KATHOLISCHE UNIVERSITÄT EICHSTÄTT INGOLSTADT

IN KUERZE

IN formationen Katholische Universität Eichstätt-Ingolstadt RechenZEntrum

Jahrgang 25 Nummer 1 ISSN 0939 – 3277 Juni 2014

E-Mails komfortabel verschlüsseln und signieren

B. Brandel

Seit vielen Jahren sichert die KU ihre Serverzugänge per TLS/SSL durch eigene X.509-Zertifikate ab, die wir über den erweiterten Zertifizierungsdienst „DFN-PKI“ des DFN-Vereins schnell und unaufwändig erhalten.
Weniger verbreitet ist, dass wir auf dem gleichen Wege für Beschäftigte der KU persönliche Nutzerzertifikate ausstellen können, mit denen eine komfortable E-Mail-Verschlüsselung samt digitaler Signatur möglich ist. Unerwünschte Eingriffe in Ihre Privatsphäre können Sie damit wirkungsvoll verhindern. Wie Sie ein solches Zertifikat erhalten und in Thunderbird, Outlook und Co. einbauen, erfahren Sie in diesem Artikel.

Was ist ein Zertifikat?

Ein X.509-Zertifikat [1] ist ein digitaler Ausweis für einen Server oder eine Person. Es ist von einer übergeordneten Zertifizierungsstelle [Certification Authority (CA)] ausgestellt, die für die Echtheit des Ausweises bürgt. Das Zertifikat enthält außer dem digitalen Stempel auch noch den Namen des Servers bzw. Benutzers sowie dessen öffentlichen Schlüssel. Je „offizieller“ der Stempel, desto glaubwürdiger das Zertifikat:
Alle Zertifikate der KU sind über eine Zertifikatskette mit dem Wurzelzertifikat der T-Systems (Deutsche Telekom Root CA 2) verbunden. Da dieses Wurzelzertifikat in jedem gängigen Browser und E-Mail-Programm fest eingebaut ist, werden alle KU-Zertifikate automatisch weltweit als korrekt erkannt. Dies gilt für alle Server-Zertifikate und auch für alle Nutzer-Zertifikate der KU [2] [3] [4]!
Verwendet werden Zertifikate immer in Verbindung mit dem privaten Schlüssel des Besitzers (des Servers oder Benutzers). Dieser Key verlässt weder bei der Zertifikatserstellung noch beim Verschlüsselungsprozess den Rechner. Zertifiziert wird nämlich immer nur der öffentliche Schlüssel, denn für den privaten Schlüssel ist dies konstruktionsbedingt durch das verwendete asymmetrische Verschlüsselungsverfahren überflüssig: Aus der Echtheit des öffentlichen Schlüssels folgt die Echtheit des privaten Schlüssels automatisch.

Wo verwenden wir Zertifikate

Im KU-Alltag begegnen Sie ständig unseren Zertifikaten. Bei jedem Zugriff auf Ihre KU-Mailbox weist sich unser IMAP-Server Ihrem PC gegenüber mit seinem KU-Zertifikat aus. Entsprechende Zertifikate verwenden wir auf allen weiteren Servern der KU, auf die Sie über das HTTPS-Protokoll zugreifen, wie z.B. den Servern für WWW, EGroupware, Ilias und KU.Campus.
Genauso erfolgreich setzen Rechenzentrum und Forschungseinrichtungen der KU wie z.B unsere Hochschulambulanz Nutzerzertifikate für ihre vertrauliche E-Mail-Kommunikation ein.
Einmal eingerichtet, können Sie vollautomatisch jede E-Mail digital signieren und wichtige Nachrichten verschlüsseln!
In diesem Artikel möchten wir Ihnen zeigen, wie einfach das geht und Sie auch dazu motivieren, damit zu beginnen. Dazu brauchen Sie zuallererst ein Zertifikat.

Der Weg zum Zertifikat

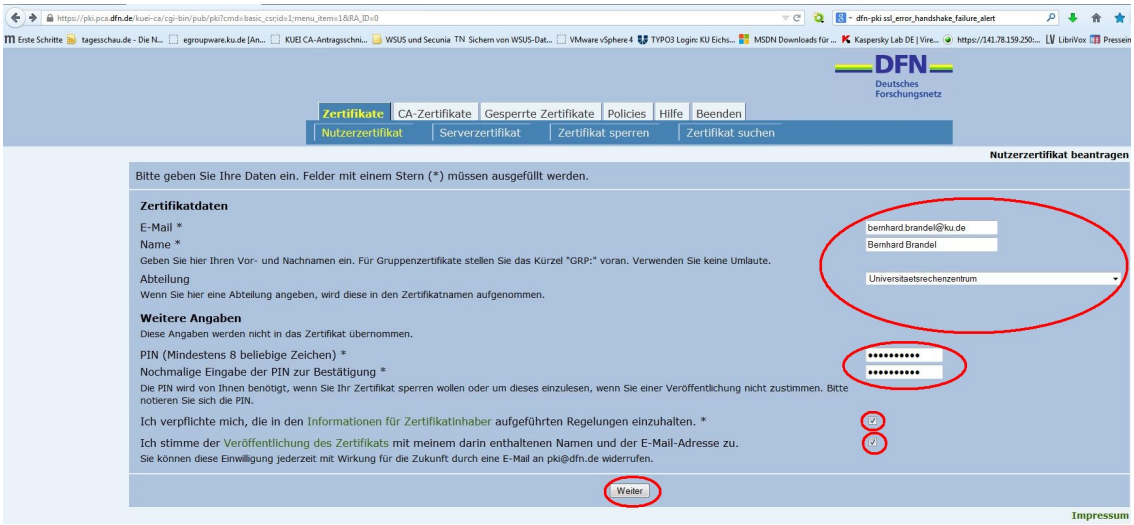
Seit Ende 2006 bietet der DFN-Verein seinen Mitgliedseinrichtungen den erweiterten Zertifizierungsdienst DFN-PKI an, mit dem diese mit vertretbarem organisatorischen und technischen Aufwand in die DFN-weite PublicKey-Infrastruktur (DFN-PKI) einsteigen können [5].
Kernidee ist die Auslagerung der aufwändigen Teilaufgaben an die DFN-PKI. Nach den Regeln (Policies) des DFN-Zertifizierungsdienstes können die Arbeiten von Registrierungsstelle [Registration Authority (RA)] und Zertifizierungsstelle (CA) getrennt voneinander durchgeführt werden [6]: Die

DFN-PKI übernimmt für uns den technisch umfangreichen Betrieb der eigentlichen Zertifizierungsstelle und ihrer Hochsicherheits-Infrastruktur und stellt dann im Namen der KU Zertifikate für die Nutzer und Ressourcen der Einrichtungen aus. Lediglich die Registrierungsstelle (RA) bleibt bei uns in unseren beiden Sekretariaten in Eichstätt und Ingolstadt.

