltfläche »Öffnen«.

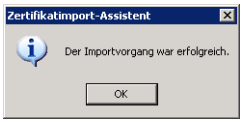
3. Daraufhin wird der Zertifikatimport-Assistent gestartet; klicken Sie auf die Schaltfläche »Weiter«.

4. Im nächsten Schritt können Sie den Zertifikatspeicher auswählen, in den das Zertifikat importiert werden soll. Übernehmen Sie die Standardeinstellung »Zertifikatspeicher automatisch wählen« und klicken Sie auf »Weiter«.



5. Im letzten Schritt wird noch eine Übersicht der gewählten Einstellungen zum Zertifikatimport angezeigt. Klicken Sie auf »Fertig stellen«.

6. Der erfolgreiche Import wird durch eine entsprechende Meldung bestätigt.

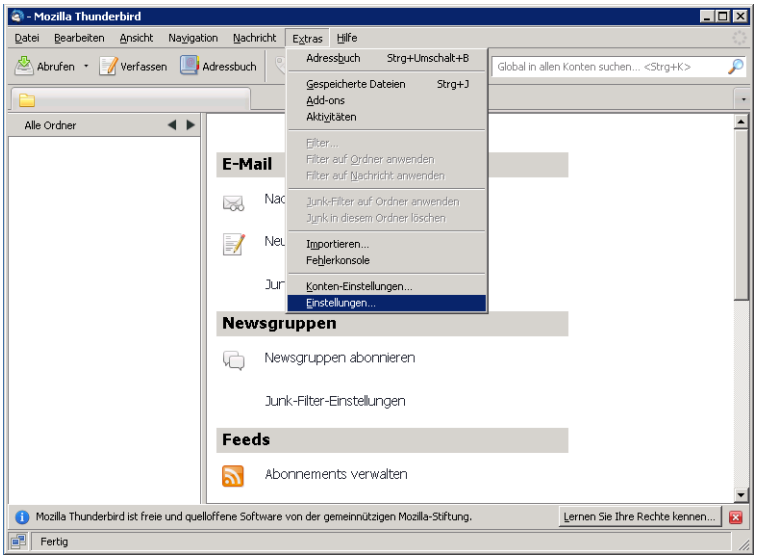


Wiederholen Sie die Schritte 1 bis 6 auch sinngemäß für die Zertifikate der KIT-CA, der UNIKA-CA und der Root-CA der Deutschen Telekom.

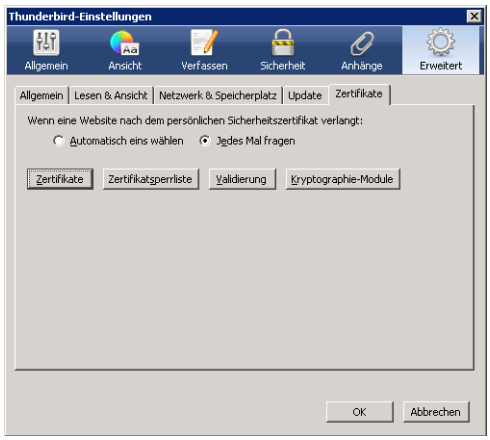
3.2.2 Mozilla Thunderbird 3.0 und 3.1

Im Gegensatz zu Outlook greift Thunderbird nicht auf den Windows-Zertifikatspeicher zu, sondern bringt vielmehr seinen eigenen Zertifikatspeicher mit, um mit den Thunderbird-Implementierungen unter anderen Betriebssystemen kompatibel zu sein. Die Zertifikate müssen daher direkt in Thunderbird importiert werden. Die Bildschirmfotos sind exemplarisch mit Thunderbird 3.1 für den Import des DFN-CA-Zertifikats erstellt worden; der grundsätzliche Vorgang ist bei Thunderbird 3.0 aber identisch.

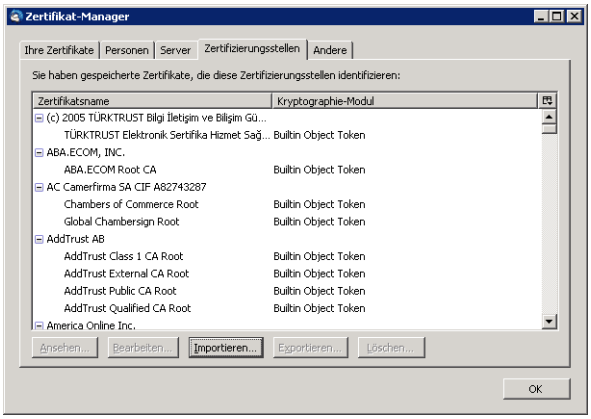
1. Klicken Sie im Thunderbird-Menü »Extras« auf den Punkt »Einstellungen«.



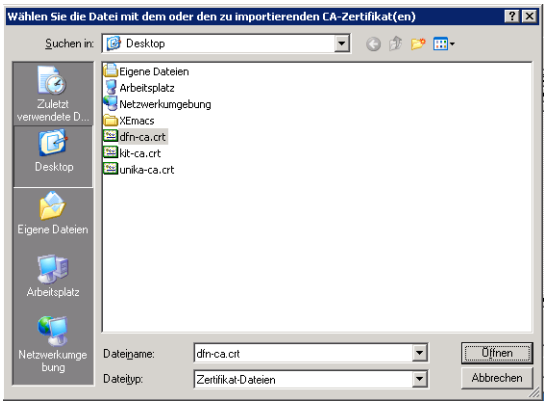
2. Klicken Sie im Dialog »Thunderbird-Einstellungen« auf die Schaltfläche »Erweitert«, dann auf den Reiter »Zertifikate« und schließlich nochmal auf die Schaltfläche »Zertifikate«.



3. Wählen Sie den Reiter »Zertifizierungsstellen« und klicken Sie auf die Schaltfläche »Importieren«.



4. Wählen Sie die Datei aus, in der das zu installierende Zertifikat gespeichert ist.



5. Setzen Sie in allen drei Kästchen die entsprechenden Haken, um dem zu importierenden Zertifikat in allen Bereichen zu vertrauen.

Es erfolgt keine Meldung, wenn der Import erfolgreich war. Wiederholen Sie die Schritte 1 bis 5 sinngemäß für die Zertifikate der KIT-CA, der UNIKA-CA und der CA der Deutschen Telekom.

4 Importieren des eigenen Nutzerzertifikats und Schlüssels

Um E-Mails signieren zu können, ist es notwendig, dem Mailprogramm den eigenen geheimen Schlüssel sowie das zugehörige X.509-Zertifikat zugänglich zu machen.

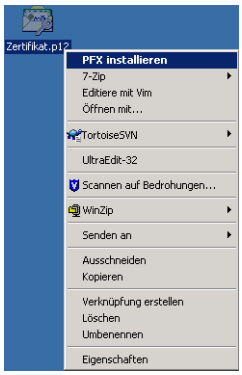
4.1 Microsoft Outlook 2003 und 2007

Microsoft Outlook 2003 und 2007 greifen zum Aufbewahren von Zertifikaten auf den zentralen Windows-Zertifikatspeicher zurück. Um das eigene X.509-Zertifikat und den dazugehörigen privaten Schlüssel für Outlook verfügbar zu machen, ist es daher nötig, ihn im Zertifikatspeicher des verwendeten Benutzerkontos auf dem verwendeten Rechner abzulegen. Wenn das verwendete Zertifikat auf demselben Rechner unter demselben Benutzerkonto mit Hilfe des Internet Explorer beantragt und heruntergeladen wurde, so sind das Zertifikat und der private Schlüssel bereits im Zertifikatspeicher vorhanden. Andernfalls ist es nötig, sie manuell zu importieren. Hierfür sind die folgenden Schritte notwendig:

