SIGNAT Certification Authority

Anleitung zur Nutzung von S/MIME

Tobias Dussa · Heiko Reese

STEINBUCH CENTRE FOR COMPUTING

<pre>p* mail.home.sdhs.de.suns Lnop.nop.TS val 46221460 ecr 90011646], length 0 7666, ack 5272, win 108, options [nop.nop.TS val 90011646], length 0 r sccsec=mobile=rz121.home.sdhs.de.51983 > mail.home.sdhs.de.51983; Flags [n 1002, options [nop.nop.TS val 46221460 ecr 90011646], length 0 r sccsec=mobile=rz121.home.sdhs.de.51983 > mail.home.sdhs.de.sun; Flags [p sccsec=mobile=rz121.home.sdhs.de.51983 > mail.home.sdhs.de.sun; Flags [n 1002, options [nop.nop.TS val 46221460 ecr 90011646], length 0 r sccsec=mobile=rz121.home.sdhs.de.51983 > mail.home.sdhs.de.sun; Flags [p sccsec=mobile=rz121.home.sdhs.de.sdhs.de.sun; Flags [p scc</pre>
Louis Lee, 01:9851 Flags [Dec 14 04:00-17
20 41 66 74 65 72 20 3a 20 4a 61 6e 20 31 36 3a 32 38 32 32 1 Antr-auth-outgoing: 1260759617,226588 end asg 204656239 20 32 30 31 32 20 47 4d 54 0a 20 25 26
74 75 74 65 20 6F 66 20 54 65 63 68 6e 6F 6c 6F 67 79 2c 43 3d 44 50 a t: CN=CR7,0EKr StrT-CERT,0U=KI d: 1260759644,956961 topserver: status: 1/40 20 20 20 20 20 20 20 20 20 20 53 75 62 6a 65 63 74 20 50 75 62 6c 69 63 20 4b Subject Public Ki 969644,956965 topserver: ok 9516 0:192,168
6c 63 20 4b 65 79 20 41 6c 67 67 72 69 74 68 6d 3a 20 <td< td=""></td<>
20 20 20 20 20 20 20 20 20 20 20 20 20 2
39 3a 61 66 3a 32 31 32 3a 34 34 3a 62 63 3a 51 19:af:21:86:56:12:44:bc:51 d: 1260/35644.30015 topserver: et auto to topserver: et auto topserver: et
20 20 61 50 5a 55 5a 55 5a 56 5a 62 34 3a 64 33 3a 64 62 3a 62 66 3a 0a 14:95:23:6f:b4:d3:db:bf:. 46 2003 34 3a 39 35 3a 32 33 3a 36 66 3a 62 34 3a 64 33 3a 64 62 3a 62 66 3a 0a 14:95:23:6f:b4:d3:db:bf:. trainel/delivermail: 126075647.465701 1 message fo
P printserver.home.sdhs.de.30203 > 192.168.1.255.30202! UP, Tendh 173 De 14 040047 means and 150050 State 150050 P printserver.home.sdhs.de 7303 > 255 255 255 255 255 255 255 255 255 2

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

www.kit.edu

Kontakt

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

Tobias Dussa Leiter

Campus Süd Zirkel 2 76131 Karlsruhe

 Telefon:
 0721 608-42479

 Fax:
 0721 608-9-42479

 E-Mail:
 tobias.dussa@kit.edu

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

Herausgeber

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

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

Stand 2012-09-24 (Revision 2323)

www.kit.edu

Inhaltsverzeichnis

1	Einleitung	4
2	Grundlagen von S/MIME	4
3	Herunterladen und Importieren der Zertifikatkette 3.1 Herunterladen der Zertifikate der DFN-CA, der KIT-CA und der UNIKA-CA 3.2 Importieren der CA-Zertifikate 3.2.1 Microsoft Outlook 2003 und 2007 3.2.2 Mozilla Thunderbird 3.0 und 3.1	5 8 8 10
4	Importieren des eigenen Nutzerzertifikats und Schlüssels4.1Microsoft Outlook 2003 und 20074.2Mozilla Thunderbird 3.0 und 3.1	12 12 15
5	Importieren von Nutzerzertifikaten anderer Anwender 5.1 Manueller Import	17 17 19 21 21 23
6	Konfigurieren Ihres Mailprogramms6.1Microsoft Outlook 20036.2Microsoft Outlook 20076.3Mozilla Thunderbird 3.0 und 3.1	23 23 24 25
7	Signieren von E-Mails7.1Microsoft Outlook 2003 und 20077.2Mozilla Thunderbird 3.0 und 3.1	27 27 28
8	Verschlüsseln von E-Mails8.1Microsoft Outlook 2003 und 20078.2Mozilla Thunderbird 3.0 und 3.1	28 28 29

Revisionshistorie

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

1 Einleitung

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

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

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

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

Im folgenden werden diese grundsätzlichen Arbeitsschritte beschrieben:

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

2 Grundlagen von S/MIME

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

- verschlüsselt und
- signiert

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

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

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

3 Herunterladen und Importieren der Zertifikatkette

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

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

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

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

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



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



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

🕙 Karlsruhe Instit	itute of Technology (KIT) - Mozilla Firefox		
Datei Bearbeiten	n Ansicht ⊆hronik Lesezeichen E⊻tras Hilfe		
C C	🖻 🗶 🏠 📗 dín. de https://pki.pca.dín.de/ki-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=28RA_ID=0 😭 🕤	Google	P
🙆 Meistbesuchte Sei	Seiten 🐢 Erste Schritte 🔝 Aktuelle Nachrichten		
📔 Karlsruhe Inst	stitute of Technology (K 🔅		-
		DEN	<u> </u>
		Deutsches	•
		Forschungsnetz	
Zertif	ifikate CA-Zertifikate Gesperrte Zertifikate Policies Hilfe Beenden		
Wurz	zelzertifikat DFN-PCA Zerti ^{el} kot KIT CA Zertifikat Zertifikatkette anzeigen		
	Link in neuem Iab öffnen		
	Lesezeichen für diesen Link hinzufügen		
	Schnittstell Link senden	D	
	Installie <u>Link-Adresse kopieren</u> Inkal das CA-Zertinkal in Infernie	srowser	
	Eigenschaften		
	 Wählen Sie "Wurzelzertifikat", "DFN-PCA Zertifikat" bzw. "KIT-CA Zertifikat" um das je Zertifikat in Ihrem Browser zu installieren. 	weilige	
	• Wählen Sie "Zertifikatkette anzeigen", wonn Sie die Zertifikate in einer Datei speicher:	n	
	möchten (PEM-Format).		
	Kontaktinformationen für Rückfragen finden Sie unter "Hilfe".		
		Impressum	
Fertig			

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

🕹 Karlsruhe Institu	e of Technology (KIT) - Mozilia Firefox
Bitte geben Sie der	Dateinamen an, unter dem die Datei gespeichert werden soll 👔 🔀
Spejchern in:	🖻 Desktop 💽 🚱 🌮 🕮 🔹 ejname=index;jd=268A_ID=0 💮 🖓 🕇 Google 🔎
Zułczi verwendele D Desktop Eigene Dateien Arbeitsplatz Netzweikunge	Eigene Datein Arbeitsplatz INetzwerkungebung teigene: dn-cd.ct geitsches Forschungsnetz s Hilfe Beenden fikat Zertifikatkette anzeigen nistratoren - CA-Zertifikate Zertifikat das CA-Zertifikat in Ihrem Browser in einer Datei speichern. teigen: dn-cd.ct Speichern Eigene: dn-cd.ct Value of the construction of the construction of the construction of the construction Abbrecher Value of the construction of the cons
	Impressum -
Fertig	

- 4. Klicken Sie mit der rechten Maustaste auf die Schaltfläche »KIT-CA-Zertifikat« und speichern Sie das Linkziel. Der vorgeschlagene Dateiname lautet cacert.crt; ändern Sie diesen in kit-ca.crt.
- 5. Öffnen Sie mit einem Webbrowser die Webseite der UNIKA-CA (https://pki.pca.dfn.de/ uni-karlsruhe-ca/pub).
- 6. Klicken Sie auf den Reiter »CA-Zertifikate«.
- 7. Klicken Sie mit der rechten Maustaste auf die Schaltfläche »UNIKA-CA-Zertifikat« und speichern Sie das Linkziel. Der vorgeschlagene Dateiname lautet cacert.crt; ändern Sie diesen in unika-ca. crt.
- 8. Klicken Sie mit der rechten Maustaste auf die Schaltfläche »Wurzelzertifikat« und speichern Sie das Linkziel. Der vorgeschlagene Dateiname lautet rootcert.crt; ändern Sie diesen in dtag-ca. crt.

3.2 Importieren der CA-Zertifikate

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

3.2.1 Microsoft Outlook 2003 und 2007

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

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

	2 Mar.
	dfn-ca.crt
Öffnen	
Zertifikat installieren	
7-Zip	•
Editiere mit Vim	
Öffnen mit	
RTortoiseSVN	•
UltraEdit-32	
💟 Scannen auf Bedrohunger	n
🗐 WinZip	•
Senden an	•
Ausschneiden	
Kopieren	
Verknüpfung erstellen	
Löschen	
Umbenennen	
Eigenschaften	

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

Datei öffnen - Sicherheitswarnung						
Möchten Sie diese Datei öffnen?						
(Angel	Name: dfn-ca.crt					
	Herausgeber: Unbekannter Herausgeber					
	Typ: Sicherheitszertifikat					
	Von: C:\Dokumente und Einstellungen\rz121\Desktop					
	Ŭlfnen Abbrechen					
Vor	dem Üffnen dieser Datei immer bestätigen					
Dateien aus dem Internet körnen nützlich sein, aber dieser Dateilyp kann eventuell auf den Computer Schaden anrichten. Üffren Sie dess Software nicht, falls Sie der Quelle nicht vertrauen. <u>Welches</u> <u>Risiko besteht?</u>						