Zertifikatsantrag und Installation in Mozilla Firefox
Da sowohl das Betriebssystem Windows selbst als auch viele Anwendungen wie Firefox, Thunderbird jeweils einen eigenen Zertifikatsspeicher besitzen, unterscheiden sich die Installationswege für Thunderbird, Outlook etc. leicht voneinander. Im folgenden beschreiben wir hier im Detail die Zertifikatserstellung und -nutzung in Mozilla Thunderbird. Sie können aber jederzeit Ihr Zertifikat auch in andere E-Mail-Programme wie Outlook oder auf ein iPad importieren und dort verwenden.

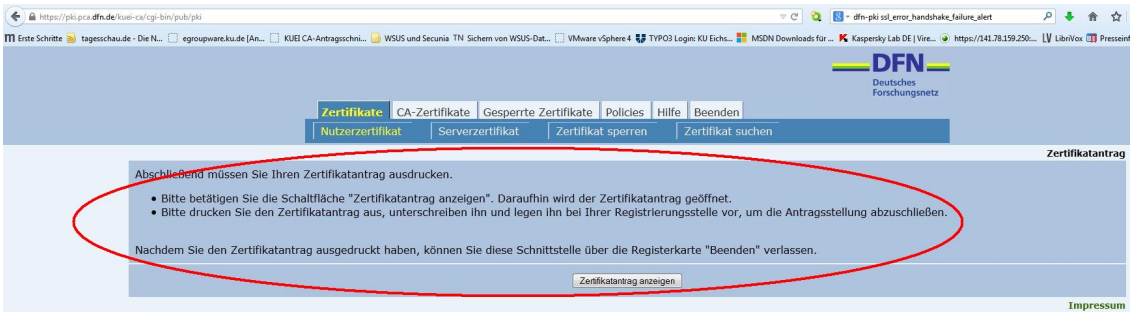
Der Zertifikatsantrag besteht aus folgenden Schritten:

- ▷ Zuallererst starten Sie Mozilla Firefox, und zwar unbedingt auf Ihrem eigenen PC. Über den Link `https://pki.pca.dfn.de/kuei-ca/cgi-bin/pub/pki?cmd=basic_csr;id=1;menu_item=1&RA_ID=0` [7] gelangen Sie zu unserer Antragsschnittstelle. Dort füllen Sie bitte folgendes kurze WWW-Formular mit Ihren Daten aus:
  Machen Sie bitte im Reiter „Nutzerzertifikat“ die nötigen Angaben (E-Mailadresse, Vor- und Nachname, Abteilung und Sperr-Pin plus Bestätigung sowie die beiden Häkchen), lesen alles gut durch und bestätigen mit „Weiter“ (siehe Bild).

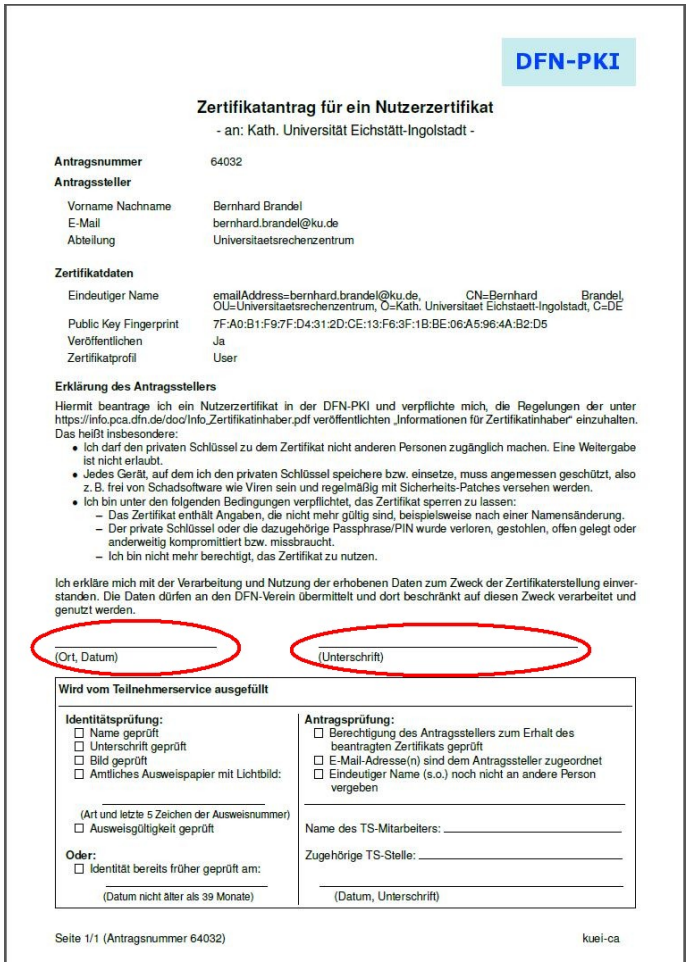


Nach Klick auf „Weiter“ und „Bestätigen“ wird nun auf Ihrem PC im Kryptomodul von Mozilla Firefox Ihr Schlüsselpaar erzeugt und der Zertifikatsantrag, der nur den öffentlichen, aber nicht den privaten Schlüssel enthält, übers WWW direkt an unsere Registrierungsstelle in unseren Sekretariaten geschickt.
Hätten Sie den Antrag von einem fremden PC aus gestellt, läge Ihr privater Schlüssel nun dort! Deshalb sollten Sie unbedingt den Antrag auf Ihrem eigenen PC stellen, damit der Key genau auf dem Rechner ist, auf den er gehört!

▷ Als nächstes müssen Sie den Zertifikatantrag wie hier beschrieben



ausdrucken



DFN-PKI

Zertifikatantrag für ein Nutzerzertifikat

- an: Kath. Universität Eichstätt-Ingolstadt -

Antragsnummer 64032

Antragssteller

Vorname Nachname	Bernhard Brandel
E-Mail	bernhard.brandel@ku.de
Abteilung	Universitaetsrechenzentrum

Zertifikatdaten

Eindeutiger Name	emailAddress=bernhard.brandel@ku.de, CN=Bernhard Brandel, OU=Universitaetsrechenzentrum, O=Kath. Universitaet Eichstaett-Ingolstadt, C=DE
Public Key Fingerprint	7F:A0:B1:F9:7F:D4:31:2D:CE:13:F6:3F:1B:BE:06:A5:96:4A:B2:D5
Veröffentlichen	Ja
Zertifikatprofil	User

Erklärung des Antragsstellers

Hiermit beantrage ich ein Nutzerzertifikat in der DFN-PKI und verpflichte mich, die Regelungen der unter https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf veröffentlichten „Informationen für Zertifikatinhaber" einzuhalten. Das heißt insbesondere:

- Ich darf den privaten Schlüssel zu dem Zertifikat nicht anderen Personen zugänglich machen. Eine Weitergabe ist nicht erlaubt.
- Jedes Gerät, auf dem ich den privaten Schlüssel speichere bzw. einsetze, muss angemessen geschützt, also z. B. frei von Schadsoftware wie Viren sein und regelmäßig mit Sicherheits-Patches versehen werden.
- Ich bin unter den folgenden Bedingungen verpflichtet, das Zertifikat sperren zu lassen:
  - Das Zertifikat enthält Angaben, die nicht mehr gültig sind, beispielsweise nach einer Namensänderung.
  - Der private Schlüssel oder die dazugehörige Passphrase/PIN wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
  - Ich bin nicht mehr berechtigt, das Zertifikat zu nutzen.