1. Kopieren Sie das zu importierende Zertifikat samt zugehörigem geheimen Schlüssel auf den verwendeten Rechner. Es ist nicht ausreichend, nur Ihr Zertifikat zu kopieren; auch der geheime Schlüssel wird benötigt! Dateien, die auf `.pem`, `.crt`, `.cer` und `.der` enden, enthalten in aller Regel *nicht* den geheimen Schlüssel, sondern lediglich das öffentliche Zertifikat. Dateien, die sowohl das Zertifikat als auch den dazugehörigen geheimen Schlüssel enthalten, haben üblicherweise Dateinamen, die auf `.pfx` oder `.p12` enden. Sollten Sie nicht über eine entsprechende Datei verfügen, so können Sie sie erzeugen, indem Sie Ihr Zertifikat und den passenden geheimen Schlüssel von

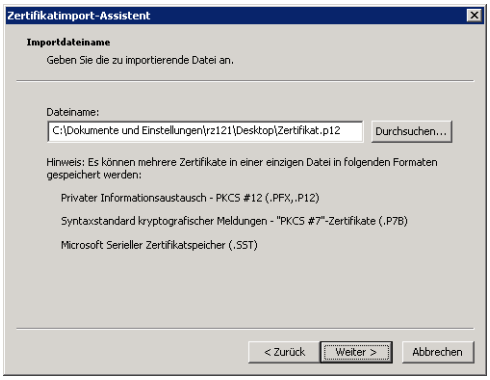
einem Rechner exportieren, auf dem beides bereits installiert ist. Details hierzu können Sie der Nutzungsanleitung der KIT-CA entnehmen, die unter dem URL `http://www.scc.kit.edu/downloads/ism/benutzungsanleitung.pdf` erhältlich ist.

2. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie den Punkt »PFX installieren« aus.



3. Der Zertifikatimport-Assistent wird gestartet.

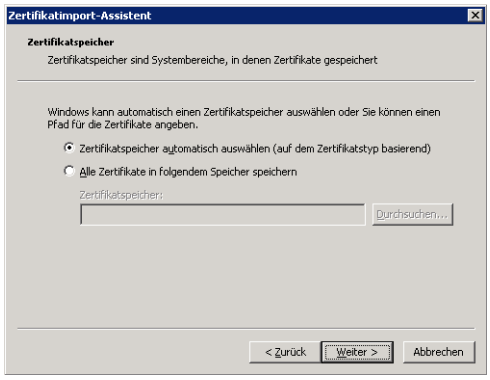
4. Die zu importierende Zertifikatdatei wird nochmals angezeigt.



5. Geben Sie das Kennwort ein, mit dem der geheime Schlüssel geschützt ist und das Sie beim Exportieren der Zertifikatdatei angegeben haben.

Setzen Sie den Haken für »Hohe Sicherheit«; damit wird eingestellt, dass Sie jeden Zugriff auf den geheimen Schlüssel einzeln bestätigen müssen. Wenn Sie Ihren geheimen Schlüssel später wieder aus dem Windows-Zertifikatspeicher exportieren möchten, setzen Sie auch den Haken »Schlüssel als exportierbar markieren«; dies ist in der Regel unnötig, da Ihr Schlüssel bereits in einer externen Datei vorliegt, die Sie sichern und auf andere Rechner kopieren können.

6. Im nächsten Schritt können Sie den Zertifikatspeicher auswählen, in den das Zertifikat importiert werden soll. Übernehmen Sie die Standardeinstellung »Zertifikatspeicher automatisch wählen« und klicken Sie auf »Weiter«.



7. Im nächsten Schritt wird noch eine Übersicht der gewählten Einstellungen zum Zertifikatimport angezeigt.

8. Wenn Sie für Ihren geheimen Schlüssel »Hohe Sicherheit« festgelegt haben, können Sie im nächsten Schritt die Sicherheitsstufe festlegen.

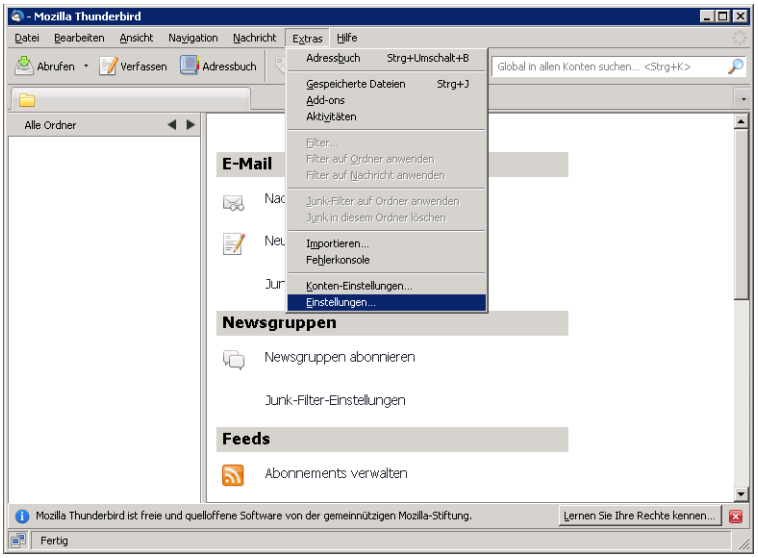
In der Regel genügt »mittlere Sicherheitsstufe«; hierbei müssen Sie jedem Zugriff auf den geheimen Schlüssel lediglich zustimmen. Wenn Sie statt dessen »hohe Sicherheitsstufe« wählen, müssen Sie noch ein Kennwort festlegen, das bei jedem Zugriff auf den geheimen Schlüssel abgefragt wird.

9. Der erfolgreiche Import wird durch eine entsprechende Meldung bestätigt.

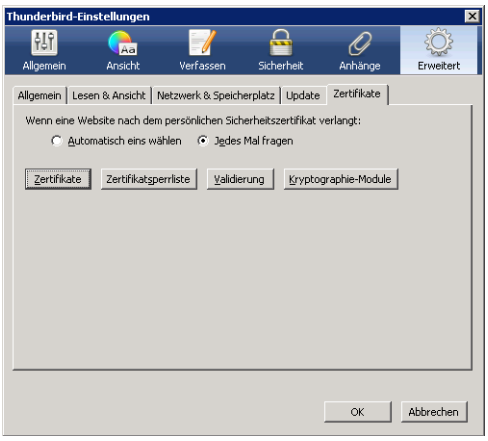
4.2 Mozilla Thunderbird 3.0 und 3.1

Im Gegensatz zu Microsoft Outlook verwendet Thunderbird nicht den Windows-Zertifikatspeicher, sondern bringt seine eigene Zertifikatablage mit, um zu den Thunderbird-Versionen für andere Betriebssysteme kompatibel zu sein. Um das eigene Zertifikat verfügbar zu machen, sind die folgenden Schritte notwendig.

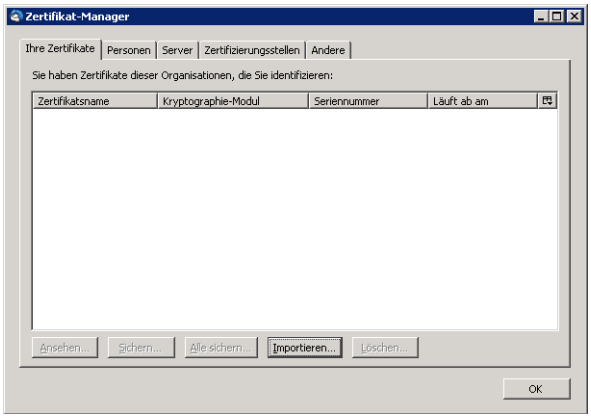
1. Klicken Sie im Thunderbird-Menü »Extras« auf den Punkt »Einstellungen«.



