# Benutzerhandbuch für die Beantragung und Verwendung von Zertifikaten mit Firefox /Thunderbird

Version 1.2 vom 15.09.2014

Diese Anleitung beruht auf dem Benutzerhandbuch der UH-CA der Leibniz Universität Hannover, das der Universität Hamburg von Frau Gersbeck-Schierholz freundlicherweise zur Verfügung gestellt wurde. Vielen Dank!

Lassen Sie sich vom Umfang dieses Dokumentes nicht abschrecken. Schritt für Schritt werden Sie durch das Beantragungsverfahren geführt, was letztlich nicht mehr als ein paar Minuten in Anspruch nimmt. Anschließend wird Ihnen beschrieben, wie Sie das fertige Zertifikat in Ihre Arbeitsumgebung einbinden. Für diesen Vorgang benötigen Sie ebenfalls nur wenige Minuten.

Im Folgenden soll den Benutzern der Zertifizierungsstelle der Universität Hamburg (UHH-CA) ein Leitfaden zur Zertifikatbeantragung und -verwendung mit Firefox / Thunderbird an die Hand gegeben werden.

Er enthält alle wichtigen Schritte, die zu einem gültigen Zertifikat innerhalb der Zertifizierungshierarchie des Deutschen Forschungsnetzes (DFN) führen.

### Inhaltsverzeichnis

1	Einführung	2
	1.1 Zertifizierungshierarchie	2
	1.2 Das PKI-Portal des DFN	3
	1.3 Die Zertifizierungsrichtlinien der Universität Hamburg	3
2	Import der CA-Zertifikate	5
	2.1 Import der CA-Zertifikate in Firefox	5
	2.2 Import der CA-Zertifikate in Thunderbird	9
3	Beantragen eines persönlichen Nutzer-Zertifikats	.11
3 4	Beantragen eines persönlichen Nutzer-Zertifikats Aufsuchen des Rechenzentrums	.11 13
3 4 5	Beantragen eines persönlichen Nutzer-Zertifikats Aufsuchen des Rechenzentrums Importieren des Zertifikats in den Browser / Mail Klienten	.11 13 14
3 4 5	Beantragen eines persönlichen Nutzer-Zertifikats Aufsuchen des Rechenzentrums Importieren des Zertifikats in den Browser / Mail Klienten 5.1 Importieren in Firefox	. <b>11</b> <b>13</b> <b>14</b> 14
3 4 5	Beantragen eines persönlichen Nutzer-Zertifikats	. <b>11</b> <b>13</b> <b>14</b> 14 16
3 4 5 6	Beantragen eines persönlichen Nutzer-Zertifikats	.11 13 14 14 16

# 1 Einführung

### 1.1 Zertifizierungshierarchie

Für das Signieren und Verschlüsseln von E-Mail erhält jeder Benutzer von der Zertifizierungsstelle der Universität Hamburg (UHH-CA) ein digitales Zertifikat gemäß dem Standard X.509v3 S/MIME, welches seine Identität beschreibt und den öffentlichen Schlüssel enthält. Jedes Zertifikat ist von der ausgebenden Stelle, in diesem Fall der UHH-CA, beglaubigt, die ihrerseits wieder von einer höheren Stelle beglaubigt ist. Das Vertrauenssystem ist streng hierarchisch. Den gemeinsamen Vertrauensanker bildet ein sog. Wurzel-Zertifikat (Root Certificate). Dieses ist das selbstzertifizierte Zertifikat der obersten Instanz der Zertifizierungshierarchie, in unserem Fall das Deutsche Telekom Root CA 2 Zertifikat.

Die folgende Abbildung zeigt die Zertifizierungshierarchie der Universität Hamburg.



### 1.2 Das PKI-Portal des DFN

Das PKI-Portal des Deutschen Forschungsnetzes (DFN) für die Universität Hamburg ist das öffentlich zugängliche Webinterface der UHH-CA. Es ist über den Link oben erreichbar. Alternativ erreichen Sie das PKI-Portal über die RRZ-Webseite

http://www.rrz.uni-hamburg.de/de/services/sicherheit/pki/beantragen-von-zertifikaten/persoenliche-zertifikate.html

Dort wählen Sie den Link "persönliches Zertifikat beantragen".

Im PKI-Portal stehen Ihnen alle wichtigen Funktionen im Zusammenhang mit der Zertifizierung zur Verfügung.



Hier können Sie

- 1. ein Zertifikat beantragen,
- 2. ein Zertifikat zurückrufen und
- 3. Zertifikate suchen.