Ich erkläre mich mit der Verarbeitung und Nutzung der erhobenen Daten zum Zweck der Zertifikaterstellung einverstanden. Die Daten dürfen an den DFN-Verein übermittelt und dort beschränkt auf diesen Zweck verarbeitet und genutzt werden.

(Ort, Datum) (Unterschrift)

Wird vom Teilnehmerservice ausgefüllt

Identitätsprüfung:
☐ Name geprüft
☐ Unterschrift geprüft
☐ Bild geprüft
☐ Amtliches Ausweispapier mit Lichtbild:
(Art und letzte 5 Zeichen der Ausweisnummer)
☐ Ausweisgültigkeit geprüft

Oder:
☐ Identität bereits früher geprüft am:
(Datum nicht älter als 39 Monate)

Antragsprüfung:
☐ Berechtigung des Antragsstellers zum Erhalt des beantragten Zertifikats geprüft
☐ E-Mail-Adresse(n) sind dem Antragssteller zugeordnet
☐ Eindeutiger Name (s.o.) noch nicht an andere Person vergeben

Name des TS-Mitarbeiters:

Zugehörige TS-Stelle:

(Datum, Unterschrift)

Seite 1/1 (Antragsnummer 64032) kuei-ca

und unterschreiben, danach beenden Sie bitte das WWW-Formular.

▷ Legen Sie nun diesen Ausdruck samt Unterschrift und Personalausweis bei der RA (im URZ-Sekretariat) vor. Das RA-Personal prüft nun Ihre Identität, den Ausdruck samt Unterschrift und erteilt anschließend ebenfalls übers WWW auf abgesicherter Verbindung mit der digitalen Unterschrift des Bearbeiters die Genehmigung zur Erstellung des Zertifikats durch die eigentliche Zertifizierungsstelle DFN-PCA in Hamburg (CA).

▷ Die CA erzeugt nun unter strengen Sicherheitskriterien das Zertifikat und leitet dieses dem Nutzer anschließend per E-Mail zu.

In dieser Mail (siehe folgendes Bild) sind die Schritte genau beschrieben, die Sie noch erledigen müssen, damit Ihr Zertifikat auf Ihrem Rechner nutzbar wird. Sie müssen dazu die drei CA-Zertifikate und Ihr eigenes jeweils per Mausklick importieren:

Von ra@ku-eichstaett.de
Betreff **KUEI CA Zertifikatinformation**
An Mich <bernhard.brandel@ku.de>
Kopie (CC) ra@ku-eichstaett.de

Sehr geehrte Nutzerin, sehr geehrter Nutzer,

die Bearbeitung Ihres Zertifizierungsantrags ist nun abgeschlossen.

Ihr Zertifikat mit der Seriennummer 6656124295772472 ist auf den Namen
CN=Bernhard Brandel,OU=Universitaetsrechenzentrum,O=Kath. Universitaet Eichstaett-Ingolstadt,C=DE
erstellt worden und im Anhang dieser Mail beigelegt.
Sie benötigen die Seriennummer, um Ihr Zertifikat gegebenenfalls sperren zu können.

Um Ihr Zertifikat nutzen zu können, müssen Sie alle folgenden Zertifikate in
Ihren Browser importieren. Achten Sie darauf, dass Sie die Zertifikate auf dem
Rechner importieren, von dem aus Sie den Antrag gestellt haben, weil sich dort
der zugehörige Schlüssel befindet.

1. Für die CA-Zertifikate wählen Sie bitte die Seite
https://pki.pca.dfn.de:443/kuei-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2
und folgen den Anweisungen.

2. Ihr eigenes Zertifikat erhalten Sie direkt über folgenden Link:
https://pki.pca.dfn.de:443/kuei-ca/cgi-bin/pub/pki?cmd=getcert&key=6656124295772472&type=CERTIFICATE

Befolgen Sie bitte die in dem Dokument "Informationen für Zertifikatinhaber" aufgeführten Regelungen: https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf

Mit freundlichen Grüßen

Ihr PKI-Team der Kath. Universitaet Eichstaett-Ingolstadt

Im ersten Link in der E-Mail klicken Sie nacheinander auf „Wurzelzertifikat“, „DFN-PCA Zertifikat“ und „KUEI CA Zertifikat“,

DFN Deutsches Forschungsnetz

Zertifikate | CA-Zertifikate | Gesperrte Zertifikate | Policies | Hilfe | Beenden

Wurzelzertifikat | DFN-PCA-Zertifikat | KUEI-CA-Zertifikat | Zertifikatkette anzeigen

Schnittstelle für Nutzer und Administratoren - CA-Zertifikate

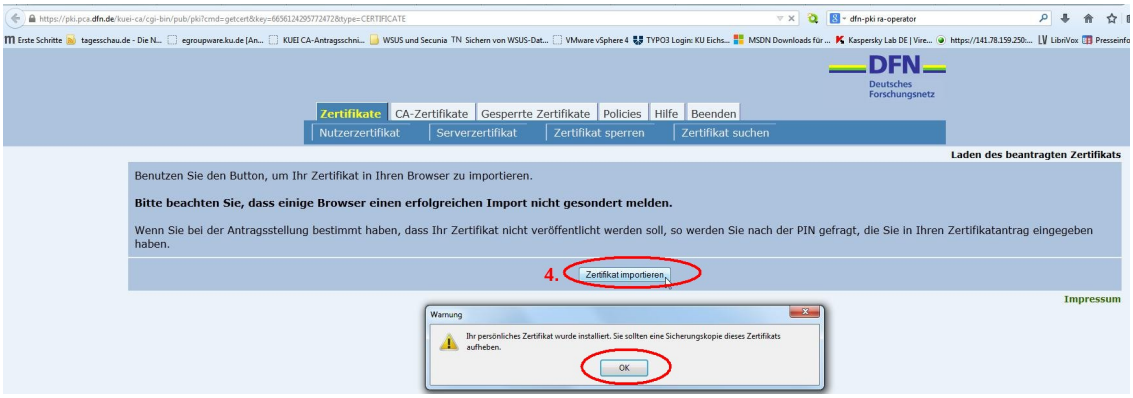
Hier können Sie das Wurzelzertifikat, das DFN-PCA-Zertifikat und das CA-Zertifikat in Ihrem Browser installieren oder alle Zertifikate in einer Datei speichern.

- Wählen Sie "Wurzelzertifikat", "DFN-PCA Zertifikat" bzw. "KUEI CA Zertifikat" um das jeweilige Zertifikat in Ihrem Browser zu installieren.
- Wählen Sie "Zertifikatkette anzeigen", wenn Sie die Zertifikate in einer Datei speichern möchten (PEM-Format).
- **Hinweis:** Die SHA-1-Version des CA-Zertifikats finden Sie hier: KUEI CA Zertifikat SHA-1, DFN-PCA-Zertifikat SHA-1

Kontaktinformationen für Rückfragen finden Sie unter "Hilfe".