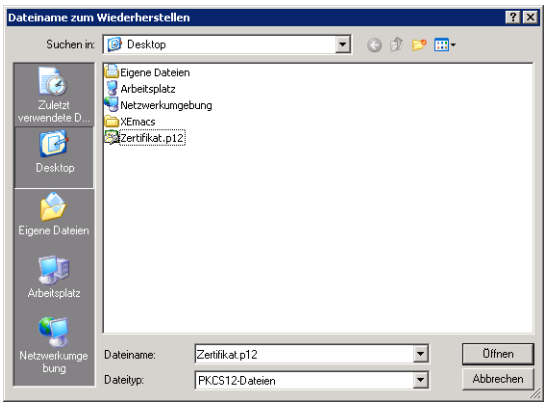
2. Klicken Sie im Dialog »Thunderbird-Einstellungen« auf die Schaltfläche »Erweitert«, dann auf den Reiter »Zertifikate« und schließlich nochmal auf die Schaltfläche »Zertifikate«.



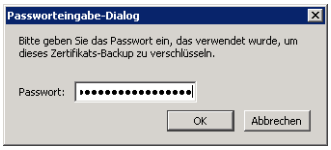
3. Wählen Sie den Reiter »Ihre Zertifikate« und klicken Sie auf die Schaltfläche »Importieren«. Wenn Sie noch kein Master-Passwort für Thunderbird gesetzt haben, wird jetzt ein Dialog geöffnet, mit dem Sie ein solches Master-Passwort setzen können.



4. Wählen Sie die Datei aus, in der das zu installierende Zertifikat gespeichert ist.



5. Geben Sie das Passwort ein, mit dem der zu importierende geheime Schlüssel geschützt ist und das Sie beim Exportieren des Zertifikats definiert haben.



6. Der erfolgreiche Import des Zertifikats sowie des geheimen Schlüssels wird gemeldet.

5 Importieren von Nutzerzertifikaten anderer Anwender

Um anderen Anwendern verschlüsselte E-Mails zu schicken, ist es notwendig, die jeweiligen X.509-Zertifikate der Empfänger zu kennen. Sie müssen also vor dem Verschlüsseln einer Mail dem Mailprogramm bekannt gemacht werden. Grundsätzlich gibt es zwei Wege, ein Nutzerzertifikat zu importieren:

- Mit Hilfe einer signierten E-Mail des jeweiligen Anwenders und
- manuell.

Diese beiden Methoden unterscheiden sich im wesentlichen darin, wie das fehlende Zertifikat beschafft wird. Beim manuellen Import müssen Sie das Zertifikat selbst beschaffen, während eine korrekt signierte E-Mails notwendigerweise das Zertifikat des Absenders enthält.

Das Importieren eines Nutzerzertifikates ist allerdings völlig unnötig, wenn der betreffende Benutzer sein Zertifikat in der Global Address List (GAL) veröffentlicht hat, Sie Outlook nutzen und dieselbe GAL verwenden. In diesem Fall ist Outlook in der Lage, das Zertifikat selbstständig aufzufinden.

5.1 Manueller Import

Für einen manuellen Import eines Nutzerzertifikats ist es zunächst nötig, das zu importierende Zertifikat zu beschaffen. X.509-Zertifikate, die von der UNIKA-CA oder der KIT-CA ausgestellt wurden und bei denen der Besitzer der Veröffentlichung zugestimmt hat, können beispielsweise direkt bei der jeweiligen CA gesucht und nach erfolgreicher Suche heruntergeladen werden:

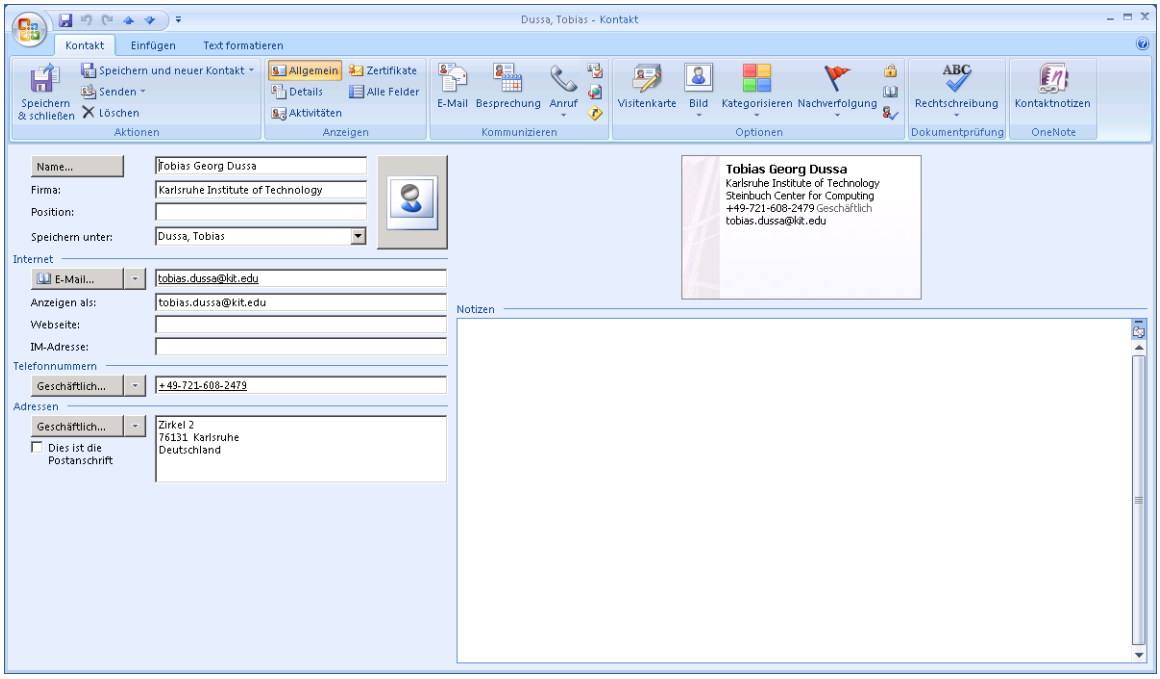
Für die UNIKA-CA: `https://pki.pca.dfn.de/uni-karlsruhe-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=search_cert`

Für die KIT-CA: `https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=search_cert`

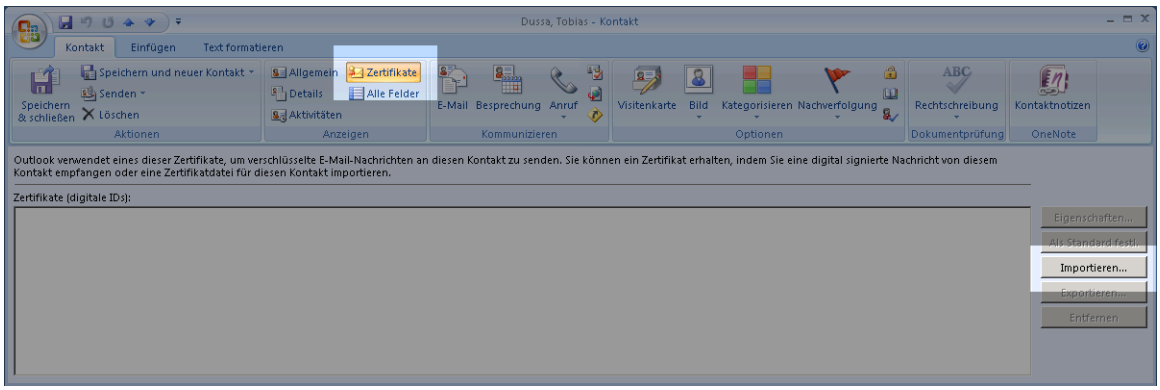
5.1.1 Microsoft Outlook 2003 und 2007

Um in Outlook ein Nutzerzertifikat manuell einem Kontakt hinzuzufügen, gehen Sie wie folgt vor. Die Bildschirmfotos sind exemplarisch mit Outlook 2007 erstellt; der grundsätzliche Vorgang ist bei Outlook 2003 aber derselbe.

