# Thunderbird - Signieren und Verschlüsseln von E-Mails

### 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 Zertifikate 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".

nein Lesen & Ans	sicht Netzwerk & Speicher	platz Update Zertifik	ate		Zertifikatsname	Kryptographie-Modul	Seri	iennummer	Läuft ab am	
nn eine Website na O Automatisch ertifikate	ach dem persönlichen Sich- eins wählen ③ Jgdes M. dierung <u>Kryptographie</u>	erheitszertifikat verlan al fragen -Module	gt:		▲ Kath. Universitaet Eichsta. Eernhard Brandel	"Software-Sicherheitsmor	dul 135	0:D6:DD:19:5C:77	06.02.2015	
🔇 Zu importie	rende Zertifikat-Datei				Ansehen Sichern	Alle sichem	portieren	Löschen	×	<u>}</u>
Organisieren	<ul> <li>▶ Computer ▶ System</li> <li>▶ Neuer Ordner</li> </ul>	(C:) + Sonstiges +	Zetifikatssicherungen				•   4y	] Zertifikatssicheru ∦≕	ngen durchs 🔎	
Organisieren	<ul> <li>Computer &gt; System</li> <li>Neuer Ordner</li> <li>penVPN</li> <li>ogramData</li> <li>ogramme</li> </ul>	(C:) ▶ Sonstiges ▶	Zetifikatssicherungen Name Nicht angegeben	^ (3)	Änderungsdatum	Тур С	<ul> <li>✓</li> <li>✓</li> <li>Øröße</li> </ul>	Zertifikatssicheru #==	ingen durchs 🔎	
Organisieren Drganisieren Pri Pri Pri	<ul> <li>Computer &gt; System</li> <li>Neuer Ordner</li> <li>penVPN</li> <li>ogramData</li> <li>ogramme</li> <li>(x86)</li> </ul>	(C:) ► Sonstiges ►	Zetifikatssicherungen Name Nicht angegeben	(3)	Änderungsdøtum 28.05.2014 22:36	Typ G	• 4) iröße 15 KB	Zertifikatssicheru 855	ingen durchs P	
Organisieren Drganisieren Pr Pr Pr	Computer      System     Neuer Ordner penVPN ogramData ogramme (x86) scovery	(C:) > Sonstiges >	Zetifikatssicherungen Name Nicht angegeben Fra-userp12 Fra-userp12 Fra-userp12	(3)	Änderungsdatum 28.05.2014 22:36 27.05.2014 19:31 30.05 2014 21:31	Typ G Privater Informati Privater Informati.	• 49 3röße 15 KB 8 KB 8 KB	Zertifikatssicheru 855	ngen 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.



Einstellen der S/MIME-Sicherheit des KU-Mailkontos

Ihr Zertifikat liegt nun im Zertifikatsspeicher von Thunderbird, ist aber noch nicht Ihrem KUMailkonto 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

	Konten-Einstellungen
bernhard.brandel@ku.de	S/MIME-Sicherheit
Server-Einstellungen Kopien & Ordner Verfassen & Adressieren Junk-Filter Synchronisation & Speicherplatz Empfangsbestätigungen (MDN) S/MIME-Sicherheit Junk-Filter Speicherplatz Postausgang-Server (SMTP)	Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben. Digitale Unterschrift Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiber: Kath. Universitaet Eichstaett-Ingolstadt ID von Bernhard Brandel Werschlüsselung Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln: Auswählen Leeren Solgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln: Kath. Universitaet Eichstaett-Ingolstadt ID von Bernhard Brandel Auswählen Leeren Solgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln: (Standard-Verschlüsselungseinstellung beim Senden von Nachrichten: Netwendig (Senden nur möglich, wenn alle Empfänger ein Zertifikat besitzen)
Konten-Aktionen	Zertifikate     Zertifikate verwalten     Kryptographie-Module verwalten 7.
	OK Abbrechen
2 110	A Zertifikat wählen

Ausgestell ngolstadt	: auf: CN=Bernhard Brandel,OU=Universitaetsrechenzentrum,O=Kath. Universitaet Eichstaett- C=DE	1
Seriennu	nmer: 17:A5:B5:B4:3A:F9:38	
Gültig vo	n 28.05.2014 21:25:24 an 27.05.2017 21:25:24	
Verwend	ing eines Zertifikatsschlüssels: unterzeichne,Non-repudiation,Schlüssel-Verschlüsselung	
E-Mail: b	rnhard.brandel@ku.de	
Ausgestell	: von: E=pki@ku-eichstaett.de,CN=Kath. Universitaet Eichstaett-Ingolstadt CA -	
G01,OU=L	niversitaetsrechenzentrum,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.