Desweiteren finden Sie hier

- 1. die Zertifizierungsrichtlinie,
- 2. die CA-Zertifikate und
- 3. die Zertifikat-Sperrlisten.

### 1.3 Die Zertifizierungsrichtlinien der Universität Hamburg

Eine Zertifizierungsrichtlinie (Certification Policy, CP) definiert die Regeln, nach denen eine oder mehrere Zertifizierungsstellen arbeiten. Die in der Universität Hamburg angesiedelte Zertifizierungsstelle (UHH-CA) formuliert ihre Zertifizierungsrichtlinie in der Weise, dass die "Zertifizierungsrichtlinie der Public Key Infrastruktur im Deutschen Forschungsnetz – Global, Classic, Basic" Anwendung findet.

Eine Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) beschreibt die Verfahrensweisen, mit denen eine Zertifizierungsrichtlinie von einer Zertifizierungsstelle umgesetzt wird. Die in der Universität Hamburg angesiedelte Zertifizierungsstelle (UHH-CA) formuliert ihre Erklärungen zum Zertifizierungsbetrieb in der Weise, dass die "Erklärung zum Zertifizierungsbetrieb betrieb der Public Key Infrastruktur im Deutschen Forschungsnetz – Global, Classic, Basic " Anwendung findet.

Der Inhalt beider Dokumente wird an einigen Stellen durch die "Erklärung zum Zertifizierungsbetrieb der UHH-CA in der DFN-PKI" um eigene Spezifikationen erweitert.

CUHH	-CA - Windows Internet Explore	er.		
00	🔹 😰 https://pki.pca.d/n.de/uni-l	namburg-ca/cgi-bin/pub/pii/cmd=getStaticPage;name	-index;id 💌 🔒 😽 🗙 Vahool Search	2.
* *	CHHH-CA		🚯 • 🗟 · 🖶 • 🔂 s	ite • 🕥 Extras •
Zer	ttifikate CA-Zertifikat	Hamburg te Gesperite Zertlfikate Po render-Policy	ides Hilfe Beenden	
	Schi Hier könne	nittstelle für Nutzer und Admir n Sie die Policy der DFN-PKI un herunterladen.	<b>istratoren - Policies</b> d Ihrer Zertifizierungsstelle	

Mit Hilfe der Zertifizierungsrichtlinien ist es für jeden Teilnehmer möglich, eine Einschätzung über die Qualität der ausgestellten Zertifikate zu treffen. Sie beschreiben die Mindestanforderungen und Abläufe der Zertifizierung und sind Teil der Vereinbarung zwischen der CA und den Benutzern. Daher sollte jeder, der ein Zertifikat der UHH-CA beantragen will, diese Richtlinien genau studieren.

## 2 Import der CA-Zertifikate

Bevor Sie Ihr persönliches Zertifikat beantragen, installieren Sie bitte per Mausklick die CA-Zertifikate der Zertifizierungshierarchie in Ihren Browser (Firefox) und E-Mail Klienten (Thunderbird) wie unten beschrieben.

#### 2.1 Import der CA-Zertifikate in Firefox

Weil es sich bei der Kombination Firefox/Thunderbird um zwei verschiedene Programme handelt, haben beide einen eigenen Zertifikatspeicher. Daher müssen die CA-Zertifikate in beide Programme eingebaut werden. Die Zertifikate werden zunächst per Mausklick in den Firefox Browser importiert. Dort wird ein Backup auf Diskette oder einen anderen externen Datenträger erstellt, anschließend werden die Zertifikate in Thunderbird importiert.

UHH-CA -	Nozilla Firefox	
yatei Bearbei	ten Ansicht Shronik Lesezeichen Extras Ulife	0
🍋 • 🛸 •	🕐 🕑 🕜 🏠 🗋 https://pki.pca.din.de/uni-hamburg-ca/cgi-bin/pub/pki?cmd=getStaticPage;name= 🖻 🔹 💌 💽 G= Google	Q.)
Erste Schritt	e 🔂 Aktuelle Nachrichten	
UH 2 ortifik	Universität Hamburg	
Murral	antifikat DEN-DCA Zertifikat LEEH-CA Zertifikat Zertifikat	0701000
THURLEN	Tourist Louis and Louis an	in a crigiciti
	• Wählen Sie "Wurzelzertifikat", "DFN-PCA Zertifikat" bzw. "UHH-CA Zertifikat" um das jeweilige Zertifikat in Ihrem Browser zu installieren.	
-		>
rtig		pki.pca.dfn.de 🕍
	aladan dan Zastifikata	
lerunt	erladen des Zertifikats	
<mark>-lerunt</mark> Sie wur	e <mark>rladen des Zertifikats</mark> den gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.	X
Herunt Sie wur Möchte	<b>erladen des Zertifikats</b> den gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen. n Sie "Deutsche Telekom Root CA 2" für die folgenden Zwecke vertrauen?	

Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien

OK

Abbrechen

Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.

und Prozeduren (wenn vorhanden) überprüfen.

Ansicht

CA-Zertifikat überprüfen

Dieser CA vertrauen, um Software-Entwickler zu identifizieren.

Klicken Sie als erstes unter dem Reiter **CA-Zertifikate** auf den Reiter **"Wurzelzertifikat"**. Dadurch wird das Wurzelzertifikat der Deutschen Telekom Root CA 2 in Ihren Browser importiert.

Zunächst aber öffnet sich das nebenstehende Fenster. Dort sollte als erstes der rot umrandete Button **Ansicht** betätigt werden, um den Inhalt des Zertifikates zu prüfen.



runterladen des Zertifikats
ie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.
löchten Sie "Deutsche Telekom Root CA 2" für die folgenden Zwecke vertrauen?
🗹 Dieser CA vertrauen, um Websites zu identifizieren.
Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.
Dieser CA vertrauen, um Software-Entwickler zu identifizieren.
ے۔ ievor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien ınd Prozeduren (wenn vorhanden) überprüfen.
Ansicht CA-Zertifikat überprüfen
OK Abbrechen



Da die CA-Zertifikate dem Browser nicht bekannt sind, werden sie auch noch nicht als vertrauenswürdig eingestuft.

In diesem Fenster Zertifikat Ansicht sind die wichtigsten Informationen zu jedem Zertifikat enthalten: Unter Herausgegeben für wird der Inhaber des Zertifikates angezeigt, in diesem Fall die Deutsche Telekom Root CA 2. Unter Herausgegeben von derjenige, der das Zertifikat unterzeichnet hat, hier wieder die Deutsche Telekom Root CA 2, da es sich um ein selbstsigniertes Wurzelzertifikat handelt. Es folgt der Gültigkeitszeitraum, in dem das Zertifikat verwendet werden kann. Zuletzt werden die Prüfsummen (Fingerabdrücke) des Zertifikates angezeigt.

Die angezeigten Fingerabdrücke sollten Sie mit den Angaben in diesem Dokument bzw. in einem anderen gedruckten Dokument der UHH-CA abgleichen.

Nach dem Schließen des Anzeigefensters müssen jeweils die Zwecke des Zertifikates aktiviert werden, um es für die angegebenen Anwendungen als vertrauensvoll einzustufen.

Bestätigen Sie danach mit **OK** und das Zertifikat wird in den Browser installiert.

Klicken Sie dann auf den Reiter "**DFN-PCA Zertifikat**". Dadurch wird das Zertifikat der DFN-Verein PCA Global in Ihren Browser importiert, nachdem Sie auch hier die Vertrauenswürdigkeit durch Aktivieren der Kontrollkästchen bestätigt haben.



Web-Suche

Downloads Add-ons

Fehler-Konsole

DOM Inspecto

Schnittstelle für Nutzer und Administratoren - CA-Zertifikate Hier können Sie das Wurzelzertifikat, das DFN-PCA Zertifikat das CA-Zertifikat in Ihrem Browser installieren oder alle Zertifikate in einer Datei spelchem.

an Private Da

Strg+k

Strg+J

Strg+Umschalt+I

UHH-CA - Mozilla Firefox

UHH

P Erste Schritte 🔂 Aktuelle Nachrichten

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

🖁 Universität Han

👍 • 🗼 • 🧭 🕓 🏠 🗋 https://pki.pc

Zertifikate CA-Zertifikate

Zuletzt klicken Sie auf den Reiter **"UHH-CA Zertifikat**". Dadurch wird das Zertifikat der CA der Universität Hamburg in Ihren Browser importiert, nachdem Sie auch hier die Vertrauenswürdigkeit durch Aktivieren der Kontrollkästchen bestätigt haben.

Zur Überprüfung, ob die CA-Zertifikate korrekt importiert worden sind, wählen Sie im Firefox-Menü unter **Extras** den Punkt **Einstellungen**.