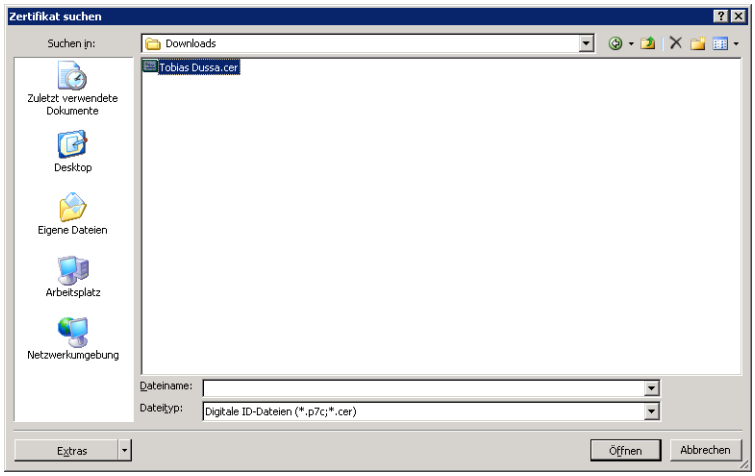
1. Öffnen Sie den Kontakt, dem Sie ein Zertifikat hinzufügen wollen.



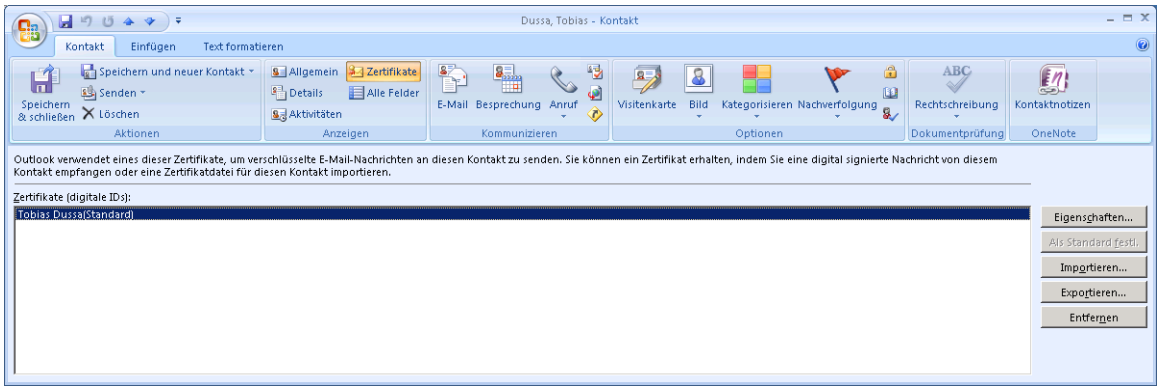
2. Klicken Sie auf das Feld »Zertifikate«, danach auf das Feld »Importieren«. Die relevanten Schaltflächen sind in der folgenden Abbildung hervorgehoben.



3. Wählen Sie die Datei aus, die das zu importierende Zertifikat enthält. Beachten Sie, dass die Datei im DER-Format vorliegen und der Dateiname auf `.cer` enden muss; es kann notwendig sein, die Datei zu konvertieren oder umzubenennen!



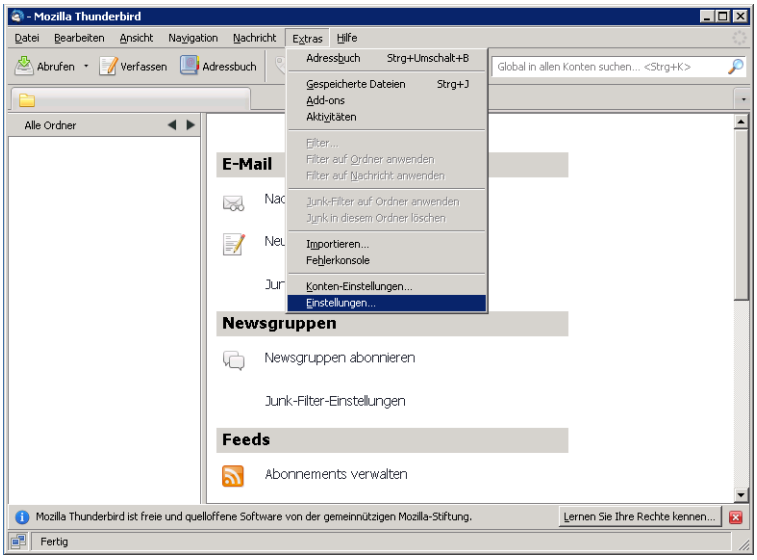
Das erfolgreich importierte Zertifikat wird dann in der Zertifikatliste des Kontaktes angezeigt.



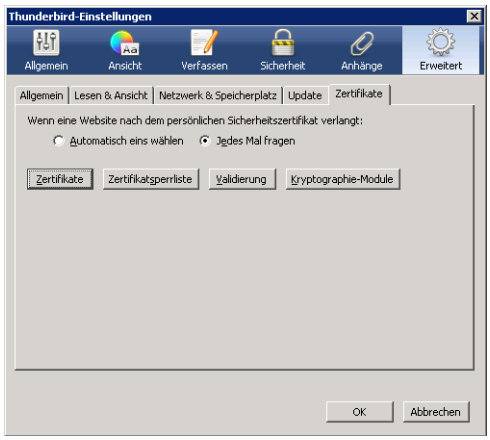
5.1.2 Mozilla Thunderbird 3.0 und 3.1

Thunderbird benötigt im Gegensatz zu Outlook keine vorherigen Verknüpfungen zwischen Kontakten und Zertifikaten. Es genügt vielmehr, das Zertifikat eines anderen Anwenders generell dem Zertifikatspeicher hinzuzufügen, um diesem Anwender verschlüsselte E-Mails schicken zu können. Die folgenden Schritte sind dafür notwendig.

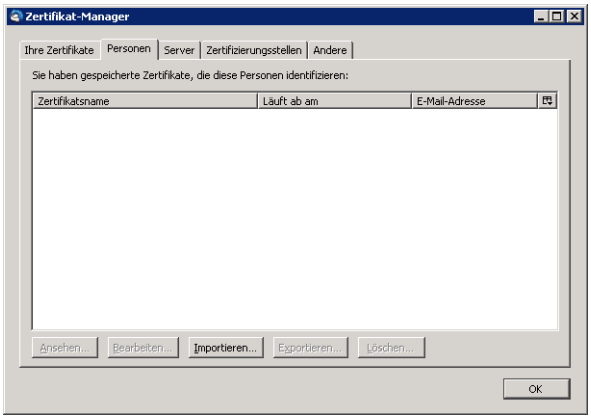
1. Klicken Sie im Thunderbird-Menü »Extras« auf den Punkt »Einstellungen«.



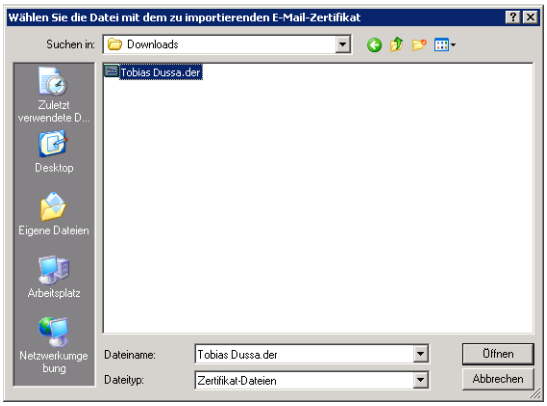
2. Klicken Sie im Dialog »Thunderbird-Einstellungen« auf die Schaltfläche »Erweitert«, dann auf den Reiter »Zertifikate« und schließlich nochmal auf die Schaltfläche »Zertifikate«.



