



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 <u>Mozilla Firefox</u>, und zwar <u>unbedingt auf Ihrem eigenen PC</u>. 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).



A https://pki.pca.dfn.de/k	uei-ca/cgi-bin/pub/pki							∀ C ₹	🕽 🕆 dfn-pki ssl_erro	r_handshake_failu	ire_alert	ρ.	合	☆
🎹 Erste Schritte 😹 tagesschau.	.de - Die N 📋 egroupware.ku.de (An 🗍 KUEI)	CA-Antragsschni 📙 WSUS ur	nd Secunia TN Sichern von WSUS	S-Dat 门 VMware	vSphere 4 💔 T	YPO3 Login:	:: KU Eichs 📒 N	SDN Downloads	für K Kaspersky Lab D)E Vire 🕥 http	os://141.78.159.250:	LV Lib	iVox 🗊	Pressein
		Zertifikate CA-	-Zertifikate Gesperrt	e Zertifikate	Policies	Hilfe	Beenden		Deutsch Forschu	N ngsnetz				
		Nutzerzertifikat	Serverzertifikat	Zertifika	at sperren	Ze	ertifikat such	en						
										Nutzerze	rtifikat beantra	agen -	Bestä	tigen
	Bitte überprüfen Sie die Daten.													
			Zert E-Ma Nam Abte Weit Verö	ifikatdaten ail e ilung tere Angabe ffentlichen	bernhard Bernhard Universit n Ja	l.brande I Brande aetsrech	el@ku.de el henzentrum							
				And	dem Bestä	tigen								
													Impre	ssum

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!

 $\triangleright\,$ Als nächstes müssen Sie den Zertifikatantrag wie hier beschrieben