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



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

tifikatimport-Assistent	>
ertifikatspeicher	
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert	
Windows kann automatisch einen Zertifikatspeicher auswählen oder Sie könner Pfad für die Zertifikate angeben.	n einen
 Zertifikatspeicher automatisch auswählen (auf dem Zertifikatstyp basier 	rend)
C Alle Zertifikate in folgendem Speicher speichern	
Zertifikatspeicher:	
Durchs	uchen
< Zurück Weiter >	Abbrechen

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

ertifikatimport-Assistent		×			
	Fertigstellen des Assistenten Der Zertfikatmport-Assistent wurde erfolgreich abgeschlossen.				
	Sie haben folgende Einstellungen ausgewählt:				
	Gewählter Zertfifikätspeicher Inhalt Zertfifikatspeicher Zertfifikat				
	4 · · · ·				
	< Zurück Fertig stellen Abbrechen				

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



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

3.2.2 Mozilla Thunderbird 3.0 und 3.1

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

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

🧟 - Mozilla Thunderbird	
Datei Bearbeiten Ansicht Navigation Nachrid	ht Extras Hilfe
🖄 Abrufen 🔹 📝 Verfassen 🔲 Adressbuch	Adressbuch Strg+Umschalt+B Global in allen Konten suchen <strg+k></strg+k>
	Gespeicherte Dateien Strg+J Add-ons Abbit Starp
Alle Ordner 🛛 🖌 🕨	
E-Mai	Elter Filter auf Ordner anwenden Filter auf Nachricht anwenden
	Vac Junk-Filter auf Ordner anwenden Junk in diesem Ordner löschen
	Vet. Importieren Fehlerkonsole
· · · · · · · · · · · · · · · · · · ·	JUI ^T Konten-Einstellungen
News	aruppen
- C	Vewsgruppen abonnieren
	Junk-Filter-Einstellungen
Feeds	
.	Abonnements verwalten
1 Mozilla Thunderbird ist freie und quelloffene Softw	are von der gemeinnützigen Mozilla-Stiftung.
Fertig	

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

Thunderbird-Ei	nstellungen				×
AL?		-/		D	SÔ2
Allgemein	Ansicht	Verfassen	Sicherheit	Anhänge	Erweitert
Allasmain	on 9. Angicht [M	Intrauerie 9. Conside	ovelata I Liedate	Zertifikate	
Aligemein Les	en & Ansicht r	eczwerk & speich	erplatz Update	Zerdrikace	1
Wenn eine W	ebsite nach dem	personlichen Sich	erheitszertihkat v Mal Ganna	erlangt:	
C Aut	iniausuri eins wa	nien (* J <u>e</u> des	marirayen		
Zertifikate	Zertifikatspe	arrliste Validie	rung Kryptog	graphie-Module	
	•				
				or	
				06	AUUrechen

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



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

Vählen Sie die D	atei mit dem ode	r den zu importiere	enden CA-Zer	tifikat(er	1)	? ×
<u>S</u> uchen in:	🞯 Desktop		•	G 🖻	• 🖭 对	
Zuletzt verwendete D Desktop Eigene Dateien	Eigene Dateien Varbeitsplatz Kenacs Eigen din-ca.ort Varbacs V	bung				
Netzwerkumge	Dateiname:	dfn-ca.crt			•	Öffnen
bung	Dateityp:	Zertifikat-Dateien			•	Abbrechen

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

erunterladen des Zertifikats 🛛 🔀
Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.
Soll "DFN-Verein PCA Global - G01" für die folgenden Zwecke vertraut werden?
🔽 Dieser CA vertrauen, um Websites zu identifizieren.
🔽 Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.
Dieser CA vertrauen, um Software-Entwickler zu identifizieren.
Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien und Prozeduren (wenn vorhanden) überprüfen.
Ansicht CA-Zertifikat überprüfen
OK Abbrechen

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

4 Importieren des eigenen Nutzerzertifikats und Schlüssels

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

4.1 Microsoft Outlook 2003 und 2007

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

1. Kopieren Sie das zu importierende Zertifikat samt zugehörigem geheimen Schlüssel auf den verwendeten Rechner. Es ist nicht ausreichend, nur Ihr Zertifikat zu kopieren; auch der geheime Schlüssel wird benötigt! Dateien, die auf .pem, .crt, .cer und .der enden, enthalten in aller Regel *nicht* den geheimen Schlüssel, sondern lediglich das öffentliche Zertifikat. Dateien, die sowohl das Zertifikat als auch den dazugehörigen geheimen Schlüssel enthalten, haben üblicherweise Dateinamen, die auf .pfx oder .p12 enden. Sollten Sie nicht über eine entsprechende Datei verfügen, so können Sie sie erzeugen, indem Sie Ihr Zertifikat und den passenden geheimen Schlüssel von einem Rechner exportieren, auf dem beides bereits installiert ist. Details hierzu können Sie der Nutzungsanleitung der KIT-CA entnehmen, die unter dem URL http://www.scc.kit.edu/downloads/ism/benutzungsanleitung.pdf erhältlich ist.