3. Wählen Sie den Reiter »Personen« und klicken Sie auf die Schaltfläche »Importieren«.



4. Wählen Sie die Datei aus, in der das zu installierende Zertifikat gespeichert ist. Der erfolgreiche Import wird nicht gesondert gemeldet.



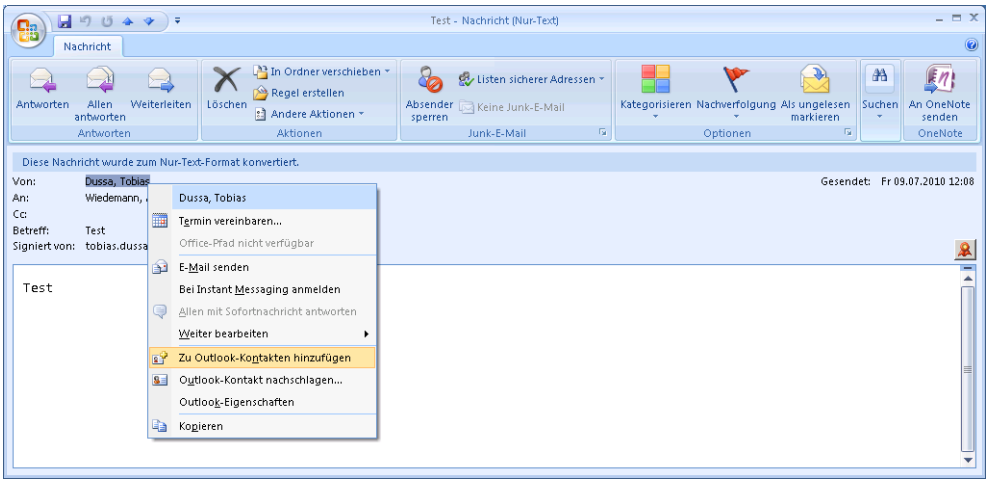
5.2 Automatischer Import

Wenn Ihnen eine signierte E-Mail vorliegt, so ist das Nutzerzertifikat des Absenders bereits vorhanden. Der Import in das Mailprogramm ist in diesem Fall deutlich einfacher als beim manuellen Import.

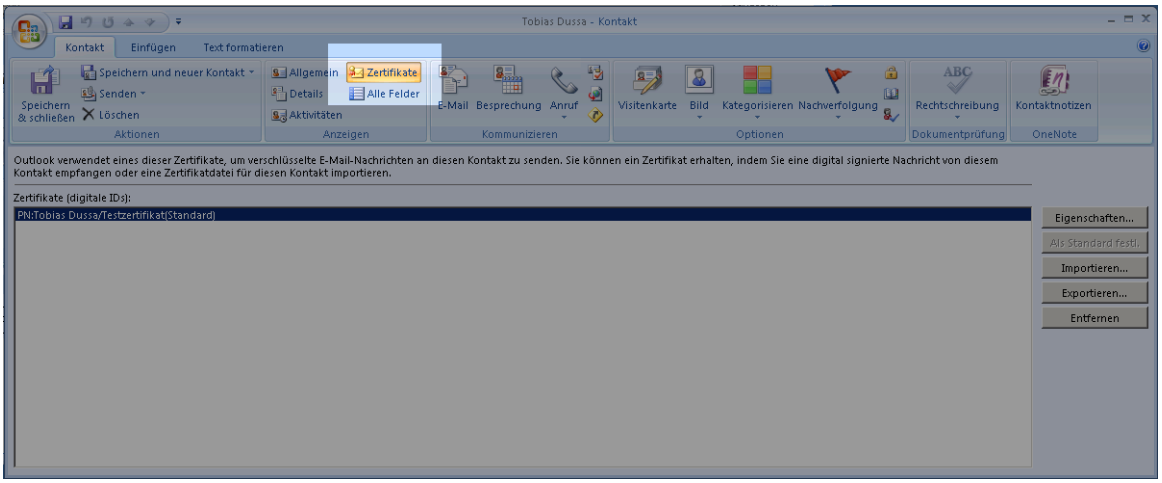
5.2.1 Microsoft Outlook 2003 und 2007

Microsoft Outlook kann Nutzerzertifikate nur mit Empfängern von E-Mails verknüpfen, die im Adressbuch vorhanden sind. Um das Zertifikat des Absenders einer signierten E-Mail zu importieren, ist es daher notwendig, den Absender als Kontakt zum Adressbuch hinzuzufügen. Sollte derselbe Kontakt bereits vorhanden sein, so wird dies nach dem Hinzufügen von Outlook erkannt; es ist zunächst dennoch notwendig, einen neuen Kontakt hinzuzufügen. Die Bildschirmfotos wurden beispielhaft mit Outlook 2007 erzeugt; der Vorgang ist bei Outlook 2003 aber derselbe.

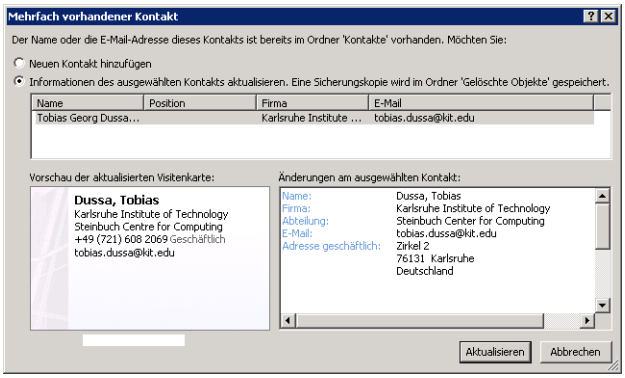
1. Klicken Sie mit der rechten Maustaste auf den Absender der signierten E-Mail und wählen Sie den Menüpunkt »Zu Outlook-Kontakten hinzufügen«.



2. Ein neues Kontaktfenster wird geöffnet, das alle gefundenen Daten anzeigt. Insbesondere ist unter dem Reiter »Zertifikate«, der in der Abbildung hervorgehoben ist, das neu hinzugefügte Zertifikat aufgeführt. Speichern und schließen Sie das Formular.



3. Sollte bereits ein Kontakt mit derselben E-Mail-Adresse im Adressbuch vorhanden sein, so wird dies von Outlook erkannt. Es wird vorgeschlagen, die Kontakte zusammenzuführen; ein entsprechender Dialog wird angezeigt. Bestätigen Sie mit »Aktualisieren«.



5.2.2 Mozilla Thunderbird 3.0 und 3.1

Thunderbird erledigt das Importieren von Zertifikaten signierter E-Mails vollautomatisch. Es ist lediglich notwendig, eine signierte Mail zu öffnen, um das Zertifikat zu importieren.

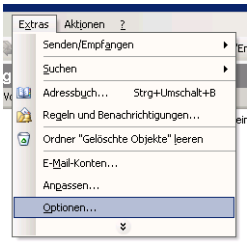
6 Konfigurieren Ihres Mailprogramms

Zum Verwenden der importierten Zertifikate ist es notwendig, das Mailprogramm entsprechend zu konfigurieren, bevor E-Mails signiert oder verschlüsselt werden können.