▶ **G**• 6

ilfe Beenden

pki.pca.dfn.de 🙆

Hier öffnet man unter **Erweitert, Reiter Verschlüsselung,** den Button **Zertifikate anzeigen** mit dessen Hilfe man in den Zertifikats-Manager gelangt.



hre Zertifikate Zertifikate anderer Per	sonen Websites Zertifizierungsstellen	
Sie haben gespeicherte Zertifikate, d	ie diese Zertifizierungsstellen identifizieren:	
Zertifikatsname	Kryptographie-Modul	C.
Secure Certificate Services	Builtin Object Token	^
Trusted Certificate Services	Builtin Object Token	
DFN-Verein		
UHH CA - G02	Software-Kryptographie-Modul	
Deutsche Telekom AG	7	
DFN-Verein PCA Global - G01	Software-Kryptographie-Modul	
-Deutsche Telekom Root CA 2	Software-Kryptographie-Modul	
DigiCert Inc		
-DigiCert Assured ID Root CA	Builtin Object Token	_
-DiniCert Global Root CA	Builtin Ohiert Token	~
Ansicht Bearbeiten Im	portieren	

Wählen Sie den Reiter Zertifizierungsstellen aus. Hier sollte sich jetzt unter der Überschrift Deutsche Telekom AG das Zertifikat der Deutschen Telekom Root CA 2 und der DFN-Verein PCA Global-G01 befinden und darüber unter der Überschrift DFN-Verein das Zertifikat der UHH CA – G02.

#### Damit sind die CA-Zertifikate der Zertifizierungshierarchie in Firefox installiert.

Um die CA-Zertifikate auch in Thunderbird verfügbar zu machen, müssen sie zunächst auf der Festplatte oder einem externen Datenträger zwischengespeichert werden. Da Sie aber Ihr eigenes Zertifikat unbedingt auf einem externen Datenspeicher zur Aufbewahrung sichern sollten, bietet es sich an, die CA-Zertifikate ebenfalls auf diesem externen Datenträger (z.B. auf Diskette, CD oder USB-Stick) zu speichern:

😂 UHH-CA - Mozilla	Firefox	
Datei Bearbeiten An	sicht Chronik Lesezeichen Eztras Hilfe	0
🍬 • 🔶 • 🕑	🕜 🏠 🗋 https://pki.pca.dfn.de/uni-hamburg-ca/cgi-bin/pub/pki?cmd=getStat 🙆 🔹 🕨 🔀 Coogle	Q.)
🗭 Erste Schritte 🔝 Ak	tuelle Nachrichten	
Zertifikate	niversität Hamburg CA-Zertifikate Policies Hilfe Beenden	
Wurzelzertifi	ent DEDLECA Zertifikat UHH-CA Zertifikat Zertifika Unkinneuen geböffnen Unkinneuen geböffnen	atkette anze
(	Zel geschen und des ruch auf der Geschen und d	
CA	Ung-Adresse kopieren hstallieren oder alle Zertifikate in einer	
	Egenschaften	
<		2
< Fertig		pki.pca.dfn.de

Klicken Sie auf im PKI-Portal (Reiter CA-Zertifikate) das **Wurzelzertifikat** mit der rechten Maustaste an und wählen Sie **Ziel speichern unter...**.

Speichern unte	90			2 🛛
Spejchern in:	🗢 Wechseld	atenträger (F:)	💌 🧿 🗊 🖻	
Zuletzt verwendete D	Documents			
Desktop Eigene Dateien				
Arbeitsplatz				
	Datei <u>n</u> ame:	g_rootcert	×	Speichern
Netzwerkumgeb	Dateityp:	Sicherheitszertifikat	*	Abbrechen

Legen Sie eine Diskette in das Laufwerk und **speichern** Sie dort das Zertifikat oder speichern Sie es auf einem anderen externen Datenträger.

Verfahren Sie ebenso mit dem DFN-PCA Zertikat und dem UHH-CA Zertifikat!