ausdrucken

	Zertifikatantra	ag für ein Nutzerzertifikat
	- an: Kath. Un	iversität Eichstätt-Ingolstadt -
Antragsnummer	64032	
Antragssteller		
Vorname Nachname	Bernhard Brandel	
E-Mail	bernhard.brandel	@ku.de
Abteilung	Universitaetsrech	enzentrum
Zertifikatdaten		
Eindeutiger Name	emailAddress=be OU=Universitaets	rnhard.brandel@ku.de, CN=Bernhard Brande rechenzentrum, O=Kath. Universitaet Eichstaett-Ingolstadt, C=DI
Public Key Fingerprint	7F:A0:B1:F9:7F:D	04:31:2D:CE:13:F6:3F:1B:BE:06:A5:96:4A:B2:D5
Veröffentlichen	Ja	
Zertifikatprofil	User	
Erklärung des Antragsste	llers	
 https://into.pca.dfn.de/doc/lt loba heißt insbesondere: lob darf den privaten S ist nicht erlaubt. Jedes Gerät, auf dem z. B. frei von Schadso lob in unter den folge Das Zertifikat en - Das Zertifikat Der private Schlü anderweitig komp 	nfo_Zertifikatinhaber.p Schlüssel zu dem Zert ich den privaten Sch tiware wie Viren sein nden Bedingungen w hält Angaben, die nic ssel oder die dazugel oromittiert bzw. missb	Der DF/F-FK und verpindne micht, der Heigeungen (der di di veröffentlichnaber einzuhalt fikkat nicht anderen Personen zugänglich machen. Eine Weiterg lüssel speichere bzw. einsetze, muss angemessen geschützt, a und regelmäßig mit Sicherheits-Patches versehen werden. arpflichtet, das Zertifikat speren zu lassen: in mehr güttig sind, beispelsweise nach einer Namensänderung öröge Passphrase/PIN wurde verloren, gestohlen, offen gelegt o raucht.
 Indo pca.dfn.de/docli Das heißt insbesondere: Ich darf den privaten s ist nicht erfaubt. Jedes Gerät, auf dem z. B. frei von Schadso Ich bin unter den folg Das Zertifikat eni	nfo.Zertifikatinhaber.p Schlüssel zu dem Zert ich den privaten Sch tware wie Viren sein inden Bedingungen v hält Angaber, die nic ssel oder die dazugel oromittiert bzw. missb romittiert bzw. missb romittiert daz vert arbeitung und Nutzur an den DFN-Verein I	Der DF/F-FK und verpindne mindt, ode Heigelungen oder au diveröffentlichen "Informationen für Zertifikatinnsber" einzuhalt iftikat nicht anderen Personen zugänglich machen. Eine Weiterg lüssel speichere bzw. einsetze, muss angemessen geschützt, nd regelmäßig mit Sicherheits-Patches versehen werden. arpflichtet, das Zertifikat sperenz vul assen: ht mehr gültig sind, beispelsweise nach einer Namensänderung nörige Passphrase/PIN wurde verloren, gestohlen, offen gelegt o raucht. gid er erhobenen Daten zum Zweck der Zertifikaterstellung ein bermittelt und dort beschränkt auf diesen Zweck verarbeitet i
https://inc.pca.dlm.de/dof/ 20.sh efiblt insbesondere: is thin chief relatab. is thin chief relatab. 2. B. frei loven Schadso i chi bin unter den folge — Das Zurfikate en — Der private Schild and derweitig kom — I chi bin nicht meh Ich erktitter mich mit der Ves genutzt werden.	No.Zertifikatinhaber.p ichlüssel zu dem Zert ich den privaten Sch tware wie Viren sein nden Bedingungen v hält Angaben, die nic ssel oder die dazugel vomittiert bzw. missb sel berechtigt, das Zerti arbeitung und Nutzur an den DFN-Verein i	Der Derkerk und verpilichte mitch, die reigelungen oder die die vollfentlichten Informationen für Zertifikalinhaber einzuhla fikkat nicht anderen Personen zugänglich machen. Eine Weiterg üssel speichere bzw. eineste, muss angemessen geschützt, auf negienfälig mit Scherheits Paches versehen werden. zerflichtet, das Zertifikat speren zu lassen: tim der gölt spälig ein Scherheitse isn ach einer Namensänderung vörige Passphrase/PIN wurde verloren, gestohlen, offen gelegt or racht. Sikat zu nutzen. gi der erhobenen Daten zum Zweck der Zertifikaterstellung ein übermittelt und dort beschränkt auf diesen Zweck verarbeitet i
https://inc.pca.dln.de/doc/U Das heißt insbesondere: • Ich darf den privaten 5 ist nicht ertaubt. • Jedes Gerät, auf dem 2. B. Fri dvon Schadso • Ich bin unter den folge – Das zurfikate en – Der private Schlü anderweitig kom – Ich bin nicht meh Ich erklitze mich mit der Vas tatanden. Die Daten dürfen genutzt werden.	fo_Zertifikatinhaber,p ichlüssel zu dem Zert ich den privaten Sch Warae wie Viren sein nden Bedingungen v hält Angaber, die nic ssel oder die dazuget roberechtigt, das Zerti arbeitung und Nutzur an den DFN-Verein i	Der Derkerkt und verpilichte mitch, die regelungen oder die diveröffentlichten Informationen für Zertifikalinhaber einzuhalt filikat nicht anderen Personen zugänglich machen. Eine Weiterg lüssel speichere bzw. einsetze, muss angemessen geschützt, a und regelunäßig mit Sicherheits-Patches versehen werden. erpflichtet, das Zertifikat generen zu lassen: hr mehr gültig sind, beispielsweise nach einer Namensänderung nörige Passpirase/PIN wurde verloren, gestohlen, offen gelegt c raucht. sig der erhobenen Daten zum Zweck der Zertifikaterstellung ein übermittelt und dort beschränkt auf diesen Zweck verarbeitet i
https://inco.pca.dfn.de/doc/U Das heißt insbesondere: • Ich darf den privaten 5 ist nicht ertaubt. • Jedes Geräft, auf dem 2. B. Frei von Schadso • Ich bin unter den folge — Das Zertifikat en — Der private Schli anderweißt komy – Ich bin nicht meh- Ich erklare mich mit der Ver- standen. Die Daten dürfen gerutzt werden. (Ort, Datum)	fo.Zertlifkatinhaber.p ichlüssel zu dem Zert ich den privaten Sch ware wie Viren sein nden Bedingungen v halt Angaban. die nic seel oder die dazugel oromitiert bzw. mitseb herechtigt, das Zert arbeitung und Nutzur an den DEN-Verein I	Jer Driverk und verplindne mindt, die regelungen foer un di veröffentlichten Informationen för Zertifikatinsber einzuhalt fitikat nicht anderen Personen zugänglich machen. Eine Weiterg lüssel speichere bzw. einsetze, muss angemessen geschützt, a und regelimäßig mit Sicherheits-Patches versehen werden. applichtet, das Zertifikat sperenz u lassen: ht mehr gültig sind, beispielsweise nach einer Namensänderung nörige Passphrase/PIN wurde verloren, gestohlen, often gelegt c raucht. fikat zu nutzen. ng der erhobenen Daten zum Zweck der Zertifikaterstellung ein ibermittelt und dort beschränkt auf diesen Zweck verarbeitet n (Unterschrift)
https://inc.pca.dfn.de/do/U Das heißt insbesondere: • Ich darf den privaten 5 ist nicht ertaubt. • Jedes Gerät, auf dem 2. B. rei von Schadso • Ich bin unter den folge – Das zurfikate em – Der private Schild anderweitig kom – Ich bin nicht meh Ich erklitter mich mit der Vas istanden. Die Daten dürfen genutzt werden. (Ort, Datum) Wird vom Teilnehmerserv	In the second se	User Derkerk und verplachte mitch, der regelungen for un diveröffentlichen Informationen för Zertifikatinhaber einzuhalt filkat nicht anderen Personen zugänglich machen. Eine Weiterg lüssel speichere bzw. einsetze, muss angemessen geschützt, a und regelunäßig mit Sicherheits-Patches versehen werden. and regelunäßig mit Sicherheits-Patches versehen werden. sprifichtet, das Zertifikat sperener zu lassen: ihr mehr gültig sind, beispielsweise nach einer Namensänderung nörige Passphrase/PIN wurde verloren, gestohlen, offen gelegt c raucht. sig der erhobenen Daten zum Zweck der Zertifikaterstellung ein übermittelt und dort beschränkt auf diesen Zweck verarbeitet t (Unterschrift)