Impressum

danach im zweiten Link auf „Zertifikat importieren“



DFN Deutsches Forschungsnetz

Zertifikate | CA-Zertifikate | Gesperrte Zertifikate | Policies | Hilfe | Beenden

Nutzerzertifikat | Serverzertifikat | Zertifikat sperren | Zertifikat suchen

Laden des beantragten Zertifikats

Benutzen Sie den Button, um Ihr Zertifikat in Ihren Browser zu importieren.

Bitte beachten Sie, dass einige Browser einen erfolgreichen Import nicht gesondert melden.

Wenn Sie bei der Antragsstellung bestimmt haben, dass Ihr Zertifikat nicht veröffentlicht werden soll, so werden Sie nach der PIN gefragt, die Sie in Ihren Zertifikatantrag eingegeben haben.

4. Zertifikat importieren

Impressum

Warnung

Ihr persönliches Zertifikat wurde installiert. Sie sollten eine Sicherungskopie dieses Zertifikats aufheben.

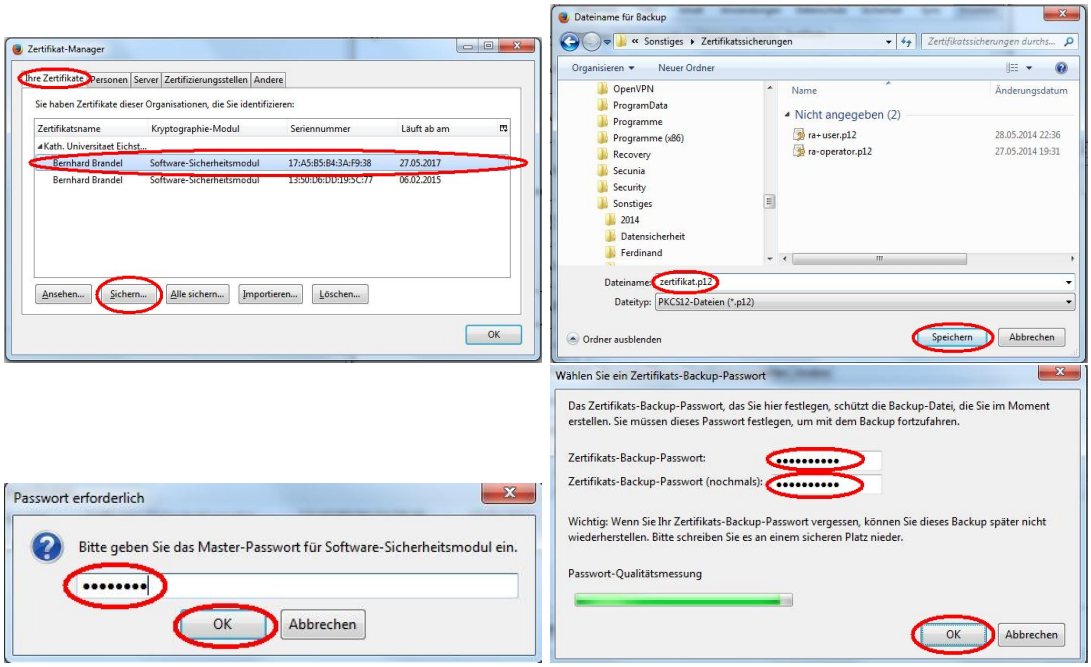
OK

und zum Schluss auf „OK“. Fertig!
Schon sind die drei CA-Zertifikate und Ihr persönliches Nutzerzertifikat in Mozilla Firefox installiert. Beachten Sie auch die ebenfalls in der Mail verlinkten Regelungen für Zertifikatsinhaber!

Ihr Nutzerzertifikat ist ein digitaler Ausweis mit integriertem öffentlichen Schlüssel, der von der Zertifizierungsstelle geprüft und abgestempelt wurde. Das Verfahren ähnelt der Ausstellung eines Personalausweises über das Meldeamt (Antragsannahme, Identitätsprüfung) und die Bundesdruckerei (Ausweiserstellung). Ausführliche Informationen finden Sie unter [8].

Sicherung des Zertifikats samt privatem Schlüssel und Export
Bevor wir mit dem Verschlüsseln und Signieren von E-Mails beginnen können, müssen wir noch Zertifikat und Schlüssel aus Mozilla Firefox exportieren und nach Mozilla Thunderbird importieren, damit Thunderbird auf Zertifikat und Schlüssel zugreifen kann. Als Nebeneffekt erhalten Sie beim Export eine Sicherung von Zertifikat und Schlüssel, die Sie unbedingt an einem getrennten und sicheren Ort aufbewahren sollten.
Gehen Sie dazu wie unter [9] beschrieben vor:

- ▷ Exportieren Sie Ihr Zertifikat mit privatem Schlüssel:
  Unter „Extras → Einstellungen → Erweitert → Zertifikate anzeigen → Ihre Zertifikate“ markieren Sie Ihr frischgebackenes Zertifikat und klicken auf „Sichern“.