### 2.2 Import der CA-Zertifikate in Thunderbird

Jetzt installieren Sie die CA-Zertifikate in Ihren Mail Klienten Thunderbird. Öffnen Sie das Programm und gehen Sie im Menü unter **Extras** zu **Einstellungen**. Es öffnet sich folgendes Fenster:

Thunder bird-Einstellungen         Allgemein         Ansicht       Verfassen         Datenschutz       Anhänge         Erweitert         Allgemein       Netzwerk & Speicherplatz         Update       Zertifikate         Verwalten der Sicherheitskomponenten:       Zertifikate         Zertifikate       CRLS         QCSP       Kryptographie-Module         OK       Abbrechen	Dort klicken Sie unter Erweitert im Reiter Zertifikate auf den Button Zerti- fikate (je nach Thunderbird Version kann sich dieser auch unter Daten- schutz im Reiter Sicherheit befinden).
Zertifikat-Manager   Ihre Zertifikate Zertifikate   Ihre Zertifikate Zertifikate   Sie haben gespeicherte Zertifikate, die diese   Zertifikatsname Kryptographie-Modul   Autoridad de Certificacion Firmapro   Builtin Object Token ABA.ECOM, INC.   ABA.ECOM Root CA Builtin Object Token   AC Camerfirma SA CIF A82743287 Chambers of Commerce Root   Global Chambersign Root Builtin Object Token   Ansicht Bearbeiten   Importieren Löschen	Sie gelangen in den Zertifikat Mana- ger. Unter dem Reiter <b>Zertifizierungs- stellen</b> wählen Sie <b>Importieren</b> .
Wählen Sie die Datei mit dem oder den zu importierenden CA-Zertifikat(en)       Image: Composition of the second sec	Markieren Sie das zuvor gespeicherte Wurzelzertifikat <b>g_rootcert.crt</b> und ge- hen Sie auf <b>Öffnen</b> .

erunterlader	ı des Zertifikats			
Sie wurden gebe	eten, einer neuen Zertifizierun	igsstelle (C	A) zu vertrauen.	
Möchten Sie "De	utsche Telekom Root CA 2" fü	ùr die folge	nden Zwecke vertrauer	17
Dieser CA v	ertrauen, um Websites zu ide	ntifizieren.		
🗹 Dieser CA v	ertrauen, um E-Mail-Nutzer zu	u identifizie	ren.	
Dieser CA v	ertrauen, um Software-Entwi	ckler zu ide	ntifizieren.	
und Prozeduren	(wenn vorhanden) überprüfe CA-Zertifikat überprüfen	n.	ОК	Abbrechen
7ortifikat.N	anager			
Certifikat-in				

Vertrauen Sie der Zertifizierungsstelle, indem Sie die drei Haken setzen. Drücken Sie **OK**. Das Zertifikat wird in Thunderbird importiert.

Wiederholen Sie den Vorgang mit den beiden anderen CA-Zertifikaten **g\_intermediatecacert.crt** und **g\_cacert\_crt!** 

Anschließend...

...finden Sie die CA-Zertifikate im Zertifikat-Manager von Thunderbird unter dem Reiter Zertifizierungsstellen.

nre Zertifikate Zertifikate anderer Perso	onen Websites Zertifizierungsstellen	
Sie haben gespeicherte Zertifikate, die	diese Zertifizierungsstellen identifizieren:	
Zertifikatsname	Kryptographie-Modul	EŞ.
DFN-Verein	Builtin Object Token	<ul> <li>Image: A state of the state of</li></ul>
Deutsche Telekom AG	Sortware-Kryptographie-Modul	
DFN-Verein PCA Global - G01 Deutsche Telekom Root CA 2	Software-Kryptographie-Modul Software-Kryptographie-Modul	~
Ansicht Bearbeiten Impo	Sortware-Krypcographie-Modul	

### 3 Beantragen eines persönlichen Nutzer-Zertifikats

Für die Beantragung Ihres persönlichen Nutzer-Zertifikates, wählen Sie im PKI-Portal des DFN unter dem Reiter **Zertifikate** den Punkt **Nutzerzertifikat** aus, der zum folgenden Fenster führt.



Füllen Sie bitte den Antrag mit Ihren Daten aus und wählen Sie **Weiter**.

Unter **Zertifikatdaten** werden die Daten erfasst, die in das Zertifikat mit aufgenommen werden. Jedes Zertifikat beinhaltet u.a. einen eindeutigen Namen (Distinguished Name, DN). Dieser wird von den Feldern **E-Mail, Name** und **Abteilung** zusammen mit den festgelegten Einträgen O=Universitaet Hamburg und C=DE gebildet.

Geben Sie auch eine PIN ein und bestätigen Sie diese noch einmal, stimmen Sie der Zertifizierungsrichtlinie zu und stimmen Sie bitte unbedingt auch einer Veröffentlichung Ihres Zertifikates zu. Nur wenn Sie der Veröffentlichung zustimmen, ist Ihr Zertifikat später über den Button "Zertifikate suchen" zu finden und Sie sind damit für andere Teilnehmer nachvollziehbar vertrauenswürdig. Genauso aber werden Sie auch andere Teilnehmer als vertrauenswürdig einstufen können, wenn diese Ihr Zertifikat veröffentlicht haben zugestimmt haben.