https://inc.pca.dln.de/do/U abs.httl: https://ansenderei ist nicht erfaubt. • Jedes Gerät, auf dem 2. B. frei von Schadso • Ich bin unter den folge — Das Zertifikat en — Der private Schlid anderweitig kom — Ich bin nicht meh Ich erklätre mich mit der Ver standen. Die Daten dürfen gerutzt werden. (Ort, Datum) Wird vom Teilnehmerser- Identitätsprüfung:	fo_Zertlifkatinhaber.p ichlüssel zu dem Zert ich den privaten Sch Warar wie Viren sein haft Angaben. die nic ssel oder die azugel romitiert bzw. missb r berechtigt, das Zertl arbeitung und Nutzur an den DFN-Verein I ice ausgefüllt	Der Derkerk und verpiliertie micht die Pregeningen foer un die vordientlichten Informationen für Zertifikatinhaber einzuhalt fiktat nicht anderen Personen zugänglich machen. Eine Weiterg lüssel speichere bzw. einsetze, muss angemessen geschützt, a und regelimäßig mit Sicherheits-Patches versehen werden. appflichtet, das Zertifikat sperenz ul assen: ht mehr gültig sind, beispielsweise nach einer Namensänderung nörige Passphrase/PIN wurde verloren, gestohlen, often gelegt of raucht. fiktat zu nutzen. ag der erhobenen Daten zum Zweck der Zertifikaterstellung ein ibermittelt und dort beschränkt auf diesen Zweck verarbeitet tr (Unterschrift) Antragsprüfung:
https://inc.pca.dln.de/do/U bas.heißt insbesondere: • Ich darf den privaten 5 ist nicht ertaubt. • Jedes Gerät, auf dem 2. B. Fri dvon Schadso • Ich bin unter den folge – Das Zurfikate en – Der private Schild anderweißt kom – Ich bin nicht mer Ich erklare mich mit den dürfen gerutzt werden. (Ort, Datum) Wird vom Tellnehmersern Identitätsprüfung: – Name gerpfit	Io.Zertlifikatinhaber.p ichlüssel zu dem Zert ich den privaten Sch Ware wie Vien sein nden Bedingungen v ware wie Vien sein abl Angaben, die nic seel oder die azugel romittier tzw. missis r berechtigt, das Zerti arbeitung und Nutzur an den DEN-Verein in vice ausgefüllt	ter DF-FAC und verplache mich, der Pegeungen (der und frikat nicht anderen Personen zugänglich machen. Eine Weiterg lüssel speichere bzw. einsetze, muss angemessen geschützt, a und regelmäßig mit Sicherheits-Patches verschen werden. spflichtet, das Zertlikat sperenz u/ lassen: ht mehr gültig sind, beispielsweise nach einer Namensänderung öräge Passphrase/PIN wurde verloren, gestohlen, offen gelegt or araucht. g der erhobenen Daten zum Zweck der Zertlifkatserstellung ein ibermittelt und dort beschränkt auf diesen Zweck verarbeitet r (Unterschrift) Antragsprüfung: Berechtigung des Antragsstellers zum Erhalt des
titps://inc.pca.dfn.de/dof/ tittps://inc.pca.dfn.de/dof/ Josh krift insbesondere: • Ich darf den privaten 5 • Ich darf den privaten 5 • Ich bin unter den folge — Das Zurfikate en — Der private Schild anderweitig komp — Ich bin nicht meh Ich erkläre mich mit der Va- tranden. Die Dalen dürfen genutzt werden. Ort, Datum) Wird vom Teilnehmerseren — Inderschitt geprüft — Name geprüft	fo.Zertlifkatinhaber.p ichlüssel zu dem Zert ich den privaten Sch Ware wie Viren sein nden Bedingungen v ware wie Viren sein alt Angaben, die nic ssel oder die dazugel r berechtigt, das Zerti arbeitung und Nutzur an den DFN-Verein i ice ausgefüllt	Der Der kerk und verpilichte mitch, die reigenungen foer un der vollentlichten Informationen für Zertifikalinhaber einzuhl fikat nicht anderen Personen zugänglich machen. Eine Weiterg lüssel speichere bzw. einsetze, muss angemessen geschützt, e und regelmäßig mit Sicherheits-Patches versehen werden, erpflichtet, das Zertifikat sperern zu lassen: in mehr gültig sind, beispeisweise nach einer Namensänderung nörige Passphrase/PN wurde verloren, gestohlen, offen geligt e aucht. gid er enhobenen Daten zum Zweck der Zertifikaterstellung ein ibermittelt und dort beschränkt auf diesen Zweck verarbeitet n (Unterschrift) Berechtigung des Antragsstellers zum Erhalt des beantragten Zertifikats gepröft
https://inc.pca.dln.de/dof/l bas.heißt insbesondere: • Ich darf den privaten 5 ist nicht ertaubt. • Jedes Gerät, auf dem r.d. Brei von Schadso • Ich bin unter den folge – Das Zurtlikat en – Der private Schill anderweißt kom – Ich bin nicht meh Ich erklate mich mit der Vet standen. Die Daten dürfen gerutzt verden. //ort, Datum) Wird vom Teilnehmerserv //ort, Datum //ort, Datum //ort vom Teilnehmerserv //ort unne gerüft Unnerschrift gerüft Bild geprüft Bild geprüft	fo.Zertlifkatinhaber.p chlüssel zu dem Zert ich den privaten Sch Ware wie Vien sein nden Bedingungen v Ware wie Vien sein als Angaber., die nic seel oder die dazugel romtitier bzw. missb r berechtigt, das Zertl arbeitung und Nutzur an den DEN-Verein I vien ausgefüllt pier mit Lichtbild:	Der Der Verk fund Verpindne mindt, der Pregelungen foer un der der dieflichten Informationen för Zertifikatinsber einzuhalt fikat nicht anderen Personen zugänglich machen. Eine Weiterg lössel speichere bzw. einsetze, muss angemessen geschützt, e nor regelimäßig mit Sicherheits-Patches versehen werden. repflichtet, das Zertifikat sperenz ul assen: fikat zu nutzen. gder erhobenen Daten zum Zweck der Zertifikatserstellung ein bemittigt und dort beschränkt auf diesen Zweck verarbeitet n (Unterschrift) Antragsprüfung: Berechtigung des Antragsstellers zum Erhalt des beantraginer Zertifikat sperioft Endeutiger Name (so.) noch nicht an andere Person vergeben
titps://inc.pca.dfn.de/dof/ tittps://inc.pca.dfn.de/dof/ 208.hight insbesondere: i ch darf den privaten 5 ist nicht erfaubt. . de/des Gerät, auf dem . D. Er di von Schadso i ch bin unter den folge - Das Zuffikat en - Der private Schlid anderweitig kom - Leh bin nicht meh ich erkützer mich mit der Vey i chaten dürfen genutzt werden. //t. Datum) Wird vom Teilnehmerseren //t. Datum) Wird vom Teilnehmerseren // Inderschrift gepröft Bild gepröft Amtliches Ausweisptligkeit ge)	fo.Zertlifikatinhaber.p ichlüssel zu dem Zert ich den privaten Sch Ware wie Viren sein nden Bedingungen v ware wie Viren sein inden Bedingungen v sesel oder de azuget r berechtigt, das Zerti arbeitung und Nutzur an den DFN-Verein i ice ausgefüllt pier mit Lichtbild: der Ausweisnummer) prüft	Berechtigung des Antragsstellers zum Erhalt des bearterspfrug: [Unterschrift] [Unterschrift] [Endudger Antragsstellers zum Erhalt des bearterspfen Zertifikatigsereit
https://inc.pca.dln.de/dof/U https://inc.pca.dln.de/dof/U list inciht ertaubt. • Jedes Gerät, auf dem z. B. Friel von Schadso • Ich bin unter den folge — Das Zertifikat en – Der private Schild anderweitig kom – Ich bin nicht meh Ich erklare mich mit der Wei standen. Die Daten dürfen gerutzt werden. (Ort, Datum) Wird vom Teilnehmerseru Minders Ausweisptliche Bild geprächt — Name gepröft — Unterschrift gepröft — Bild geprächt geprächt — Bild geprächt geschatter — Kanweisptlichgeit ge Oder: — Ich beritikt bereits fröht	Io.Zertifikatinhaber.p ichlüssel zu dem Zert ich den privaten Sch Ware wie Vien sein inden Bedingungen v ware wie Vien sein inden Bedingungen v wormtiter bzw. missb r berechtigt, das Zerti arbeitung und Nutzur an den DEN-Verein i ice ausgefüllt pier mit Lichtbild: der Ausweisnummer) rotit	Ber Childer Verführt in Bindt, der Pregenungen führ und Verpfleintlichnaber einzuhl fürkat nicht anderen Personen zugänglich machen. Eine Weiterg Bissel speichere bzw. einsetze, muss angemessen geschützt, e ind regelmäßig mit Sicherheits-Patches versehen werden. repflichtet, das Zertifikat speriort t mehr gültig sind, beispielsweise nach einer Namensänderung vörige Passphrase/PIN wurde verloren, gestohlen, often geligt c raucht. fikat zu nutzen. gder erhobenen Daten zum Zweck der Zertifikatserstellung ein beerntigung des Antragsstellers zum Erhalt des beentragen Zertifikats geprüft Endeuliger Name (s.o.) noch nicht an andere Person vergeben Name des TS-Mitarbeiters: Zugehörige TS-Stelle:

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:



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",

🕼 https://pil.pc.dfn.det.tueri-cal-cpi-bin/pub/pillcmd-getStaticPagenamesindecclu-2 🖤 C 🍳 🕼 - dfn-pill re-operator 🔎 🖡 🇌	습
m Ente Schritte 📓 tageschaude - Die N. 🗌 egroupwarekude (Jan. 🗌 KUEI CA-Antragoschn 📴 WSUS und Securia TN Sichern von WSUS-Dat 🗋 Where röphere 4 🐺 TPPOI Logie KU Eichs 🚏 MSDN Downloadsfar 🧍 Kapersky Lab DE [Vine 🖗 Mtpp://dl.D.19.2929 [V Libriva 🛄 P	esseinfe
Zertflikate CA-Zertflikate Gesperrte Zertflikate Polices Hilfe Beenden Uurzebzertflikat OFN-PCA-Zertflikat VUEI-CA-Zertflikat Dertflikate Dertfli	
Impre	

danach im zweiten Link auf "Zertifikat importieren"

🔶 🔒 https://pki.pca.dfn.de/ku	ei-ca/cgi-bin/pub/pki?cmd=getcert&key=6656124	295772472&type=CERTIFICATE				v x Q	😵 - dfn-pki ra-operator		۶ 🖡	A	☆ 0
🎹 Erste Schritte 🔊 tagesschau.d	de - Die N 🗍 egroupware.ku.de (An 🗍 KUE	CA-Antragsschni 📙 WSUS und	Secunia TN Sichern von WSUS-Da	t 📋 VMware vSphere 4 👪 TYPO:	3 Login: KU Eichs 👫 MSDN E	Downloads für	K Kaspersky Lab DE Vire	https://141.78.159.250:	LV LibriVo	ax 🇊 Pro	resseinfo
							DFN_				
							Deutsches Forschungsnetz				
		Zertifikate CA-Z	ertifikate Gesperrte :	Zertifikate Policies Hil	lfe Beenden						
		Nutzerzertifikat	Serverzertifikat	Zertifikat sperren	Zertifikat suchen						
								Laden des beant	ragten 2	Zertifik	kats
	Benutzen Sie den Button, um I	hr Zertifikat in Ihren Br	owser zu importieren.								
	Bitte beachten Sie, dass eini	ige Browser einen erf	folgreichen Import n	icht gesondert melden	ı.						
	Wenn Sie bei der Antragsstellur haben.	ng bestimmt haben, das	ss Ihr Zertifikat nicht v	eröffentlicht werden soll,	, so werden Sie nach	der PIN g	efragt, die Sie in Ihre	en Zertifikatantrag	eingege	ben	
				4. Zertifikat importieren	\triangleright						
			Warnung Ihr persönliches Zerti aufheben.	fikat wurde installiert. Sie sollten eine :	Sicherungskopie dieses Zertifikat	ts			Ir	npress	um

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 \rightarrow Einstellungen \rightarrow Erweitert \rightarrow Zertifikate anzeigen \rightarrow 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".

Aa	Vadaraa		0 (Ihre Zertifikate Personen Sen	ver Zertifizierungssteller	Andere			
mein Ansicht	venassen	Chat Sichern	eit Annange Er	weitert	Sie haben Zertifikate dieser (Organisationen, die Sie ic	lentifizieren:			
nn eine Website nach	nt Netzwerk & Speic h dem persönlichen S ns wählen 💿 J <u>e</u> de	Sicherheitszertifikat verl s Mal fragen	ingt:		Zertifikatsname #Kath. Universitaet Eichsta Bernhard Brandel	Kryptographie-Modul Software-Sicherheitsm	Ser odul 13:	iennummer 50:D6:DD:19:5C:77	Läuft ab am 06.02.2015	
Co Zu importierer	rung <u>K</u> ryptograp	hie-Module			Ansehen Sichern	<u>Alle sichern</u>	mportieren	Löschen		0
	Computer Sys	item (C:) 🕨 Sonstiges	 Zertifikatssicherungen 				• •	Zertifikatssicheru	ingen durchs 🔎	•
Organisieren V Der	Computer > Sys Neuer Ordner nVPN rramData	tem (C:) ► Sonstiges	Zertifikatssicherungen Name Nicht angegeben	(3)	Änderungsdatum	Тур	✓ ✓ Größe	Zertifikatssicheru ∄≣ ∄≣	ingen durchs D	•
Organisieren v Organisieren v Oper Prog Prog	Computer Sys Neuer Ordner NVPN IramData Iramme Iramme (x86)	tem (C:) Sonstiges	 Zertifikatssicherungen Name Nicht angegeben ra+user.p12 	(3)	Änderungsdatum 28.05.2014 22:36	Typ Privater Informati	+ +9 Größe 15 KB	.] Zertifikatssicheru ≋≣	ingen durchs P	• • • • •
Organisieren • Organisieren • Prog Prog Prog Recco	Computer Sys Neuer Ordner nVPN ramData ramme (x86) rvery nia	tem (C:) > Sonstiges	 Zertifikatssicherungen Name. Nicht angegeben ra+user,p12 ra-user,p12 zertifikat,p12 	(3)	Änderungsdatum 28.05.2014 22:36 27.05.2014 19:31 30.05.2014 21:36	Typ Privater Informati Privater Informati Privater Informati	 ✓ 49 Größe 15 KB 8 KB 8 KB 	Zertifikatssicheru	ingen durchs P	• • • • • •
Organisieren * Organisieren * Prog Prog Prog Reco Secu Secu Sons	Computer Sys Computer Computer Sys Computer Computer Computer Sys Computer C	tem (C:) > Sonstiges	 Zertifikatssicherungen Name Nicht angegeben re-user,p12 zertifikat,p12 	(3) Typ: Priva Große: 7,1 Änderung	Änderungsdatum 28.05.2014 22:36 22.05.2014 19:31 30.05.2014 21:36 ter Informationsautausch 4.88 datum: 30.05.2014 21:36	Typ Privater Informati Privater Informati Privater Informati	 ✓ ✓ Größe 15 KB 8 KB 8 KB 8 KB 	3. Zertifikatssicheru 8	ingen durchs 👂	• • • • • • • • • • • •
Organisieren v Organisieren v Organisieren v Organisieren v Prog Prog Prog Reco Secu Secu Sons 200 Da Fre Fre Fre	 Computer > Sys Neuer Ordner NVPN ramme (x86) vvery mia mitiges tensicherheit tdinand nesspläne 	tem (C.) + Sonstiges	 Zertifikatssicherungen Name Nicht angegeben av user,pl2 zertifikat.p12 	(3) Typ: Privat Große: 7,1 Anderung	Anderungsdatum 28.05.2014 22:36 27.05.2014 19:31 30.05.2014 21:36 ter Informationsaustausch 4 K8 sdatum: 30.05.2014 21:36	Typ Private Informati Private Informati	 ▼ 4g Größe 15 KB 8 KB 8 KB 8 KB 	I Zertifikatssicheru	ingen durchs P	· · · · · · · · · · · · · · · · · · ·