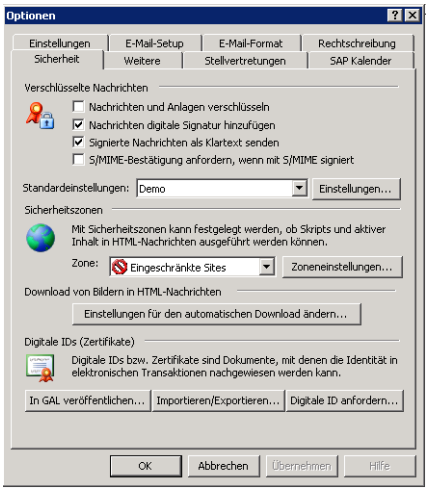
6.1 Microsoft Outlook 2003

In Outlook 2003 gehen Sie wie folgt vor, um die notwendigen Konfigurationen vorzunehmen.

1. Klicken Sie im Menü »Extras« auf den Eintrag »Optionen«.

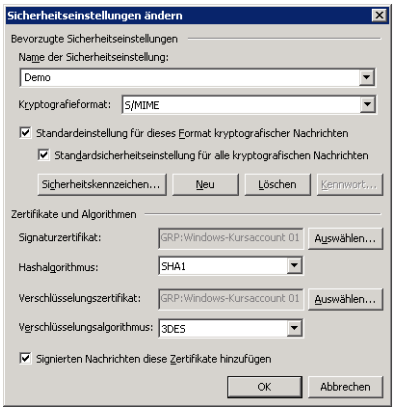


2. Klicken Sie auf den seitlichen Reiter »Sicherheit« und aktivieren Sie die folgenden Einstellungen:
   - »Nachrichten und Anlagen verschlüsseln«, sofern Sie ausgehende E-Mails standardmäßig verschlüsseln möchten,
   - »Nachrichten digitale Signatur hinzufügen«, sofern Sie ausgehende E-Mails standardmäßig verschlüsseln möchten,
   - »Signierte Nachrichten als Klartext senden« sowie



3. Klicken Sie auf die Schaltfläche »Einstellungen« und führen Sie die folgenden Einstellungen durch.
   - Wählen Sie Ihr Signaturzertifikat aus, indem Sie auf die zugehörige Schaltfläche »Auswählen« klicken, Ihr Zertifikat auswählen und bestätigen.
   - Wählen Sie als Hashalgorithmus »SHA1« aus.

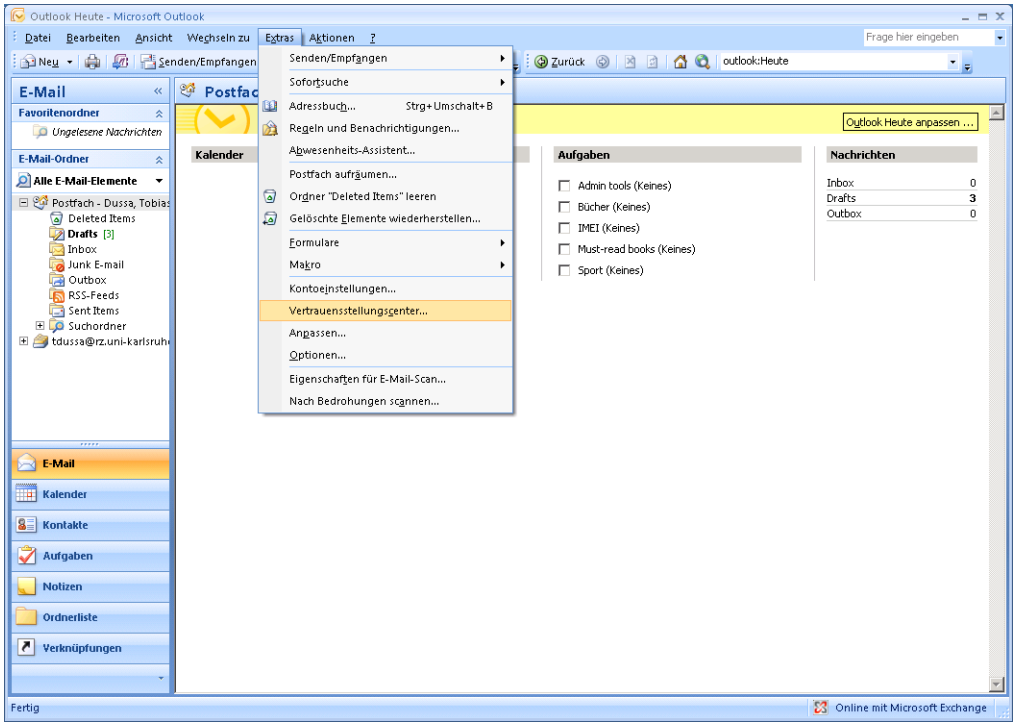
- Wählen Sie Ihr Verschlüsselungszertifikat aus, indem Sie auf die zugehörige Schaltfläche »Auswählen« klicken, Ihr Zertifikat auswählen und bestätigen.
- Wählen Sie als Verschlüsselungsalgorithmus »3DES« aus. Aus Kompatibilitätsgründen mit älteren Windows-Versionen ist »AES-256« nicht empfehlenswert.



6.2 Microsoft Outlook 2007

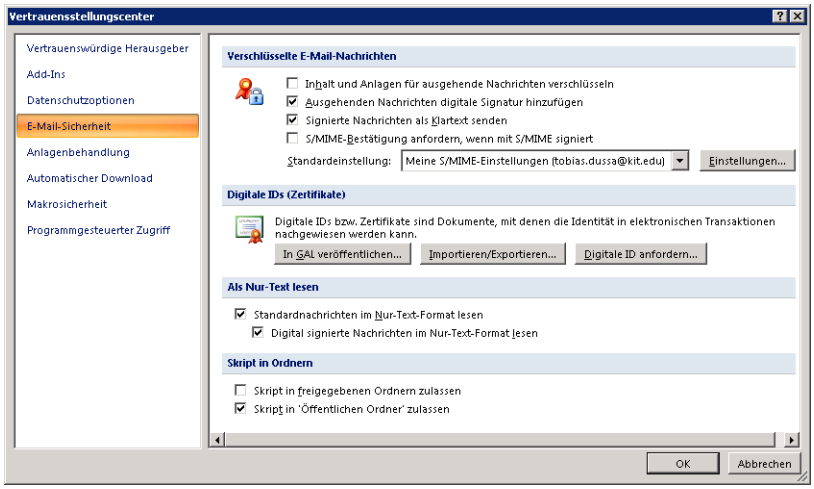
In Outlook 2007 gehen Sie wie folgt vor, um die notwendigen Konfigurationen vorzunehmen.

1. Klicken Sie im Menü »Extras« auf den Eintrag »Vertrauensstellungscerter«.

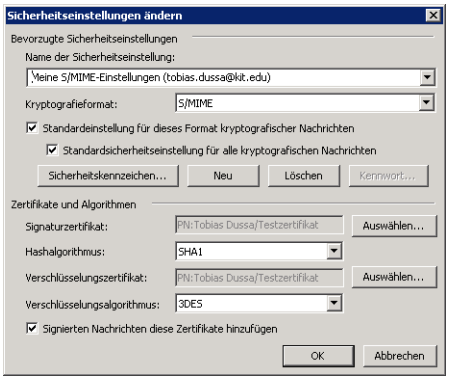


2. Klicken Sie auf den seitlichen Reiter »E-Mail-Sicherheit« und aktivieren Sie die folgenden Einstellungen:
   - »Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln«, sofern Sie ausgehende E-Mails standardmäßig verschlüsseln möchten,
   - »Ausgehenden Nachrichten digitale Signatur hinzufügen«, sofern Sie ausgehende E-Mails standardmäßig verschlüsseln möchten,

- »Signierte Nachrichten als Klartext senden«,
- »Standardnachrichten im Nur-Text-Format lesen« sowie
- »Digital signierte Nachrichten im Nur-Text-Format lesen«.