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



3. Der Zertifikatimport-Assistent wird gestartet.

Zertifikatimport-Assistent		×			
	Willkommen				
	Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und -speriisten vom Datenträger in den Zertifikatspeicher.				
	Ein Zerthfikat wird von einer Zertifizierungsstelle ausgestellt und dient der Bestätigung Threr Identität. Zerthfikate enthalken Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkreverlindungen. Ein Zerthfikatspeicher ist der Systembereich, in dem Zerthfikate gespeichert werden.				
	Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.				
		=			
	< Zurück Weiter > Abbrecher				

4. Die zu importierende Zertifikatdatei wird nochmals angezeigt.



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

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

Zertifikatimport-Assistent	x
Kennwort	
Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.	
Geben Sie das Kennwort für den privaten Schlüssel ein.	
Kennwort:	
•••••	
 Hohe Sicherheit für den privaten Schlüssel aktivieren. Immer wenn der private Schlüssel von einer Anwendung verwendet wird, werden Sie zur Eingabe aufgefordert, wenn Sie diese Option aktivieren. Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen. 	
<2urück Weiter > Abbrechen	

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

Zertifikatimport-Assistent			×
Zertifikatspeicher			
Zertifikatspeicher sind Systembereiche, in	denen Zertifikate gespeiche	ərt	
Windows kann automatisch einen Zertifika Pfad für die Zertifikate angeben.	tspeicher auswählen oder S	ie können einen	
 Zertifikatspeicher automatisch ausv 	rählen (auf dem Zertifikatst	yp basierend)	
C Alle Zertifikate in folgendem Speich	er speichern		
Zertifikatspeicher:			
		Durchsuchen	
	< <u>Z</u> urück <u>W</u> eiter	> Abbrechen	

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

ertifikatimport-Assistent		×					
	Fertigstellen des Assistenten						
	Der Zertifikatimport-Assistent wurde erfolgreich abgeschlossen.						
	Sie haben folgende Einstellung	en ausgewählt:					
	Gewählter Zertifikatspeicher Inhalt Dateiname	Auswahl wird vom Assisten PFX C:\Dokumente und Einstelk					
	•	- F					
	< 7 mick	Eartia stallan Abbrachan					
	< Zuruck	Abbrechen					

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

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

import des pri	ivaten Austauschschlüssels	×
	Eine Anwendung erstellt ein geschütztes Objekt.	
	Privater Schlüssel des CryptoAPIs	
	Sie haben die mittlere Sicherheitsstufe gewählt.	
	OK Abbrechen Details	

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



4.2 Mozilla Thunderbird 3.0 und 3.1

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

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



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

hunderbird-Ei	nstellungen				>
<mark>상위</mark> Allgemein	Ansicht	Verfassen	Sicherheit	Ø Anhänge	Erweitert
Allgemein Les	en & Ansicht N	ietzwerk & Speich	erplatz Update	Zertifikate	
Wenn eine W	'ebsite nach dem amatisch eins wä	persönlichen Sich	erheitszertifikat v Mal fragen	verlangt:	
. 200	1	. I	1	1	
Zertifikate	Zertifikatspe	rrliste <u>V</u> alidie	rung <u>K</u> ryptoj	graphie-Module	
				ок	Abbrechen

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

3	Zertifikat-Manager				_ 🗆 ×
	Ihre Zertifikate Personen	Server Zertifizierungsstellen	Andere		
	Sie haben Zertihikate diese	r Organisationen, die Sie identifizi	ieren:		
	Zertifikatsname	Kryptographie-Modul	Seriennummer	Läuft ab am	<u> </u>
	Ansehen Sichern.	Alle sichern Importie	Löschen		
					or 1
					UK

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



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

Passworteingabe-Dialog	×
Bitte geben Sie das Passwort ein, das verwendet wurde, um dieses Zertifikats-Backup zu verschlüsseln.	
Passwort:	
OK Abbrechen	