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



	Einstellungen	Constanting Processing	an Code	achage inc	Lafet.ov 1	Property.	deriver.	×
			页		60		0	iğ:
	Allgemein	Tabs	Inhalt A	nwendungen	Datenschutz	Sicherheit	Sync	Erweitert
	Allgemein D	atenübermi	ttlung Netzw	verk Update	Zertifikate			
	Wenn eine	Website na atisch eins	ch dem persö <u>w</u> ählen 💿	önlichen Sicher Jedes Mal frag	heitszertifikat ve en	rlangt:		
	Zertifikat	e anzeigen	Validierun	g <u>K</u> ryptog	raphie-Module			
Warnung								
1 Ihre Sicherheitszertifikate und privaten Schlüssel wurden erfolgreich wiederhergestellt.								
ОК					ОК	Abbreche	n 🗌	<u>H</u> ilfe

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 \rightarrow 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.

	Konten-Einstellungen
rnhard.brandel@ku.de	S/MIME-Sicherheit
Server-Einstellungen Kopien & Ordner	Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben.
Junk-Filter	Digitale Unterschrift
Synchronisation & Speicherplatz	Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiben: 1.
Empfangsbestätigungen (MDN)	Kath. Universitaet Eichstaett-Ingolstadt ID von Bernhard Brandel Auswählen
5/MIME-Sicherheit kale Ordner	Nachrichten digital unterschreiben (als Standard)
Junk-Filter	Verschlüsselung
Speicherplatz stausgang-Sonvor (SMTP)	Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln: 3.
stausgang-server (sivirr)	Kath. Universitaet Eichstaett-Ingolstadt ID von Bernhard Brandel Aus <u>w</u> ählen
	6 Standard-Verschlüsselungseinstellung beim Senden von Nachrichten:
	Nie (keine Verschlüsselung verwenden)
	Notwendig (Senden nur möglich, wenn alle Empfänger ein Zertifikat besitzen)
	Zertifikate
	Zertifikate vonuelten
Konten-Aktionen	• <u>Zertinkate verwaiten</u> Nyptographie- <u>miodule verwaiten</u> 7.
	OK Abbreche
2. und 4.	Zertifikat wählen
Zertifikat: Kath. Universitaet	: Eichstaett-Ingolstadt ID von Bernhard Brandel [17:A5:B5:B4:3A:F9:38]
	kats:
Details des gewählten Zertifi	
Details des gewählten Zertifik	d Brandal OII-Universitaetsrechenzentrum O-Kath Universitaet Eichstaett-
Details des gewählten Zertifik Ausgestellt auf: CN=Bernhar Ingelstadt C=DF	d Brandel,OU=Universitaetsrechenzentrum,O=Kath. Universitaet Eichstaett-
Details des gewählten Zertifik Ausgestellt auf: CN=Bernhar Ingolstadt,C=DE Seriennummer: 17:A5:B5:B4	d Brandel,OU=Universitaetsrechenzentrum,O=Kath. Universitaet Eichstaett-
Details des gewählten Zertifik Ausgestellt auf: CN=Bernhar Ingolstadt,C=DE Seriennummer: 17:A5:B5:B4 Gültig von 28.05.2014 21:2	rd Brandel,OU=Universitaetsrechenzentrum,O=Kath. Universitaet Eichstaett- 4:3A:F9:38 25:24 an 27.05.2017 21:25:24
Details des gewählten Zertifik Ausgestellt auf: CN=Bernhar Ingolstadt,C=DE Seriennummer: 17:A5:B5:B4 Gültig von 28.05.2014 21:2 Verwendung eines Zertifika	rd Brandel,OU=Universitaetsrechenzentrum,O=Kath. Universitaet Eichstaett- 4:3A:F9:38 25:24 an 27.05.2017 21:25:24 Itsschlüssels: unterzeichne,Non-repudiation,Schlüssel-Verschlüsselung
Details des gewählten Zertifik Ausgestellt auf: CN=Bernhar Ingolstadt,C=DE Seriennummer: 17:A5:B5:B4 Gültig von 28.05.2014 21:2 Verwendung eines Zertifika E-Mail: bernhard.brandel@	rd Brandel,OU=Universitaetsrechenzentrum,O=Kath. Universitaet Eichstaett- 4:3A:F9:38 25:24 an 27.05.2017 21:25:24 Itsschlüssels: unterzeichne,Non-repudiation,Schlüssel-Verschlüsselung ku.de
Details des gewählten Zertifik Ausgestellt auf: CN=Bernhar Ingolstadt,C=DE Seriennummer: 17:A5:B5:B4 Gültig von 28.05.2014 21:2 Verwendung eines Zertifika E-Mail: bernhard.brandel@ Ausgestellt von: E=pki@ku-4	rd Brandel,OU=Universitaetsrechenzentrum,O=Kath. Universitaet Eichstaett- 4:3A:F9:38 25:24 an 27.05.2017 21:25:24 Itsschlüssels: unterzeichne,Non-repudiation,Schlüssel-Verschlüsselung ku.de eichstaett.de,CN=Kath. Universitaet Eichstaett-Ingolstadt CA -
Details des gewählten Zertifik Ausgestellt auf: CN=Bernhar Ingolstadt,C=DE Seriennummer: 17:A5:B5:B4 Gültig von 28.05.2014 21:2 Verwendung eines Zertifika E-Mail: bernhard.brandel@ Ausgestellt von: E=pki@ku-4 G01,OU=Universitaetsrecher	d Brandel,OU=Universitaetsrechenzentrum,O=Kath. Universitaet Eichstaett- 4:3A:F9:38 25:24 an 27.05.2017 21:25:24 itsschlüssels: unterzeichne,Non-repudiation,Schlüssel-Verschlüsselung ku.de eichstaett.de,CN=Kath. Universitaet Eichstaett-Ingolstadt CA - izentrum,O=Kath. Universitaet Eichstaett-Ingolstadt C=DE

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.