Wenn alle Angaben korrekt sind, bestätigen Sie mit **Bestätigen**.

Wenn Sie noch keine Zertifikate in Firefox verwalten, müssen Sie ein Master-Passwort für den internen Schlüsselspeicher wählen. Dieses wird später jeweils vor dem Verwenden oder Exportieren eines privaten Schlüssels abgefragt. Weiter geht es mit **Ok**.

Firefox veranlasst nun die Generierung Ihres Schlüsselpaares auf Ihrem Rechner. Privater und öffentlicher Schlüssel ermöglichen später im Zusammenhang mit dem Zertifikat das Unterschreiben und Verschlüsseln von E-Mail.

Anschließend werden Sie aufgefordert, sich den Zertifikatantrag auszudrucken.

### 4 Aufsuchen des Rechenzentrums

Sind alle Angaben auf dem Ausdruck korrekt, unterschreiben Sie ihn und suchen Sie nach telefonischer Absprache die Registrierungsstelle im RRZ (UHH-RA) auf.

Regionales Rechenzentrum der Universität Hamburg Schlüterstraße 70 20146 Hamburg

Hr. J. Baftijari Raum 417 Telefon: 040 - 42838 4625

Hr. R. Kurtz Raum 408 Telefon: 040 - 42838 7977

Terminabsprachen sind für den Vertretungsfall auch unter -3097 (Herr Dr. C. Benecke).

#### Folgendes ist mitzubringen

- 1. Der vollständig ausgefüllte Zertifikatantrag,
- 2. der Personalausweis oder Pass,
- 3. ein Dokument, das die Zugehörigkeit zur Universität bestätigt.

Wenn Sie den Mitarbeitern persönlich bekannt sind, kann auf das Dokument über die Zugehörigkeit (3.) verzichtet werden.

#### Prüfung und Beglaubigung des Zertifikatantrages

Nach Kontrolle des Zertifikatantrages wird dieser beglaubigt von der RA an die CA weitergeleitet. Dort wird das Zertifikat erstellt und Sie erhalten umgehend eine Benachrichtigung per E-Mail.

### 5 Importieren des Zertifikats in den Browser / E-Mail Klienten

#### **5.1 Importieren in Firefox**

Nachdem die UHH-CA Ihr Zertifikat erstellt hat, erhalten Sie eine E-Mail vom PKI-Team der Universität Hamburg...

Datei Bearbeiten Ansicht Navjgation Nachricht Extras Hill	e 0
Artworten Allen antworten Weil	erfeten Schlagwörter Löschen Jurk Drucken 2000 - 😡 -
Betreff: UHH CA Zertifikatinformation	Von: uhh-ca@uni-hamburg.de 17.09.2007 13:40
Sehr geehrte Nutzerin, sehr geehrter Nutzer,	
lie Bearbeitung Ihres Zertifizierungsantrage	) ist nun abgeschlossen.
Ihr Zertifikat mit der Seriennummer 18546000	)7 ist auf den Namen OleKommunikationsnatze Gelleiversitaat
Hamburg, L=Hamburg, ST=Hamburg, C=DE	
erstellt worden und im Anhang dieser Mail be	sigelegt.
Sie benötigen die Seriennummer, um Ihr Zert:	fikat gegebenenfalls sperren zu können.
Um Ihr Zertifikat nutzen zu können, müssen S	die alle folgenden Zertifikate in
Ihren Browser importieren. Achten Sie daraut	1, dass Sie die Zertifikate auf dem
Rechner importieren, von dem aus Sie den Ant	rag gestellt haben, weil sich dort
der zugehörige Schlüssel befindet.	
1. Für die CA-Zertifikate wählen Sie bitte o	tie Seite
https://pki.pca.dfn.de:443/uni-hamburg-ca/co	ji-bin/pub/pki?cmd=getStaticPage;name=index;id=2
und folgen den Anweisungen.	
2. The eigenes Zertifikat erhalten Sie direl	st über folgenden Link:
or and degener destruction consistent over sites	to men avagemen bannt
https://pki.pca.dfn.de:443/uni-hamburg-ca/co	<pre>yi-bin/pub/pki?cmd=getcert&amp;key=185460007&amp;type=CERTIFICATE</pre>
Nit freundlichen Grüßen	
UHH CA	
80	
cert-185460007 nem	
and the mean from	

... mit der Information, dass Sie Ihr Zertifikat nun abholen können. Es reicht ein Mausklick auf den markierten Link, um Ihr persönliches Zertifikat in Ihren Browser zu integrieren.