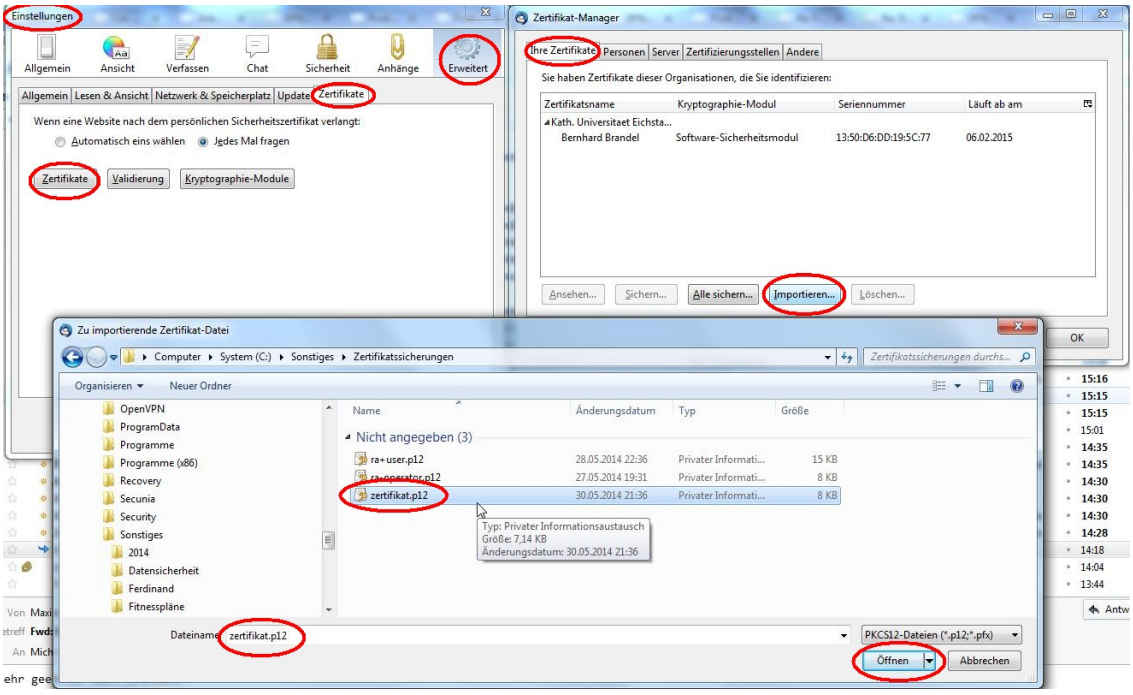


Nachdem Sie einen Dateinamen (z.B. `zertifikat.p12`) für die Sicherung ausgewählt und Ihr Master-Passwort in Firefox eingegeben haben, geben Sie ein geeignetes Backup-Passwort ein, mit dem die exportierte Datei verschlüsselt werden soll und speichern mit Klick auf „OK“ das Zertifikat, das auch Ihren privaten Schlüssel enthält, ab.

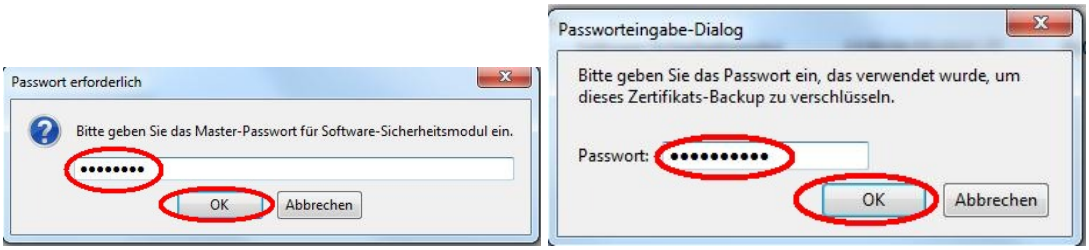
Re-Import von Zertifikat samt privatem Schlüssel nach Thunderbird

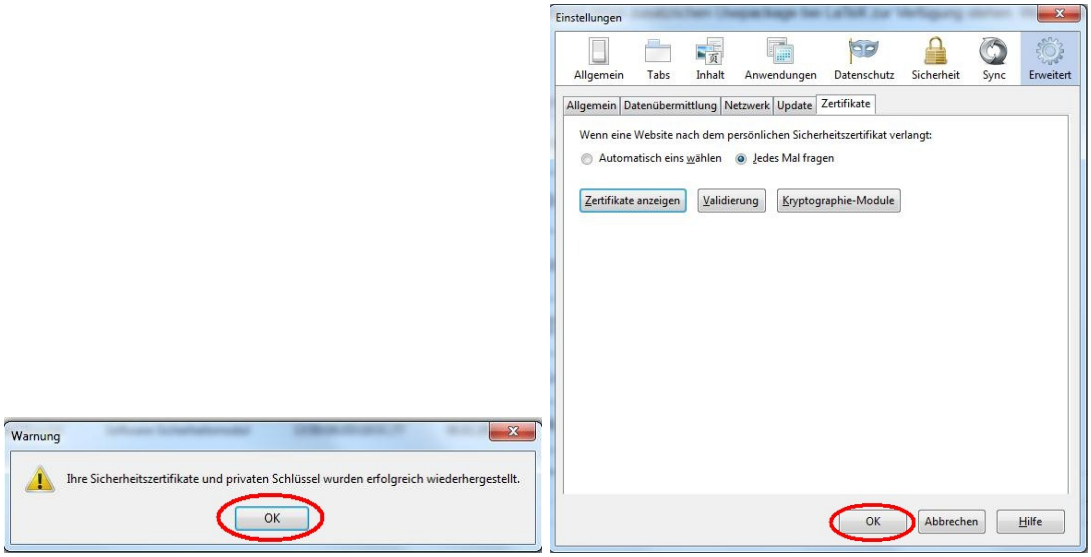
Wir benötigen die Datei gleich im nächsten Schritt zum Re-Import nach Thunderbird wieder. Bewahren Sie diese Datei auch für später noch gut auf einem externen Datenträger an einem sicheren Platz auf – sie dient gleichzeitig als Sicherheitskopie, falls Ihr Rechner einmal defekt wird! Wir gehen nun folgendermaßen vor:

- Starten Sie Mozilla Thunderbird und öffnen dort unter „Extras“ → Einstellungen → Erweitert im Reiter „Zertifikate“ mit Klick auf „Zertifikate“ den Zertifikat-Manager.
- Klicken Sie im Karteireiter „Ihre Zertifikate“ auf „Importieren“.
- Wählen Sie die gerade abgespeicherte Datei (im Beispiel: zertifikat.p12) aus, und geben Sie das vorhin verwendete „Zertifikats-Backup-Passwort“ an und klicken auf „Öffnen“.



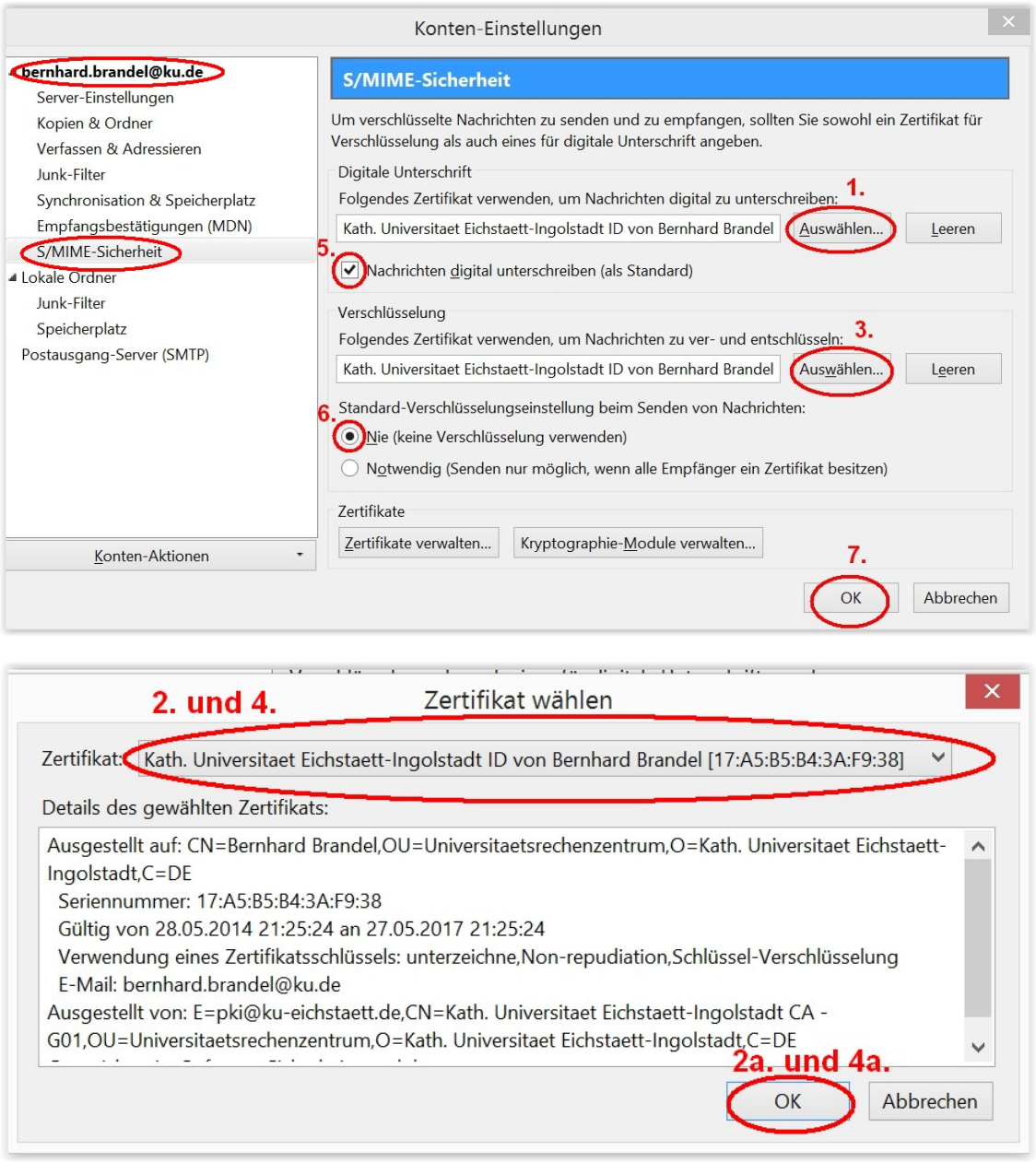
- Nach Eingabe des Masterpasswords von Thunderbird und des Backup-Passworts von soeben ist der Import erfolgreich abgeschlossen und Sie können den Zertifikatsmanager mit Klick auf „OK“ schließen.