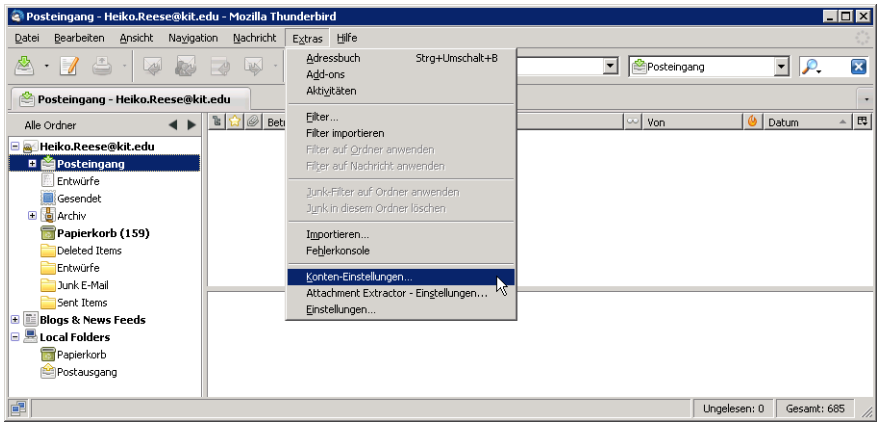
3. Klicken Sie auf die Schaltfläche »Einstellungen« und führen Sie die folgenden Einstellungen durch.
   - Wählen Sie Ihr Signaturzertifikat aus, indem Sie auf die zugehörige Schaltfläche »Auswählen« klicken, Ihr Zertifikat auswählen und bestätigen.
   - Wählen Sie als Hashalgorithmus »SHA1« aus.
   - Wählen Sie Ihr Verschlüsselungszertifikat aus, indem Sie auf die zugehörige Schaltfläche »Auswählen« klicken, Ihr Zertifikat auswählen und bestätigen.
   - Wählen Sie als Verschlüsselungsalgorithmus »3DES« aus. Aus Kompatibilitätsgründen mit älteren Windows-Versionen ist »AES-256« nicht empfehlenswert.



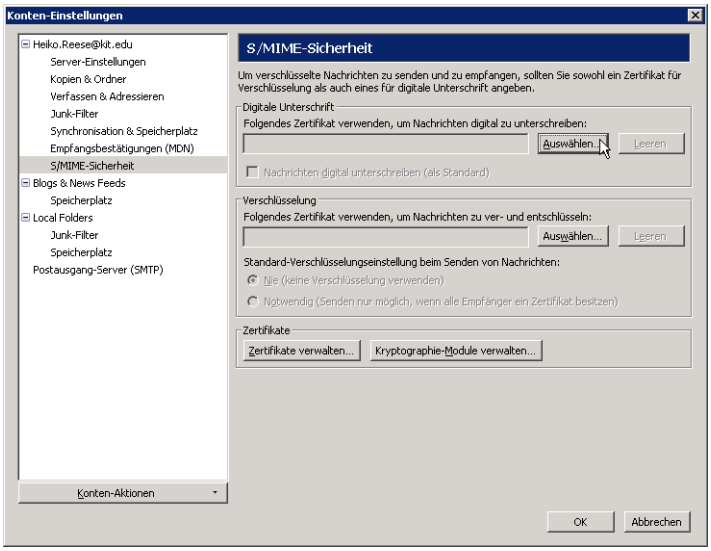
6.3 Mozilla Thunderbird 3.0 und 3.1

Um Ihr Konto in Mozilla Thunderbird zum Verschlüsseln oder Signieren von E-Mails zu konfigurieren, sind die folgenden Schritte notwendig. In den Abbildungen werden Bildschirmfotos der einzelnen Schritte gezeigt. Die Bildschirmfotos wurden beispielhaft mit Thunderbird 3.1 erstellt; die wesentlichen Bearbeitungsschritte sind aber bei Thunderbird 3.0 identisch.

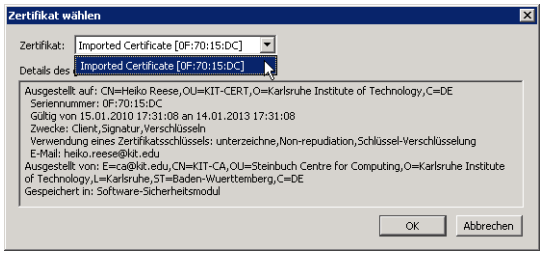
1. Klicken Sie im Menü »Extras« auf den Punkt »Konten-Einstellungen«.



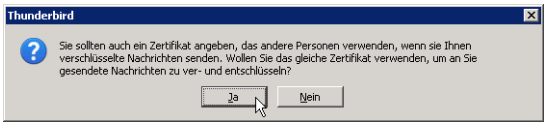
2. Wählen Sie links den Bereich »S/MIME-Sicherheit«. Klicken Sie dann im rechten Teil im Abschnitt »Digitale Unterschrift« auf die Schaltfläche »Auswählen«.



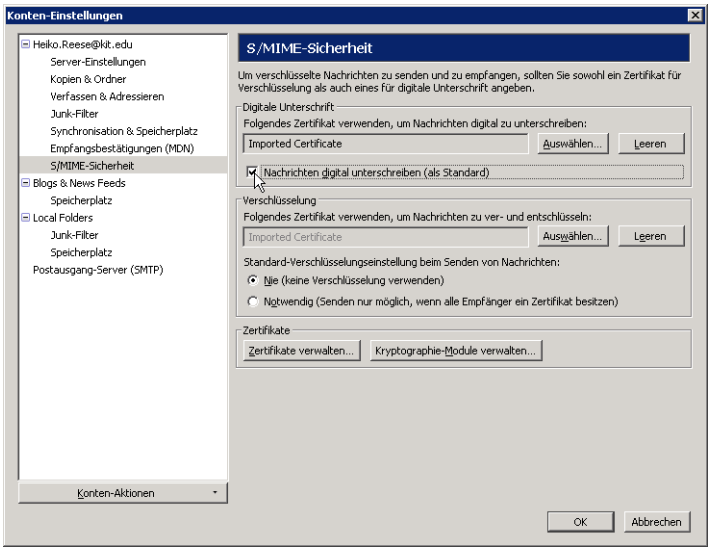
3. In der folgenden Dialogbox können Sie das Zertifikat auswählen, das Sie zum Signieren Ihrer E-Mails verwenden möchten. In der Regel wird Ihnen nur ein einziges Zertifikat zur Auswahl angeboten; die Bezeichnung des Zertifikats in der Auswahlliste ist dabei leider nicht besonders aussagekräftig (»Imported Certificate [0F:70:15:DC]« im Beispiel in der Abbildung). Im unteren Teil des Fensters werden aber die Detailinformationen des jeweils ausgewählten Zertifikats ausführlich aufgeführt.



4. Thunderbird fragt in der folgenden Dialogbox, ob Sie dasselbe Zertifikat auch zum Ver- beziehungsweise Entschlüsseln von E-Mails an Sie selber verwenden möchten. Bestätigen Sie dies, indem Sie auf die Schaltfläche »Ja« klicken.



5. Wenn Sie ausgehende Nachrichten standardmäßig signieren möchten, so setzen Sie im Dialog »S/MIME-Sicherheit« den Haken bei »Nachrichten digital unterschreiben (als Standard)«. Es ist nach wie vor möglich, bei jeder ausgehenden E-Mail einzeln die Signierung zu aktivieren oder zu deaktivieren; mit dieser Einstellung wird lediglich die Voreinstellung ausgewählt.