Ihr Zertifikat ist außerdem noch als PEM-Datei als Anlage der E-Mail beigefügt (in diesem Format müssen die Sie es aber nicht nutzen).

CHIFT-CA - MOZITIA FIFETOX		
Datei Bearbeiten Ansicht Ghronik Lesezeichen	Egtras Hife	4
🦛 - 📄 - 🧖 🖓 🎊 🗋 https://pki.pc	Web-Syche Strg+K	G - Google
P Erste Schritte 🔝 Aktuelle Nachrichten	Downloads Strg+J Add-ons	
UHH ata	Fehler-Konsole DOM Igspector Strg+Umschalt+I Seiteninformationen	
Universität Har	Private Daten löschen Strg+Umschalt+Entl	
	En overhunden un	
Zertifikate CA-Zertifikate G	esperrte Zertifikate   Policies	Hilfe Beenden
Zertifikate         CA-Zertifikate         G           Nutzerzertifikat         Serverzer	esperrte Zertifikate   Policies tifikat   Zertifikat sperre	n Zertifikat suchen
Zertifikate CA-Zertifikate G	esperrte Zertifikate   Policies tifikat   Zertifikat sperre Laden des beant	Hilfe Beenden n Zertifikat suchen tragten Zertifikats
Zertifikate CA-Zertifikate G	esperrte Zertifikate   Policies tifikat   Zertifikat sperre Laden des beant n, um Ihr Zertifikat in Ihren B	THIIfe Beenden N Zertifikat suchen Stragten Zertifikats Krowser zu
Zertifikate CA-Zertifikate G Nutzerzertifikat Serverzer Benutzen Sie den Buttor Importieren.	esperrte Zertifikate   Policies tifikat   Zertifikat sperre Laden des beant n, um Ihr Zertifikat in Ihren B	n Zertifikat suchen ragten Zertifikats rowser zu

Nachdem Sie das Zertifikat in Firefox importieren haben, sollten Sie ein Backup für Thunderbird machen, denn hier wollen Sie es ja hauptsächlich für das Signieren und Verschlüsseln von E-Mail benutzen. Gehen Sie bitte im Programm Firefox, Menü **Extras,** auf **Einstellungen.** 

Wählen Sie unter **Erweitert** den Reiter **Verschlüsselung**. Drücken Sie den Button **Zertifikate anzeigen**.





### 5.2 Importieren in Thunderbird

Um Ihr persönliches Zertifikat in den Zertifikatspeicher von Thunderbird zu importieren, öffnen Sie das Programm und wählen unter **Extras** den Punkt **Einstellungen**.



Master-Passwort ändern 🛛 🛛 🔀						
Kryptographie-Modul: Software-Kryptographie-Modul						
Aktuelles Passwort:	(nicht festgelegt)					
Neues Passwort:	*****					
Neues Passwort (nochmals):	*****					
Passwort-Qualitätsmessung						
OK Abbrechen						

X

Abbrechen

Wenn Sie noch keine Zertifikate in Thunderbird benutzt haben, werden Sie aufgefordert, ein Master-Passwort für den Zertifikatspeicher von Thunderbird zu wählen. Dieses wird später für den Zugriff auf den Schlüssel beim Signieren und Entschlüsseln von Mails abgefragt. Nach zweimaliger Eingabe des Passworts bestätigen Sie mit **OK**.

Geben Sie das von Ihnen beim Exportieren auf Firefox vergebene **Backup-Passwort** an und wählen Sie **OK**.



OK

Passworteingabe-Dialog

Passwort: \*\*\*\*\*\*\*

Bitte geben Sie das Passwort ein, das verwendet wurde, um dieses Zertifikats-Backup zu verschlüsseln.

Bestätigen Sie mit OK.