Einstellen der S/MIME-Sicherheit des KU-Mailkontos

Ihr Zertifikat liegt nun im Zertifikatsspeicher von Thunderbird, ist aber noch nicht Ihrem KU-Mailkonto zugeordnet. Sie könnten schließlich in Thunderbird mehrere Zertifikate und mehrere Mailkontos verwenden – daher braucht Thunderbird noch weitere Informationen von Ihnen:
Damit Sie das soeben importierte Zertifikat zum Verschlüsseln und Signieren verwenden können, müssen Sie es noch mit Ihrem KU-Mailkonto verknüpfen. Dazu ist hier das richtige Zertifikat auszuwählen, siehe auch [11]. Klicken Sie dazu in Thunderbird im Menüpunkt „Extras → Konten-Einstellungen...“ bei Ihrem KU-Konto auf „S/MIME-Sicherheit“. Klicken Sie nun auf „Auswählen“ und wählen sowohl fürs Signieren als auch fürs Verschlüsseln Ihr soeben importiertes Zertifikat aus. Wir empfehlen als Voreinstellung die standardmäßige Anwendung der digitalen Unterschrift bei allen Nachrichten, jedoch nicht die standardmäßige Anwendung der Verschlüsselung. Denn verschlüsseln können Sie nur in den konkreten Fällen, in denen alle Adressaten einer E-Mail ein Zertifikat besitzen. Für vertrauliche Kommunikation sollten sich beide Kommunikationspartner Zertifikate beschaffen.



Nun steht Ihr Zertifikat mit privatem Schlüssel in Mozilla Thunderbird zur Verfügung und kann zum Verschlüsseln und Signieren Ihrer E-Mails genutzt werden.

Signieren von E-Mails – Vorteile von S/MIME gegenüber GnuPG

Über das Signieren und Verschlüsseln von elektronischer Post mit GnuPG wurde an dieser Stelle bereits geschrieben [10]. Noch einfacher als mit GnuPG-Schlüsseln lässt sich in Thunderbird & Co. elektronische Post mit S/MIME, also mit X.509-Zertifikaten, digital signieren. Ist das Zertifikat inklusive des privaten Schlüssels einmal installiert, können Sie sogar alle Post automatisch digital unterschreiben.

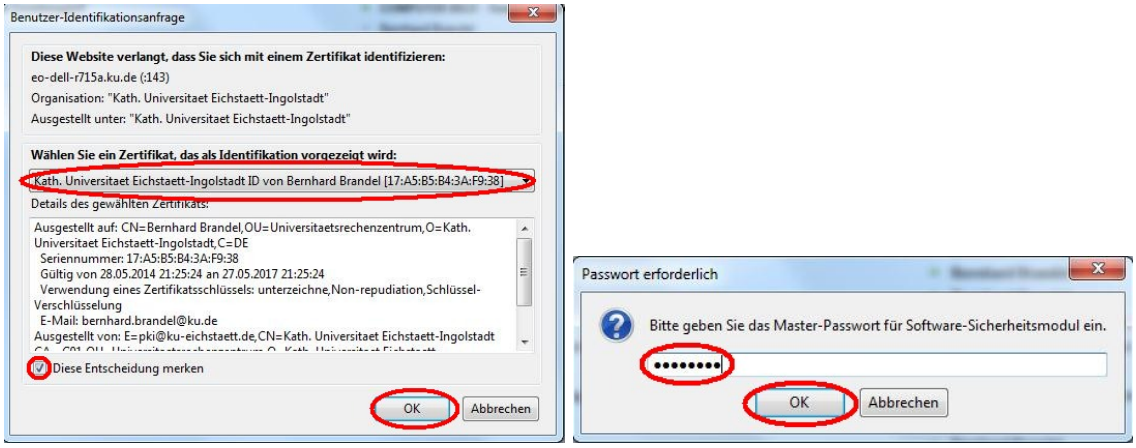
Um eine digitale Signatur zu erzeugen, benutzt der Verfasser eines Dokuments sein Zertifikat und seinen dazugehörigen privaten Schlüssel. Das E-Mail-Programm des Empfängers prüft dann anhand

dieses Zertifikats automatisch die digitale Signatur sowie die Unversehrtheit des signierten Dokuments.
Die Vorteile von S/MIME gegenüber GnuPG sind folgende:

- Die Krypto-Software ist bereits im Mailclient integriert, deshalb muss keine Plugin-Software wie Enigmail nachinstalliert werden.
- In allen gängigen E-Mail-Programmen steht Ihnen die komplette Zertifikatshierarchie des DFN „ab Werk“ zur Verfügung.
- Die Korrektheit Ihrer digitalen Unterschrift wird so von allen E-Mail-Kommunikationspartnern automatisch in ihrem Mailprogramm erkannt, ohne dass Ihre Adressaten Ihren öffentlichen Schlüssel mühsam per Hand einsammeln müssen. Deshalb müssen Sie sich auch nicht mit den Umständlichkeiten eines Web of Trust herumärgern!