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



5 Importieren von Nutzerzertifikaten anderer Anwender

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

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

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

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

5.1 Manueller Import

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

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

5.1.1 Microsoft Outlook 2003 und 2007

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

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

[] [Dussa, Tob	ias - Kontakt			_ = ×
Kontakt Einfügen Text formatiere	in					۲
Speichern von neuer Kontakt *	Allgemein Zertifikate	E-Mail Besprechung Anru	f Visitenkarte E	Bild Kategorisieren Nachverfolgung	ABC Rechtschreibung Dokumentarijfung	Kontaktnotizen
Aktionen Name Firma: Firma: Firma: Firma: Firma: Firma: Speichern unter: Dussa, Tobias Internet Firma: F	Anzeigen rchnology	Kommunizieren		Optionen Tobias Georg Dussa Kafsruhe Institute of Technology Steihubch Center for Computing +49-721-608-2479 Geschäftlich tobias.dussa@Mk.edu		OneNote
Dies ist die Postanschrift 76131 Karlsruhe Deutschland						-

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

(1) 4 * *		Dussa, Tobias - Ko	ontakt				- = ×
Kontakt Einfügen Text formati	eren						0
Speichern und neuer Kontakt * Speichern & schließen * Aktionen	Allgemein Zertifikate Details Alle Felder Aktivitäten Anzeigen	E-Mail Besprechung Anruf	Visitenkarte Bild Kategoris	ieren Nachverfolgung	ABC Rechtschreibung	Kontaktnotizen OneNote	
Outlook verwendet eines dieser Zertifikate, um ver Kontakt empfangen oder eine Zertifikatdatei für di Zertifikate (digitale IDs):	schlüsselte E-Mail-Nachrichten ar iesen Kontakt importieren.	i diesen Kontakt zu senden. Sie könn	en ein Zertifikat erhalten, indem	Sie eine digital signierte Na	achricht von diesem	_	
						Eigensch Als Standa	aften ardifesti.
						Importi	eren
						Exportie	nen

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

Zertifikat suchen				? ×
Suchen in:	C Downloads	•	🎯 • 🖄	X 📬 🖬 •
Zuletzt verwendete Dokumente	Tobias Dussa.cer			
Desktop				
Eigene Dateien				
Arbeitsplatz				
Netzwerkumgebung				
	Dateiname:		-	
	Dateityp: Digitale ID-Dateien (*.p7c;*.cer)	_	-	
E <u>x</u> tras •			Öffnen	Abbrechen

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

and of the second seco									
Kontakt Einfügen Text formation	eren								۲
Speichern und neuer Kontakt * Speichern & schließen & coschen	Allgemein Zertifikate Details Aktivitäten	E-Mail Besprechung	Anruf Ø	Visitenkarte E	Ild Kategorisierer	Nachverfolgung	Rechtschreibung	() Kontaktnotizen	
Aktionen	Anzeigen	Kommunizier	en		Optionen		Dokumentprüfung	OneNote	
Kontakt empfangen oder eine Zertifikatdatei für di Zertifikate (digitale ID:): Toblas Dussa(Standard)	esen Kontakt importieren.							Eigensch Als Stand: Imp <u>o</u> rti Expo <u>r</u> ti Entfer	aften ard <u>f</u> esti. eren eren

5.1.2 Mozilla Thunderbird 3.0 und 3.1

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

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

🧟 - Mozilla Thunderbird		l ×
Datei Bearbeiten Ansicht Navigation Nachricht	Extras Hife	-12
🐣 Abrufen 🔹 🃝 Verfassen 🔲 Adressbuch 🕓	Adressbuch Strg+Umschalt+B Global in allen Konten suchen <strg+k></strg+k>	$\mathbf{\rho}$
	Gespeicherte Dateien Strg+J Add-ons Aktivitikten	•
Alle Ordner 🚽 🕨	Mitiguateri	4
E-Mail	Eriter Filter auf Qidner anwenden Filter auf <u>N</u> achricht anwenden	
Na	ac Junk-Filter auf Ordner anwenden Jynk in diesem Ordner löschen	
Ne	EL Importieren Fehlerkonsole	
Ju	I ^r Konten-Einstellungen Einstellungen	
Newsg	ruppen	
R Ne	ewsgruppen abonnieren	
Ju	ink-Filter-Einstellungen	
Feeds		
ab Ab	ponnements verwalten	•
1 Mozilla Thunderbird ist freie und quelloffene Software	e von der gemeinnützigen Mozilla-Stiftung.	
Fertig		

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

Thunderbird-Ei	nstellungen				×
AL P		-/		Ø	₹Ô}
Allgemein	Ansicht	Verfassen	Sicherheit	Anhänge	Erweitert
Allgemein	en & Ansicht M	Jetzwerk & Speich	erolatz Lindate	Zertifikate	
Milgemeint Les	istration and dealers				1
C Aut	eusice nach dem amatisch eins wä	hlen 🛈 ledes	erneitszertinkat v Mal fragen	enange:	
- <u>H</u> uc		1000 SE 2002	Harragon		
Zertifikate	Zertifikatspe	errliste <u>V</u> alidie	rung <u>K</u> ryptog	graphie-Module	
				ОК	Abbrechen