## 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:

Benutzer-Identifikationsanfrage	
Diese Website verlangt, dass Sie sich mit einem Zertifikat identifizieren: eo-dell-r715a.ku.de (:143) Organisation: "Kath. Universitaet Eichstaett-Ingolstadt" Ausgestellt unter: "Kath. Universitaet Eichstaett-Ingolstadt"	
Wählen Sie ein Zertifikat, das als Identifikation vorgezeigt wird:	
Kath. Universitaet Eichstaett-Ingolstadt ID von Bernhard Brandel [17:A5:B5:B4:3A:F9:38]	
Details des gewählten Zertrikäts:	
Ausgestellt auf: CN=Bernhard Brandel, OU=Universitaetsrechenzentrum, O=Kath. Universitaet Eichstaett-Ingolstadt, C=DE Seriennummen 17:45:85:84:34:59:38 Gültig von 28:05:2014 21:25:24 an 27:05:2017 21:25:24 Verwendung eines Zertifikatsschlüssels: unterzeichne, Non-repudiation, Schlüssel- Verschlüsselung E-Mai: bernhard.brandel@ku.de Ausgestellt von: E=pki@ku=eichstaett.de, CN=Kath. Universitaet Eichstaett-Ingolstadt	Passwort erforderlich     X       Image: State of the state o
OK Abbrechen	OK Abbrechen

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.

	C Verfassen: Test- signierte E-Mail
	Datei Bearbeiten Ansicht Einfügen Format Optionen Extras Hilfe
	🎆 Senden) 🖌 Rechtschr. 👻 🔋 Anhang 👻 🕒 S/MIME 💌 🕞 Speichern 💌
	Von: Bernhard Brandel < bernh Nachricht verschlüsseln
	An: 🔒 bernhard.brandel@ku🕜 Nachricht unterschreiben
	An: An: Peter Kahoun < peter. Sjcherheitsinformationen anzeigen
	▼ An: 8
	Betreff: Test- signierte E-Mail
	Normaler Text 🔻 Variable Breite 🔹 🖛 🖌 🖌 🗛 🗛 🖄 🗄 📜 🗄 🖽 🗮 - 📟 - 🌚 -
	Lieber Peter,
	diese Mail ist von mir unterschrieben.
	Viele Grüße
	Bernhard
	0.00
A Posteingang - bernhard.bran	Bernhard Brandel Phone: +49 841 937-21888
Datei Rearbeiten Ansicht Navination Nachricht Extras Hilfe	Catholic University Eichstaett-Ingolstadt
Zaci Zenocici Biscic inflation Bochicic Dings Time	Computing Centre Dept. Ingolstadt Fax: +49 841 937-218880
Abrufen Verfassen Chat 🛔 Adressbuch 🗞 Schlagwörter 👻 🔍 Schnellfilter	Auf der Schanz 49 D-85049 Ingolstadt
🗚 bernhard.brandel@ku.de 🔥 🛧 Schnellfilter: 🐢 Ungelesen 🖈 Gekennzeichnet 🛔 Konta	Germany mailto:bernhard.brandel@ku.de

Fertig – die unterschriebene E-Mail ist verschickt.

5

**±** -

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.

#### 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:

Verfessers: Verschlüse	Aungo-Test für die INALERZE	100			Concession of the local division of the loca	
Datai Baarboitan Area	icht Erritgen Ermat Opticzan	Edne bill	·			
💶 Sandan) 🖌 Racht	nche. * 👌 Anbung 🖓 51/19	ati 🔊 🖬 s	peichara *			
Non:	Bumhard Branckel + Service Net	hight geach	kitoseln			
* An	8 bemtarzibrance@ou 🖉 has	high annual	chroliben			
<ul> <li>Arc</li> </ul>	🚊 PaterKalcous (pater 1 50)	en els morn	stienen area	igen		
• An	8					
Betpett: Verschüselunge-Text Nr. die 24C/2522						
Vorformaties * 8	inta Breite 🔹 💻 y	A' A' A	AAH	10 B C	<b>Ξ·</b> ≡·©·	
Hallo Peter,						
hier ist eine versch	hlüsselte und signierte E-Mail					
beste oruse	Beste Grüße					
Bernhard						
Berrhard Boardel		Photes	-59 861	937-218	0.0	
Catholic Univers	ity Eichstaett-Ingolstart	E.	149 643	101 110		
Computing Centre		Engli	10 014	037.110	0.00	
Auf den Schanz 4	Dept. Ingolstadt Fai: +49 841 937-218888 Auf der Schanz 40					
D-85840 Ingolstadt						
Germany		14-120-	carrierara.	pranta ria	0.01.016	

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.

	Emails_verschluenieren_ik114.pdf
Quelle:	