In Ihrem Thunderbird ändert sich fast nichts

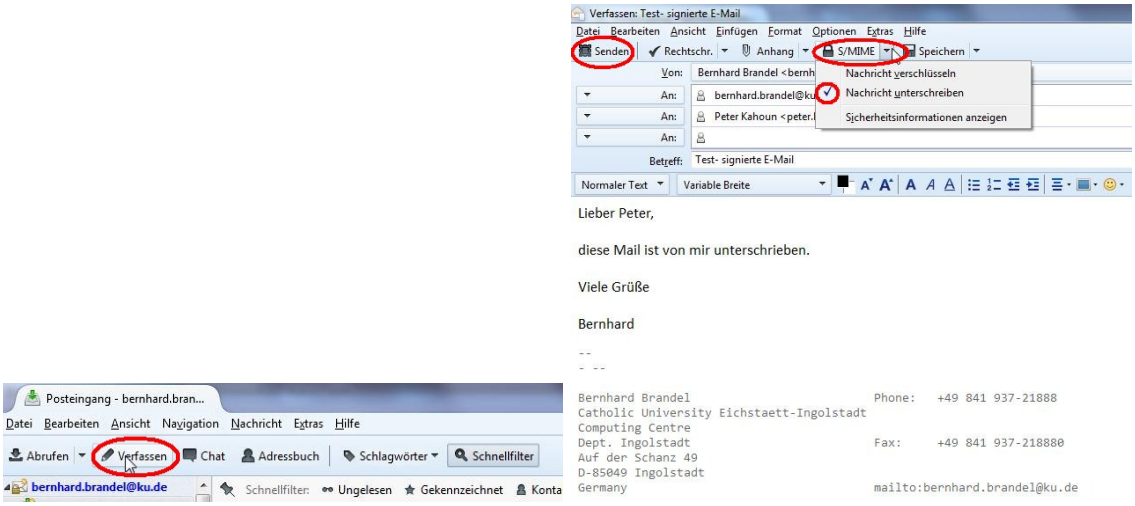
Nachdem Ihr Zertifikat in Thunderbird importiert ist, müssen Sie sich gegenüber dem IMAP-Server bei jedem Start von Thunderbird mit Ihrem Zertifikat identifizieren. Sie müssen es nur per Maus auswählen und anschließend noch, wenn Sie dazu aufgefordert werden, das Masterpasswort von Thunderbird eingeben:



Das ist fast das Einzige, was sich für Sie bei Ihrer Thunderbird-Bedienung ändert! Ansonsten schreiben und lesen Sie Ihre Mails wie gewohnt!

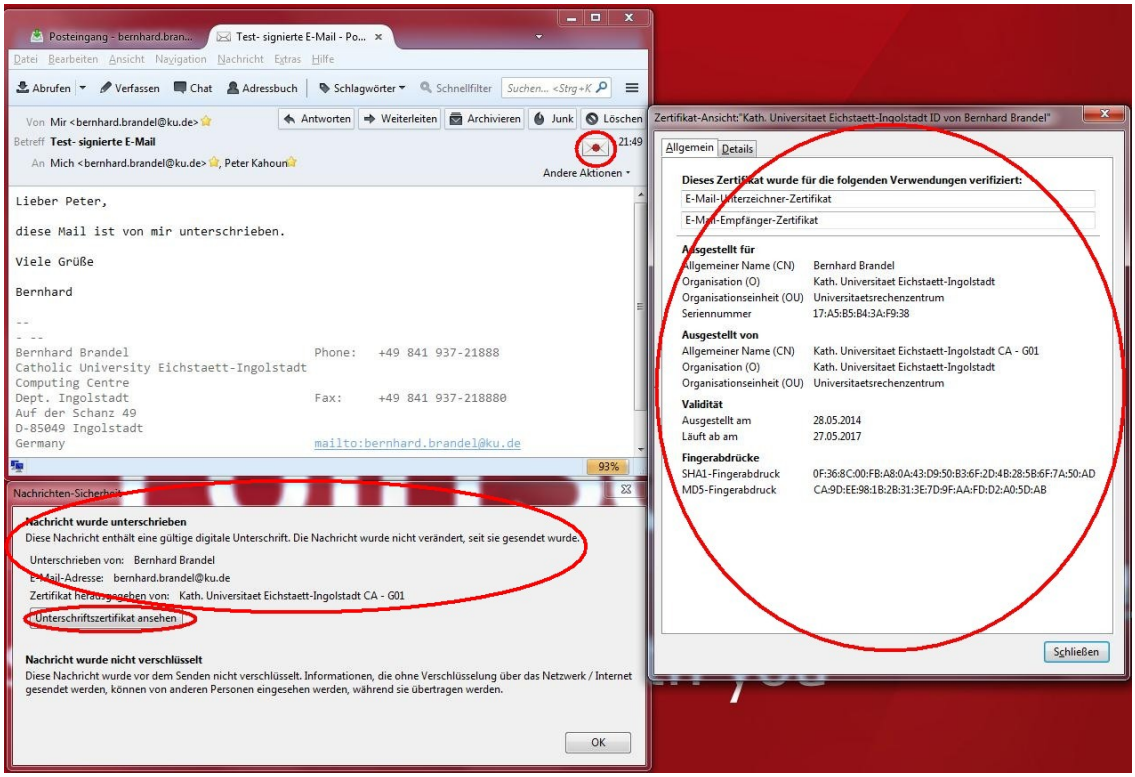
Signieren von E-Mails in Thunderbird

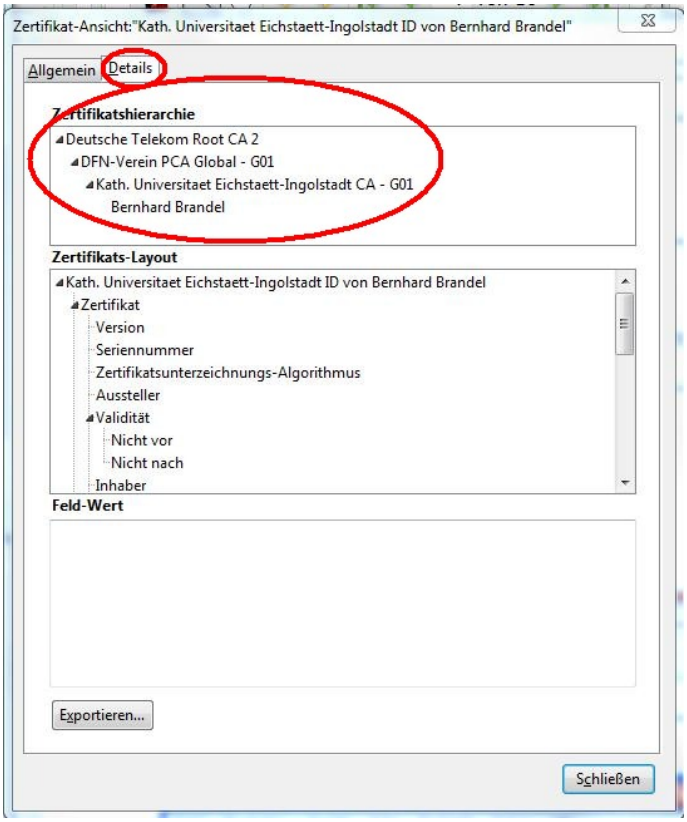
Zum Verfassen einer signierten E-Mail klicken Sie wie gewohnt auf das „Verfassen“-Symbol. Das Fenster für die neue E-Mail öffnet sich. Schreiben Sie nun wie gewohnt Ihre Mail an die gewünschten Adressaten.
Danach klicken Sie auf den Reiter „S/MIME“ und kreuzen dort „Nachricht unterschreiben“ an. Zum Schluss klicken Sie auf „Senden“ – Fertig – die unterschriebene E-Mail ist verschickt.