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

Zertifikat-Mai	nager					_ 🗆 ×
Ihre Zertifikate	Personen	Server Zertifiz	ierungsstelle	n Andere		
Sie haben gesp	oeicherte Zert	ifikate, die diese	Personen id	entifizieren:		
Zertifikatsnan	ne		Läuft a	b am	E-Mail-Adresse	E.
Ansehen	Bearbeiter	Importier	en Exp	ortieren	ien	
						ОК

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

Wählen Sie die D	atei mit dem zu ir	nportierenden E-Mail	-Zertifikat		? ×
Suchen in:	🗁 Downloads		• 3	ø 🖻 📰	
Zuletzt verwendete D Desktop Eigene Dateien	Tobias Dussa.d	er			
Netzwerkumge bung	Dateiname: Dateityp:	Tobias Dussa.der Zertifikat-Dateien		•	Öffnen Abbrechen

5.2 Automatischer Import

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

5.2.1 Microsoft Outlook 2003 und 2007

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

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



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

Can U A ★ ↓ ▼		Tobias Dussa - Kon	itakt		_ = ×
Kontakt Einfügen Text formati	eren				۲
Speichern und neuer Kontakt * Speichern * & schließen * Löschen	S Allgemein Zertifikate Details Alle Felder	E-Mail Besprechung Anruf	Visitenkarte Bild Kategorisieren Na	achverfolgung	Kontaktnotizen
Outlook verwendet eines dieser Zertifikate, um ver Kontakt empfangen oder eine Zertifikatdatei für d	schlüsselte E-Mail-Nachrichten an iesen Kontakt importieren.	diesen Kontakt zu senden. Sie könne	n ein Zertifikat erhalten, indem Sie eine	digital signierte Nachricht von diesem	
Zertfrikate (digitale IDs); PN-Toblas Dussa/Testzertrifikat(Standard)					Eigenschaften Als Standard restl. Importeren Exportieren Entfernen

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



5.2.2 Mozilla Thunderbird 3.0 und 3.1

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

6 Konfigurieren Ihres Mailprogramms

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

6.1 Microsoft Outlook 2003

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

- 1. Klicken Sie im Menü »Extras« auf den Eintrag »Optionen«.
 - Extras Aktionen ? Senden/Empfangen Fr Suchen Fr Quite Adressbych... Strg+Umschalt+B Regeln und Benachrichtigungen... eir Ordner "Selöschte Objekte" [seren E-Mal-Konten... Angassen... Qptionen... X
- 2. Klicken Sie auf den seitlichen Reiter »Sicherheit« und aktivieren Sie die folgenden Einstellungen:
 - »Nachrichten und Anlagen verschlüsseln«, sofern Sie ausgehende E-Mails standardmäßig verschlüsseln möchten,
 - »Nachrichten digitale Signatur hinzufügen«, sofern Sie ausgehende E-Mails standardmäßig verschlüsseln möchten,
 - »Signierte Nachrichten als Klartext senden« sowie



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

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

5icherheitseinstellungen ändern	×
Bevorzugte Sicherheitseinstellungen Name der Sicherheitseinstellung:	
Demo	•
Kryptografieformat: S/MIME	•
☑ Standardeinstellung für dieses Eormat kryptografischer Na	chrichten
Standardsicherheitseinstellung für alle kryptografischer	n Nachrichten
Sigherheitskennzeichen Neu Löschen	Kennwort
Zertifikate und Algorithmen	
Signaturzertifikat: GRP:Windows-Kursaccount 01	Auswählen
Hashalgorithmus: SHA1	
Verschlüsselungszertifikat: GRP:Windows-Kursaccount 01	Auswählen
Verschlüsselungsalgorithmus: 3DES	
☑ Signierten Nachrichten diese Zertifikate hinzufügen	
OK	Abbrechen

6.2 Microsoft Outlook 2007

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

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

😔 Outlook Heute - Microsoft Outlool	ik			_ = >
Datei Bearbeiten Ansicht We	'e <u>c</u> hseln zu E <u>x</u>	tras Aktionen ?	-	Frage hier eingeben
🔂 Neu 🔹 🧰 🕼 🔁 Senden/	/Empfangen	Senden/Empf <u>a</u> ngen	🕨 🚽 🞯 Zurück 💿 🖄 📄 🚮 😋 outlook:Heute	• •
E-Mail « 🧐	Postfac	Sofortsuche		
Favoritenordner		Adressbuc <u>h</u> Strg+Umschalt+B Regeln und Benachrichtigungen		Outlook Heute anpassen
E-Mail-Ordner 😞 K	Kalender	A <u>b</u> wesenheits-Assistent	Aufgaben	Nachrichten
Alle E-Mail-Elemente Alle E-Mail-Elemente Constant - Dussa, Tobia: Deteted items Dintox Junk E-mail Outbox Subuck E-mail Outbox Subuck E-mail Sub	19 19	Postfach aufrägumen Postfach aufrägumen Orginer "Deleted Items" leeren Gelöschte Elemente wiederherstellen Eormulare Magro Kontoeijnstellungsen Vertrauensstellungsgenter Angassen Optionen Eigenschaftgen für E-Mail-Scan Nach Bedrohungen scgnnen	Admin tools (Keines) Bücher (Keines) IMEI (Keines) Must-read books (Keines) Sport (Keines)	Inbox 0 Drafts 3 Outbox 0
Content of the second				
ertig				🔀 Online mit Microsoft Exchange