Constraining - Lennand Kannangen - Leal Test ingeinet - Mail - Pen. × Constraining - Lennand Kannagel - Mail - Kanna		
Date genteeten genket Negignion Bjechekt Egten Hilfe Advion Verfasen Chat Advestue Hilfe Anvion Verfasen Chat Advestue Methode Schlagwohrer Chat Schlagwohrer Chat Schlagwohrer Chat Schlagwohrer Chat Advestue Methode Schlagwohrer Chat Advestue Methode Schlagwohrer Chat Schlagwohrer Chat Advestue Methode Schlagwohrer Chat Advestue Methode Schlagwohrer Chat Schlagwohrer	🖄 Posteingang - bernhard.bran 🛛 🖂 Test- signierte E-Mail - Po 🗙 🗢	
Abdurden Verfassen Chat Adverstouch Schleigkouter * Schleigkouter	Datei Bearbeiten Ansicht Navigation Nachricht Extras Hilfe	
Abufun Verfassen Chal Adressbuch Schlagwörer Versenson Schlagwörer Versenson Von Mir - demhard brandel Bluudes Antworten Weiterleien Antwich versenson Antwich versenson Antwich versenson Antwich versenson Lieber Peter, diese Mall ist von nin unterschrieben. Viele Gruße Bernhard Bernhard Bernhard Phone : +49 841 937-21888 Catholit Universitet Eichstaett-Ingolstadt Computing Centre Bernhard Brandel Phone : +49 841 937-21888 Catholit Universitet Eichstaett-Ingolstadt Computing Centre Bernhard Brandel Catholit Universitet Eichstaett-Ingolstadt Catholit Universitet Eichstaett-Ingolstadt Computing Centre Bernhard Brandel Catholit Universitet Eichstaett-Ingolstadt Catholit Universitet Eichstaett-Ingolstadt Catholit Universitet Eichstaett-Ingolstadt CA - 601 Cognistionschneide Catholit Honeysenson Catholit Honeysenson Catho		
Von Mir deenhandbrandel@uude* Antworten Wetterleiter Anthinken in Wetterleiter Anthink bernhandbrandel@uude* Anthonen An Mich bernhandbrandel@uude* Peter Kahouni An Mich bernhandbrandel@uude* Peter Kahouni Lieber Peter, diese Mall ist von min unterschrieben. Viele Gruße Bernhand Bernhand Bernhand Bernhand Computing Centre Det. Lingoistadt Computing Centre Dessed Finanz 49 Dessed Finanz 49 Dessed Finanz 49 Dessed Finanz 49 Dessed Finanz 40	🛓 Abrufen 🔻 🖋 Verfassen 🔲 Chat 🛔 Adressbuch 🛛 🗞 Schlagwörter 👻 🧠 Schnellfilter 🛛 Suchen < Strg+K 🔎 🔳	
Verif Test-signer E- Mail An Mich - bernhard brandel@ku.de> , Peter Kahoun Lieber Peter, diese Mall ist von mir unterschnieben. Viele Grüße Bernhard Bernhard Bernhard Brandel 1 Phone: +49 841 937-21888 Gatholic Universityt Eichstaett-Ingoistadt CA - 601 Organisationseinheit (OU) Universiteet Eichstaett-Ingoistadt CA - 601 <th>Ver Minshandhand Leve da 🔶 🔺 Antworten 🔿 Weiterleiten 🛱 Archivieren 🕼 Junk 🛇 Löschen</th> <th>Zertifikat-Ansicht: "Kath, Universitaet Eichstaett-Ingolstadt ID von Bernhard Brandel"</th>	Ver Minshandhand Leve da 🔶 🔺 Antworten 🔿 Weiterleiten 🛱 Archivieren 🕼 Junk 🛇 Löschen	Zertifikat-Ansicht: "Kath, Universitaet Eichstaett-Ingolstadt ID von Bernhard Brandel"
An Mich sternhard brandel@ku.de* , Peter Kahouni An Mich sternhard brandel@ku.de* , Peter Kahouni Lieber Peter, diese Mail 1st von mir unterschrieben. Viele Gruße Bernhard Bernhard Bernhard Bernhard Brandel Computing Centre Dert. Ingolstadt Computing Centre Dert. Ingolstadt Gersanzy mail to: bernhard.brandel@ku.de Bernhard Brandel Computing Centre Dest. Stockber Bernhard Brandel Centre Bernhard Brandel Computing Centre Dest. Stockber Bernhard Brandel Computing Centre Dest. Ingolstadt Computing Centre Dest. Stockber Bernhard Brandel Computing Centre Dest. Stockber Bernhard Brandel Computing Centre Dest. Stockber Bernhard Brandel Computing Centre Dest. Stockber Bernhard Brandel Computing Centre Bernhard Brandel Computing C		
An Mick shernhardbrandel@kudes _ Peter Kahoon _ Andere Aktionen - Lieber Peter, Lieber Peter, diese Mall ist von mir unterschrieben. Viele Grüße Bernhard Bernhard Bernhard Brandel _ Done: +49 841 937-21888 Catholic Universityr Eichstaett-Ingolstadt Camputing Centre Dest. +49 841 937-21888 Catholic Universityr Eichstaett-Ingolstadt Camputing Centre Dest. +49 841 937-21888 Augereinen Yame (A) Bernhard Brandel Diganisation (O) Kath. Universitaet Eichstaett-Ingolstadt Corganisation (O) Kath. Universitaet Eichstaett-Ingolstadt Computing Centre Dest. +49 841 937-21888 Augereinen Yame (A) Kath. Universitaet Eichstaett-Ingolstadt Computing Centre Dest. Hachricht enthält eine gültige digibale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Unterschriteser Einhard Brandel [kuu de Zetrifikat Rohmo seiten von Kath. Universitaet Eichstaett-Ingolstadt Catholic verschristeel [kinsteatt-Ingolstadt Germany mailto:bernhard.brandel@kuu de Zetrifikat Rohmo seiten von Kath. Universitaet Eichstaett-Ingolstadt CA - 601 Organisation (O) Kath. Universitaet Eichstaett-Ingolstadt Cardollic werschristeel [kinsteat] Netwickterschristeel [kinsteat] Netwickterschristeel [kinsteat] Netwickterschristeel [kinsteat] Diese kachrickt enthält eine gültige digibale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Unterschristeel [kinsteat] Zetrifikat Rohmo seiten von Kath. Universiteat Eichstaett-Ingolstadt CA - 601 Diese kachrickt enthält eine gültige digibale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Unterschritteer einhard Brandel Zetrifikat Rohmo seiten von Kath. Universiteat Eichstaett-Ingolstadt CA - 601 Diese Kachrickt enthält eine gültige digibale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Diese Kachrickt enthält eine gültige digibale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Diese Kachrickt enthält eine gültige digibale Unterschrift. Die Nachricht w	Betreff Test- signierte E-Mail	Allgemein Details