Fertig – die unterschriebene E-Mail ist verschickt.

Der Empfänger erkennt durch ein grafisches Symbol in Form eines gesiegelten Umschlags die Gültigkeit der Signatur in der empfangenen E-Mail. Wenn er auf den Umschlag klickt, erhält er genauere Informationen über den Unterzeichner, dessen E-Mail-Adresse usw. Nach Klick auf „Unterschriftszertifikat ansehen“ erhält er im Reiter „Allgemein“ detaillierte Informationen über das Zertifikat und im Reiter „Details“ Informationen über die Zertifikatskette.





Wenn der Inhalt der E-Mail auf dem Übertragungsweg verändert wurde oder dem Zertifikat des Absenders nicht vertraut wird, wechselt das Symbol zu einem gebrochenen Siegel. Somit kann der Empfänger immer erkennen, ob Inhalt und Absender der empfangenen E-Mails authentisch sind.

Wie funktioniert die Verschlüsselung von E-Mails

Ver- und Entschlüsselung von E-Mails funktionieren ähnlich intuitiv wie die elektronische Signatur. Zum Verschlüsseln einer Nachricht wird das Zertifikat des Empfängers benötigt, das dessen öffentlichen Schlüssel enthält. Damit verschlüsselt Thunderbird die Nachricht an den Empfänger. Nach Erhalt kann der Adressat die erhaltene verschlüsselte E-Mail mit seinem eigenen privaten Schlüssel öffnen.

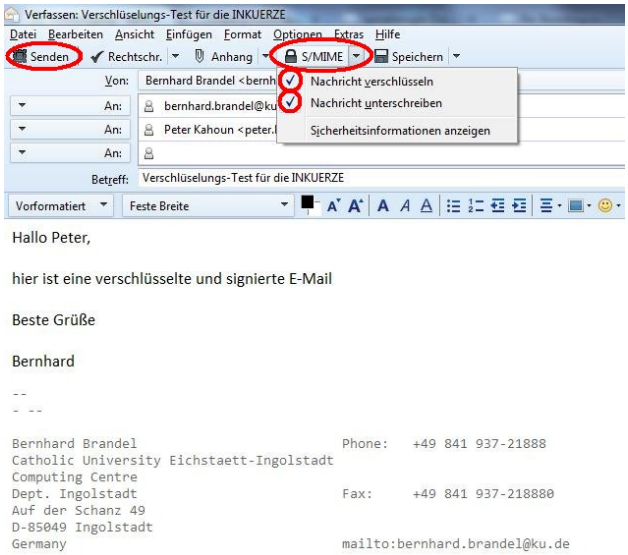
Wie gelange ich an die Zertifikate meiner Kommunikationspartner? Glücklicherweise nimmt Ihnen Mozilla Thunderbird diese Arbeit weitgehend ab. Thunderbird und ähnliche Mail-Programme sammeln gültige Nutzerzertifikate aus jeder E-Mail automatisch ein.

Daher muss Ihnen ein neuer Kommunikationspartner nur eine digital unterschriebene E-Mail zusenden, dann speichert Thunderbird sein Zertifikat automatisch im Zertifikatsspeicher ab und Sie können ab sofort mit Ihrem Mail-Partner verschlüsselt kommunizieren.

Verschlüsselung von E-Mails in Thunderbird

Zum Schreiben einer verschlüsselten E-Mail gehen Sie genauso vor wie im Abschnitt „Signieren von E-Mails in Thunderbird“.

Sie müssen lediglich vor dem Absenden der Mail zusätzlich zu „Nachricht unterschreiben“ auch noch „Nachricht verschlüsseln“ ankreuzen:



Dem Empfänger wird die E-Mail automatisch entschlüsselt angezeigt. Das geschlossene Schloss-Symbol zeigt ihm an, dass die E-Mail an ihn verschlüsselt war. Durch Klick auf das Schloss erhält er nähere Informationen. Da die E-Mail zusätzlich signiert war (Symbol: gesiegelter Brief), kann er wie im Beispiel zuvor auch Unterschrift und Zertifikatskette des Absenders prüfen.

Schlusswort

Wir hoffen, Ihnen durch diesen Artikel das Verschlüsseln und Signieren von E-Mails schmackhaft gemacht zu haben. Wir würden uns freuen, wenn Sie unsere Einladung annehmen und den Zertifikatsservice von DFN und KU nutzen würden. Bei Interesse, weitergehenden Fragen oder Schulungsterminen – auch generell zum Thema IT-Sicherheit – wenden Sie sich gerne an unsere Sekretariate und an den Autor dieses Artikels.

Ganz besonders möchten wir uns beim DFN-Verein und dem DFN-CERT bedanken, dass sie den Service DFN-PKI ins Leben gerufen und in den letzten Jahren weiter perfektioniert haben. Durch den immer kompetenten und freundlichen Support Ihrer Teams ist die praktische Nutzung von E-Mail-Verschlüsselung und Signierung wirklich kein Hexenwerk mehr!

Literatur:

[1] http://de.wikipedia.org/wiki/X.509
[2] http://www1.ku-eichstaett.de/urz/inkuerze/1_07/pki.html
[3] http://www1.ku-eichstaett.de/urz/inkuerze/2_06/sslmail.html
[4] http://www1.ku-eichstaett.de/urz/inkuerze/2_02/ssl.html
[5] https://www.pki.dfn.de/
[6] https://www.pki.dfn.de/ueberblick-dfn-pki/
[7] https://pki.pca.dfn.de/kuei-ca/cgi-bin/pub/pki?cmd=basic_csr;id=1;menu_item=1&RA_ID=0
[8] https://www.pki.dfn.de/fileadmin/PKI/Anleitung_DFN-Test-PKI.pdf
[9] https://www.pki.dfn.de/faqpki/faqpki-mozilla/#c15186
[10] http://www1.ku-eichstaett.de/urz/inkuerze/1_05/mailverschluesselung.html
[11] http://www.thunderbird-mail.de/wiki/Mailverschlüsselung_mit_S/MIME#Vertrauen_einstellen

Ansprechpartner im URZ:	*Zimmer:*	*Telefon:*	*Mail:*
Bernhard Brandel	IN: HB-204	-21888	bernhard.brandel
Tomasz Partyka	EI: eO-104	-21668	tomasz.partyka