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

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

/ertrauenswürdige Herausgeber	Verschlüsselte E-Mail-Nachrichten
Add-Ins	👩 🗖 Inhalt und Anlagen für ausgehande Nachrichten verschlüsseln
Datenschutzoptionen	Ausgehenden Nachrichten digitale Signatur hinzufügen
-Mail-Sicherheit	Signierte Nachrichten als <u>K</u> lartext senden
a la accelecta a disco a	S/MIME- <u>B</u> estätigung anfordern, wenn mit S/MIME signiert
niagenbenandlung	<u>S</u> tandardeinstellung: Meine S/MIME-Einstellungen (tobias.dussa@kit.edu) ▼ <u>E</u> instellungen
utomatischer Download	Pd-Bala TD- (Ta-Mdb-ba)
fakrosicherheit	Digitale IDS (Zertmikate)
rogrammgesteuerter Zugriff	Digitale IDs bzw. Zertifikate sind Dokumente, mit denen die Identität in elektronischen Transaktionen
	In GAL veröffentlichen Importieren/Exportieren Digitale ID anfordern
	Als Nur-Text lesen
	☑ Standardnachrichten im <u>N</u> ur-Text-Format lesen
	🔽 Digital signierte Nachrichten im Nur-Text-Format <u>l</u> esen
	Skript in Ordnern
	Skrint in freigegehenen Ordnern zulassen
	Skript in 'Öffentlichen Ordner' zulassen

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

Sicherheitseinstellungen ände	ern		×
Bevorzugte Sicherheitseinstellunge	en		
Name der Sicherheitseinstellung	g;		
Meine S/MIME-Einstellungen (tobias.dussa@kit.ed	u)	•
Kryptografieformat:	S/MIME		•
🔽 Standardeinstellung für die:	ses Format kryptogra	afischer Nachricht	en
🔽 Standardsicherheitsein	stellung für alle krypi	tografischen Nach	richten
Sicherheitskennzeichen	Neu	Löschen	Kennwort
Zertifikate und Algorithmen			
Signaturzertifikat:	PN:Tobias Dussa/1	estzertifikat	Auswählen
Hashalgorithmus:	SHA1	-	
Verschlüsselungszertifikat:	PN:Tobias Dussa/1	estzertifikat	Auswählen
Verschlüsselungsalgorithmus:	3DES	•	
🔽 Signierten Nachrichten dies	e Zertifikate hinzufü	gen	
		ОК	Abbrechen

6.3 Mozilla Thunderbird 3.0 und 3.1

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

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

Posteingang - Heiko.Reese@kit.edu - Mozilla Thu	inderbird		
Datei Bearbeiten Ansicht Navigation Nachricht	Extras Hilfe		
	Adressbuch Strg+Umschalt+B Add-ons	Posteingar	ng 🔽 🔎 🔀
🖄 Posteingang - Heiko.Reese@kit.edu	Aktivitäten		•
Alle Ordner	Eiter Filter importieren Filter auf Ordner anwenden Filter auf Nachricht anwenden	∞ Von	🧕 🕹 Datum 🔺 🖽
Entwurre	Junk-Filter auf Ordner anwenden Junk in diesem Ordner löschen		
Papierkorb (159)	I <u>m</u> portieren Fe <u>h</u> lerkonsole		
	Konten-Einstellungen Attachment Extractor - Einstellungen Einstellungen		
Local Folders Papierkorb Postausgang			
			Ungelesen: 0 Gesamt: 685 //

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

Heiko.Reese@kit.edu	S /MIME_Sicherheit
Server-Einstellungen	S/MIME-Sicherheit
Serie Laborangen Kopien & Ordner Verfassen & Adressieren Durk-Filter Synchronisation & Speicherpletz Empfangsbestätigungen (MDN) S/MME-Sicherheit El Blogs & News Feeds Speicherpletz Licola Flotders Inde Elber	Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselten ga auch eines für digitale Unterschrift angeben. Digitate Unterschrift Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiben: Auswählen. Useren Nachrichten digital unterschreiben (els Standerd) Verschlüsselung Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln:
Spielcherplatz Postausgang-Server (SMTP)	Standard-Verschlüsselungseinstellung beim Senden von Nachrichten:

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

Zertifikat wählen	×
Zertfikat: Imported Certificate [0F:70:15:DC] Details des Imported Certificate [0F:70:15:DC]	
Ausgestellt auf: CNIHeleio Rees, OLIENT-CERT, O-Karlsruhe Institute of Technology, C=DE Serienrummer: 0F:70:15:0 Giblig von 15:01, 2010 17:31:08 an 14:01, 2013 17:31:08 Zwecke: Clause, Signatu, Yeschlüsseln Verwendung eines Zertlikatsschlüssels: unterzeichne, Non-repudiation, Schlüssel-Verschlüsselung E-Mali Ihelu, reesegikk, adu, CHIENT-CA, OLI-Steinbuch Centre for Computing, O=Karlsruhe Institute of Technology, I-Karlsruhe, ST-Badan-Warrtmberg, C=DE Gespeichert in: Software-Sicherheitsmodul	
OK Abbrechen	

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



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

onten-Einstellungen	
onten-Einstellungen ■ Heko.Reese®kit.edu Server-Einstellungen Kopien & Ordner Verfassen & Adressieren Junk-Filter Synchronisation & Speicherplatz Empfangsbestkitjungen (MDN) S/MIME-Sicherheit ■ Blogs & News Feeds Speicherplatz ■ Local Folders Junk-Filter Speicherplatz Postausgang-Server (SMTP)	S/MIME-Sicherheit Um verschlüsselte Nachrichten zu senden und zu empfangen, solten Sie sowohl ein Zertrifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben. Digitale Unterschrift Folgendes Zertrifikat verwenden, um Nachrichten digital zu unterschreiben: Imported Certrificate Verschlüsselung Folgendes Zertrifikat verwenden, um Nachrichten zu ver- und entschlüsselin: Imported Certrificate Standard-Verschlüsselungseinstellung beim Senden von Nachrichten: Digitale Unterschlüsselung verwenden) Charlen Verschlüsselung verwenden) Zertrifikate Zertrifikat verwenken Kryptographie-tjodule verwalten
Konten-Aktionen •	OK Abbrechen

7 Signieren von E-Mails

7.1 Microsoft Outlook 2003 und 2007

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

Outlook 2003:



Outlook 2007:

		-	Unbe	enannt - Na	chricht (Nur-	Text)		-		
Nachricht	Einfügen				۲					
Einfügen	× <i>K</i> <u>u</u>) = × × A - ≡ =		Adressbuch	Namen überprüfen		Nachver- folgung +	b * 🔛	Rechtschreibung	Sign Encrypt	About
Zwischena 🕞	Basistex	t 🖻	Nam	en	Einsch 🖻	Optionen		Dokumentprüfung	GnuP	G
Senden Betreff:		Nac Di so se Na	hricht digital signier ese Nachricht digital dass andere Persone in können, dass Sie (schricht gesendet ha	en signieren, en sicher diese ben.						
										 ■ ■ ■ ■

7.2 Mozilla Thunderbird 3.0 und 3.1

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

🖙 Verfassen: (kein Betreff)	
Datei Bearbeiten Ansicht Einfügen Format	Einstellungen E≚tras Hilfe
Senden Africa Chitschr O Anhang -	A S/MIME - T Speichern -
Von: Tobias Dussa <tobias.dussa@kit.edu> tobias</tobias.dussa@kit.edu>	Nachricht verschlüsseln
* An: 🔒	
	Sicherheitsinformationen anzeigen
Betreff:	
Normaler Text 🔄 Variable Breite	

8 Verschlüsseln von E-Mails

8.1 Microsoft Outlook 2003 und 2007

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

Outlook 2003:

🟫 Unbena	annt - Nach	richt (Nur	-Text)									
i <u>D</u> atei I	Bearbeiten	Ansicht	Einfügen	Format	E⊻tras	Aktionen	2			-		
i 🖃 Sende	n 🛃 🎒	12 0		0 00	& 🛛	? I	ا 🖄 ا 🔻	💼 Optionen	🚑 🔁	A [‡] ∣a}		
1		-	• <u>A</u>	F K	<u>u</u> 📰	≣ ≣ ;				Nachrichter	und Anlagen	verschlüsseln
A <u>n</u>												
<u> </u>												
Betreff:												
												*

Outlook 2007:



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

8.2 Mozilla Thunderbird 3.0 und 3.1

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

🚔 Verfassen: (kein Betreff)	- · · · · · · · · · · · · · · · · · · ·	
Datei Bearbeiten Ansicht Einfügen Format	Einstellungen Extras Hilfe	
Senden Alf Rechtschr. · 🖉 Anhang •	As S/MIME - Speichern -	
Yon: Tobias Dussa <tobias.dussa@kit.edu> tobias</tobias.dussa@kit.edu>	✓ Nachricht verschlüsseln	•
* Ap: 8	Vachricht unterschreiben	_
	Sicherheitsinformationen anzeigen	
		_
		_
Betreff:		
Normaler Text 💌 Variable Breite		
		<u> </u>

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