Lieber Peter, diese Mail ist von mir unterschrieben. Viele Grüße Bernhard 	An Mich < bernhard.brandel@ku.de> 😫, Peter Kahounia Andere Aktionen *	
Lieber Peter, diese Mail ist von mir unterschrieben. Viele Grüße Bernhard 		Dieses Zertürkat wurde für die folgenden Verwendungen verifiziert:
diese Mall ist von mir unterschrieben. Viele Grüße Bernhard 	Lieber Peter,	E-Mail-Unterzeichner-Zertifikat
Viele Grüße Bernhard	diese Mail ist von mir unterschrieben.	E-Mail-Empfänger-Zertifikat
Viele Grüße Bernhard Bernhard Serienum Serienum Bernhard Serienum		Assaestellt für
Bernhard	Viele Grüße	Allgemeiner Name (CN) Bernhard Brandel
Bernhard Organizationseinheit (DU) Universitatestrechenzentrum Bernhard Brandel Phone: +49 841 937-21888 Seriennummer TrASBS1843AF938 Computing Centre Allgemeiner Name (CN) Kath. Universitate Eichstatet-Ingolstadt CA - 601 Organizationseinheit (DU) Universitatesterchenzentrum Seriennummer Auf der Schanz 49 Auf der Schanz 49 Universitatesterchenzentrum DesSelag Ingolstadt Barnhard. brandel [kku. de Saszellt von Seriennung Saszellt von Saszellt von Nachrichten-Sicheghan Barnhard Brandel Barnhard Brandel Organizationseinheit (DU) Universitatestrechenzentrum Validität Validität Saszellt von Saszellt von Organizationseinheit (DU) Universitatestrechenzentrum Mosentrechenzentrum Diese Nachricht wurde unterschrieben Saszellt von Saszellt von Uniterschrieben von: Benhard Brandel Kath. Universitate Eichstatet-Ingolstadt CA - 601 Mosentrechenzentruk Validität Strömswachn von: Kath. Universitate Eichstatet-Ingolstadt CA - 601 Saszellt von Saszellt von Validität Strömswachn von: Kath. Universitate Eichstatet-Ingolstadt CA - 601 Saszellt von Saszellt von	Developed and the second se	Organisation (O) Kath. Universitaet Eichstaett-Ingolstadt
Seriennummer 17.5555.943ArP38 Augestellt von Bernhard Brandel Phone: +49 841 937-21888 Catholic University Eichstaett-Ingolstadt Cooputing Constant (CN) Kath. Universitaet Eichstaett-Ingolstadt Cooputing Constant (CN) Universitaet Eichstaett-Ingolstadt Cooputing Constant (CN) Universitaet Eichstaett-Ingolstadt Cooputing Constant (CN) Universitaet Eichstaett-Ingolstadt Cooputing Coopu	Bernhard	Organisationseinheit (OU) Universitaetsrechenzentrum
Augestell von Bernhard Brandel Phone: +49 841 937-21888 Catholic University Eichstaett-Ingolstadt Camputing Centre Dept. Ingolstadt Auf der Schanz 49 		Seriennummer 17:A5:B5:B4:3A:F9:38
Bernhard Brandel Phone: +49 841 937-21888 Catholic University Eichstaett-Ingolstadt Allgemeiner Name (CN Kath. Universitet Eichstaett-Ingolstadt (CA - 001 Computing: Centre Organisationseinheit (OU) Universitet Eichstaett-Ingolstadt Organisationseinheit (OU) Ders. Ingolstadt Fax: +49 841 937-218880 Validität Validität Auf der Schanz. 49 mailto:bernhard.brandel@ku.de Bassettilt am 28.05.2014 Bernhardt Brandell@ku.de Bassettilt am 27.05.2017 Fingerabdrücke Stath. Universitaet Eichstaett-Ingolstadt CA - 601 Moschricht wurde unterschrieben Bassettilt am 28.05.2014 Diese Nachricht wurde nicht verändert, seit sie gesendet wurde. Wolf-Fingerabdrücke Validität Kath. Universitaet Eichstaett-Ingolstadt CA - 601 Unterschrieben vom: Benhard Brandel Kath. Universitaet Eichstaett-Ingolstadt CA - 601 Unterschrieben vom: Benhard Brandel Kath. Universitaet Eichstaett-Ingolstadt CA - 601 Unterschrieben vom: Benhard Brandel Kath. Universitaet Eichstaett-Ingolstadt CA - 601 Unterschrieben vom: Benhard Brandel Kath. Universitaet Eichstaett-Ingolstadt CA - 601 Unterschrieben vom: Kath. Universitaet Eichstaett-Ingolstadt CA - 601 Schlieben Dire Nedwicht wurde nicht verschlissett<		Ausgestellt von
Catholic University Eichstaett-Ingolstadt Computing Centre Dept. Ingolstadt Auf der Schaz 49 0-85849 Ingolstadt Gemany mailto:bernhard.brandel@ku.de 93% Nachrichten:Sichebai Schricht wurde unterschrieben Diese Nachricht malt eine gultige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Unterschrieben von: Bernhard Brandel Extrijk.Adresse bernhardberandel@ku.de Zerifikat Nachrogeseign von: Kath. Universitaet Eichstaett-Ingolstadt CA - 601 Unterschriftsetrifikat ansehen I	Bernhard Brandel Phone: +49 841 937-21888	Allgemeiner Name (CN) Kath. Universitaet Eichstaett-Ingolstadt CA - G01
Computing Centre Organisationsemment (Uo) Unvestitative contractive mentative contractive mentative contractive mentative contractive mentative mentat	Catholic University Eichstaett-Ingolstadt	Organisation (O) Kath. Universitaet Eichstaett-Ingolstadt