Ihr eigenes Zertifikat wurde in den Zertifikatspeicher von Thunderbird importiert.

re Zertifikate	Zertifikate a	nderer Personen	Websites	Zertifizierungsstell	en	
Zertifikatsna	me Krypt	ographie-Modul	Zwecke	Seriennummer	Läuft ab am	E,
Universitae	t lert Softwa	are-Kryptograp	Client,U	. 0B:0D:E5:27	16.09.2010	
Ansicht	Backup	B <u>a</u> ckup v	on allen	Importieren	Löschen	

## 6 Sicherungskopie des privaten Schlüssels

#### Verwahren Sie den externen Datenträger mit den Zertifikaten an einem sicheren Ort!

Die Datei, welche Sie dort vorhalten, beinhaltet nicht nur Ihr Zertifikat, sondern auch Ihren privaten Schlüssel. Der private Schlüssel wird zusammen mit dem Zertifikat vom System für das Signieren von E-Mail und für das Entschlüsseln von an Sie verschlüsselt gesendete Mails eingesetzt. Er muss deshalb geschützt werden! Bei Missbrauch durch Dritte ist das Zertifikat hinfällig! Mit einer Kopie des Schlüssels kann der Angreifer eine falsche Identität vortäuschen und vertrauliche Daten entschlüsseln.

Ihre Anwendungen Firefox und Thunderbird speichern außerdem den privaten Schlüssel in einer Software-PSE (Private Security Environment). Hierbei handelt es sich um einen passwortgeschützten, sicheren Bereich. So steht Ihnen komfortabel und sicher die Signier- und Verschlüsselungsfunktionalität von Mozilla Thunderbird jederzeit zur Verfügung.

### 7 Versenden einer signierten E-Mail

Mit Ihrem Zertifikat können Sie nun E-Mails, die Sie versenden, digital signieren. Damit kann der Empfänger sicher sein, dass es sich wirklich um eine E-Mail von Ihnen handelt. Das Verund Entschlüsseln von E-Mails wird in der Anleitung zum Einrichten des LDAP-Verzeichnisdienstes beschrieben. Zum Signieren einer E-Mail erstellen Sie diese wie gewohnt mit Thunderbird. Vor dem Absenden...

숙 Verfassen: Signierte Em	ail		klicken Sie auf den kleinen Pfeil
Datei         Bearbeiten         Anskht           Senden         Kontakte         Rechtsche           Yon:         Olaf Gellert         - Olaf Gellert	Enfügen Format Enstellungen Extras Hilfe	0	nach unten im Button <b>SMIME.</b> In dem erscheinenden Menü wählen Sie den Eintrag <b>Nachricht unterschreiben</b> .
An: and Claf Gel Betreff: Signierte Email Normaler Text: Variable Eine signierte Email	ert <olaf geller<br="">Nachricht ynterschreiben Sicherheitsinformationen anzeigen Breite ↓ A* A* B / U I III 12 € €</olaf>	2 <b>2 • 2 •</b> 0 •	J
		1) 195	
Thunderbird Sie müssen ein oder verwenden können.	mehrere persönliche Zertifikate einrichten, bevor Sie diese Sich Möchten Sie dies jetzt machen? 23 Nein	erheitsfunktion	Wenn Sie noch keine signierten E- Mails verschickt haben, fragt Thunder- bird, ob Sie Ihr Zertifikat einrichten wol Ien. Wählen Sie <b>Ja</b> .
Konton  Control Cellert  Server-Einstelungen Kopien & Ordner Verfassen & Adressieren Offine & Speicherplatz -Junk-Filter Einsforlangebeskälsungen Us/Mit/Eischerher Einsforlangebeskälsungen Us/Mit/Eischerher Postausgang-Server (SMTP)  Konto bjezufügen Ak Standard (estegen	S/MIME-Sicherheit Un verschlüsselen Nachrichten zu senden und zu englangen, sollen Sie sowol Verschlüsselung als auch eines für digitale Unterschrift angeben. Obglabe Unterschrift Folgendes Zertifikat zum Absenden digital unterschriebener Nac Verschlüsselung Folgendes Zertifikat verwenden, um Nachrichten zu ver- und ertschlüsselung Folgendes Zertifikat verwenden, um Nachrichten zu ver- und ertschlüsselung Sandard-Verschlüsselung verwenden) Netschlüsselung beim Senden von Nachrichten: Die (denne Verschlüsselung verwenden) Zertifikate um dirsptographie-Module verwelen Zertifikate Eryptographie-Module	N en Zertfiket for	Im Dialogfeld wählen Sie unter <b>Digita- le Unterschrift</b> den Button <b>Auswäh- len</b> .
Konto entfernen		K Abbrechen	



Betreff: Signierte Email..

Eine signierte Email ...



Wenn Sie eine signierte E-Mail empfangen, wird Ihnen dies symbolisch in der Kopfzeile der E-Mail angezeigt. Wenn Sie das Symbol anklicken...

... wird der genaue Status der Signatur angezeigt.