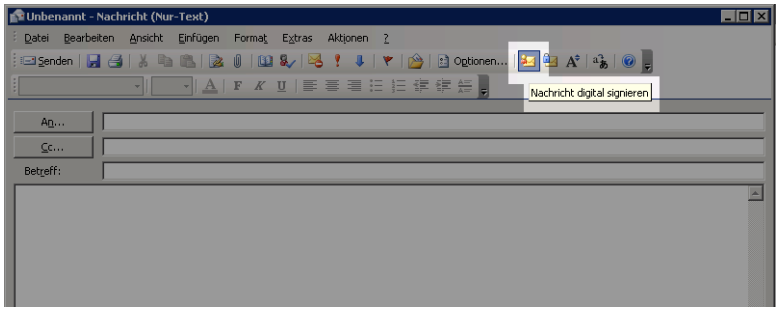


7 Signieren von E-Mails

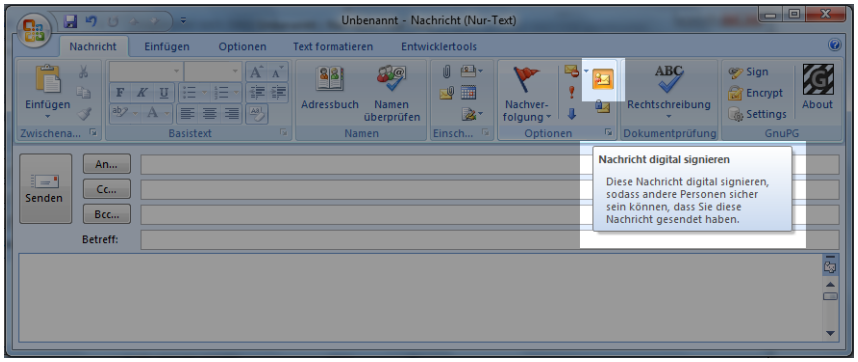
7.1 Microsoft Outlook 2003 und 2007

Um mit Outlook eine ausgehende Nachricht zu signieren, müssen Sie die Schaltfläche zum Signieren von E-Mails im Nachrichteneditor aktivieren; siehe hierzu auch die folgenden beiden Abbildungen. Wenn Sie in den Einstellungen Outlook so konfiguriert haben, dass ausgehende Nachrichten standardmäßig signiert werden sollen, so ist diese Schaltfläche bereits aktiviert; andernfalls müssen Sie sie manuell aktivieren. Gegebenenfalls müssen Sie beim Absenden noch den Zugriff auf Ihren geheimen Schlüssel bestätigen.

Outlook 2003:

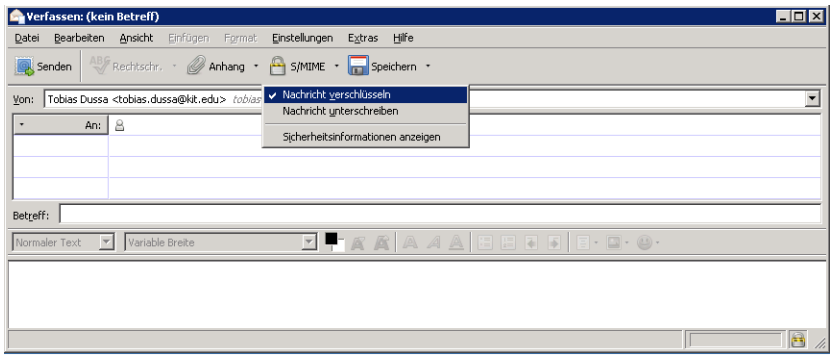


Outlook 2007:



7.2 Mozilla Thunderbird 3.0 und 3.1

Um mit Thunderbird eine ausgehende Nachricht zu signieren, müssen Sie nur die entsprechende Option zum Signieren der E-Mail aktivieren.

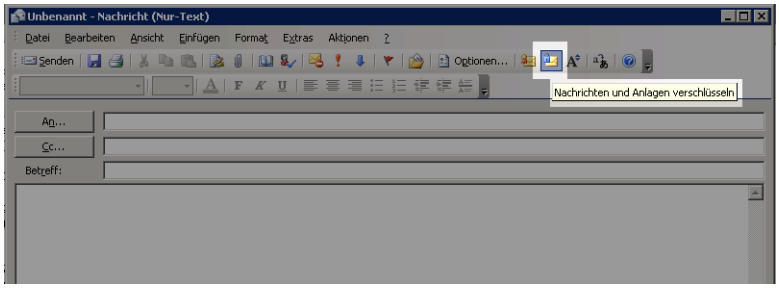


8 Verschlüsseln von E-Mails

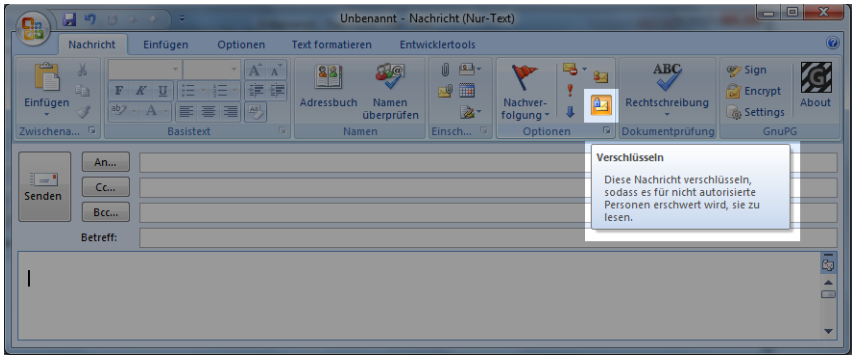
8.1 Microsoft Outlook 2003 und 2007

Um mit Outlook eine ausgehende Nachricht zu verschlüsseln, müssen Sie die Schaltfläche zum Verschlüsseln von E-Mails im Nachrichteneditor aktivieren; siehe hierzu auch die folgenden beiden Abbildungen. Wenn Sie in den Einstellungen Outlook so konfiguriert haben, dass ausgehende Nachrichten standardmäßig verschlüsselt werden sollen, so ist diese Schaltfläche bereits aktiviert; andernfalls müssen Sie sie manuell aktivieren.

Outlook 2003:



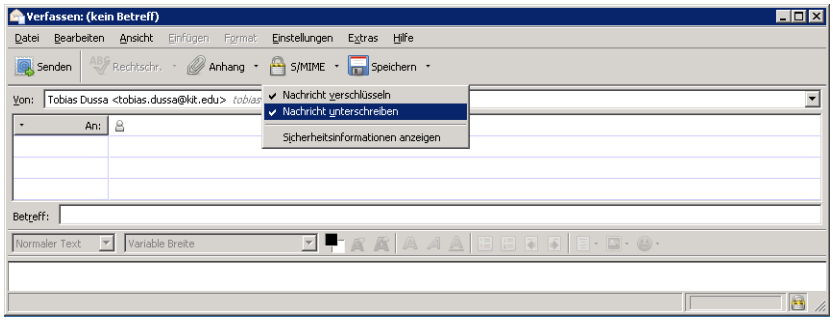
Outlook 2007:



Outlook verschlüsselt E-Mails automatisch auch an den Absender, damit dieser die Nachricht später auch noch lesen kann, wenn Sie im »Gesendet«-Ordner abgelegt ist. Daher ist es auch zum Senden verschlüsselter Nachrichten notwendig, das eigene X.509-Zertifikat sowie den passenden geheimen Schlüssel zu importieren.

8.2 Mozilla Thunderbird 3.0 und 3.1

Um mit Thunderbird eine ausgehende Nachricht zu verschlüsseln, müssen Sie nur die entsprechende Option zum Verschlüsseln der E-Mail aktivieren.



Thunderbird verschlüsselt E-Mails automatisch auch an den Absender, damit dieser die Nachricht später auch noch lesen kann, wenn Sie im »Gesendet«-Ordner abgelegt ist. Daher ist es auch zum Senden verschlüsselter Nachrichten notwendig, das eigene X.509-Zertifikat importiert und konfiguriert zu haben.