Auf den Schanz 49 O-85649 Ingolstadt Germany Machinet Schenzeite Machinet Schenzeite Machinet Schenzeite Machinet wurde unterschrieben Diese Nachricht wurde unterschrieben Diese Nachricht wurde unterschrieben Diese Nachricht wurde nicht verändeit, seit sie gesendet wurde. Unterschrieben vom: Benhand Brandel Auflichterseiter Schenzeiter Mostersteiter wurde nicht verschlussett Diese Nachricht wurde	Dent Ingolstadt Fax: +49 841 937-218880	Organisationseinneit (OU) Universitäetsrechenzentrum
D-85899 Ingolstadt Germany mailto:bernhard.brandel@ku.de 93% Nachrichten-Sicheghain 64chricht wurde unterschrieben Diese Nachricht mital eine gultige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Unterschrieben von: Bernhard Brandel 24chricht halt eine gultige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Unterschrieben von: Bernhard Brandel 24chricht halt eine gultige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Unterschrieben von: Bernhard Brandel 24chricht durde nicht verschlüsselt Dinterschriftstat nichte werschlüsselt Nachricht wurde nicht verschlüsselt	Auf der Schanz 49	Validität
Germany mailto:bernhard.brandel@ku.de Germany 93% Nachrichter:Sichgebei 93% Nachrichter:Sichgebei 93% Dies Nachricht wurde unterschrieben 28 Dies Nachricht wurde unterschrieben 28 Dies Nachricht wurde unterschrieben 28 Zerifikat Nachweite Unterschrieben 28 Machricht wurde nicht versitet Eichsteet-Ingolstadt CA - 601 28 Unterschrieben von: Eich ister werschlüssett Dies Nachricht wurde nicht verschlüssett Schließen	D-85049 Ingolstadt	Ausgestellt am 28.05.2014
	Germany mailto:bernhard.brandel@ku.de	21.05.2017
Nachrichten-Sickerburg XX Machrichten-Sickerburg XX Diese Nachricht enthält eine gültige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Machrichtenschrieben von: Unterschrieben von: Bernhard Brandel Xx4 Zertifikat hördssegehen von: Kahn Universitate Eichstaett-Ingolstadt CA - 601 Schlieben Nachricht wurde nicht verschlüsselt Schlieben Schlieben	93% ·	Fingerabdrucke 0E-36-8C-00-EB-08-00-43-D9-50-B3-6E-2D-4B-28-5B-6E-7A-50-AD
Nachricht wurde nicht verschlüsselt Schließen Nachricht wurde nicht verschlüsselt Schließen	Nachrichten Sicharheit	MD5-Fingerabdruck CA:9D:EE:98:1B:2B:31:3E:7D:9F:AA:FD:D2:A0:5D:AB
bischricht wurde unterschrieben Diese Nachricht mitalt eine gültige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Unterschrieben von: Benhardbrandel@ku.de Zentifikat herzongegehen von: Kath. Unterschriebt eicht verschlasset Unterschriftszertifikat ansehen Nachricht wurde nicht verschlässet Schließen		
Diese Nachricht enthält eine gultige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde. Unterschrieben von: Bernhard Brandel Er Mail-Adresse: Bernhard.brandel@ku.de Zertfinkal höftenspegehen von: Kah. Universitaet Einstaett-Ingolstadt CA - 601 Unterschriftszentifikat ansehen Nachricht wurde nicht verschlüsselt Dires Nachricht wurde nicht verschlüsselt leisen die eine Verschlüsseline über die Naturet / Intersch	Machricht wurde unterschrieben	
Unterschrieben von: Bernhard Brandel R. Mail-Adresse: bernhard Brandel@ku.de Zetrifikat härdrosgeden von: Kah. Universitate Eichstaett-Ingolstadt CA - 601 Unterschriftstertifikat ansehen I Nachricht wurde nicht verschlüsselt Dires Nachricht wurde nicht werschlüsselt	Diese Nachricht enthält eine gültige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde.	
Partigi-Adresse: bernhardbande@Rude Zerifikat härdsspecken von: Kath. Universitet Eichstaett-Ingolstadt CA - 601 Unterschriftszertrifikat ansehen	Unterschrieben von: Bernhard Brandel	
Zertifikat härangesehen von: Kath. Universitatet Eichstett-Ingolstadt CA - 601 Unterschriftszertifikat ansehen Nachricht wurde nicht verschlüsselt Schließen	E-Mail-Adresse: bernhard.brandel@ku.de	
Chterschriftszentifikat ansehen Nachricht wurde nich verschlüsselt Schließen	Zertifikat herausgegeben von: Kath. Universitaet Eichstaett-Ingolstadt CA - G01	
Nachricht wurde nicht verschlüsselt Schließen die bes Verschlüsselt ferenztiesen die aben Verschlüsselten über der Naturek (Interest	Unterschriftszertifikat ansehen	
Nachricht wurde nicht verschlüsselt Schließen		
Diese Nichnicht wurde um Senden nicht verschlüsselt Informationen, die ahne Verschlüsseltung über der Netwurde / Internet	Nachricht wurde nicht verschlüsselt	Schließen
Diese Nachnicht wurde vor dem Seinden micht verschlusseld, die Onne Verschlusselding duel das Netzwerk / Internet	Diese Nachricht wurde vor dem Senden nicht verschlüsselt. Informationen, die ohne Verschlüsselung über das Netzwerk / Internet	
gesendet werden, können von anderen Personen eingesehen werden, während sie übertragen werden.	gesendet werden, können von anderen Personen eingesehen werden, während sie übertragen werden.	
OK	OK	

38

ertifikatshierarchie	
Deutsche Telekom Root CA 2	
▲DFN-Verein PCA Global - G01	
Kath. Universitaet Eichstaett-Ingolstadt CA - G01	
Bernhard Brandel	
Certifikats-Layout	
Kath. Universitaet Eichstaett-Ingolstadt ID von Bernhard Brandel	*
#Zertifikat	
Version	E
Seriennummer	
Zertifikatsunterzeichnungs-Algorithmus	
Aussteller	
▲Validität	
Nicht vor	
Nicht nach	
Inhaber	-
eld-Wert	

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.

Schließen

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