Benutzerhandbuch für die Zertifizierung mit dem Internet Explorer

Version 1.0 vom 10.10.2007

Im Folgenden soll den Benutzern der Zertifizierungsinstanz der Universität Hamburg, der UHH-CA, ein Leitfaden zur Zertifikatbeantragung und -verwendung mit dem Internet Explorer an die Hand gegeben werden. Er enthält alle wichtigen Schritte, die zu einem gültigen Zertifikat innerhalb der Zertifizierungshierarchie des Deutschen Forschungsnetzes (DFN) führen.

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.

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!

Inhaltsverzeichnis

1 Zur 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
3 Beantragen eines persönlichen Nutzer-Zertifikates	11
4 Aufsuchen des Rechenzentrums	15
5 Antwort E-Mail und Zertifikat in den Browser importieren	16
6 Sicherungskopie des privaten Schlüssels	17
7 Wichtiger Hinweis zum Einstellen der Sicherheitsstufe	21

1 Zur Einführung

1.1 Zertifizierungshierarchie

Für das Signieren und Verschlüsseln von E-Mail kann jeder Universitätsangehörige (Studierende, Mitarbeiter) 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 die 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 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/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

- ein Zertifikat beantragen,
- ein Zertifikat zurückrufen und
- Zertifikate suchen.

Desweiteren finden Sie hier

- die Zertifizierungsrichtlinie,
- die CA-Zertifikate und
- 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 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 - V	Vindows Internet Explorer	- • 🛛
G - [🔊 https://pki.pca.dfn.de/uni-hamburg-ca/cgi-bin/pub/pki7cmd=getStaticPage;name=index;id 💌 🔒 🚱 🔀 [Yahool Search	P -
* * 🏉	unn-ca 💁 🖬 🗧 🖶 🕯 Sobo	• 🎯 Extras • 🎇
Zertifik DFN-PK	Universität Hamburg ate CA-Zertifikate Gesperte Zertifikate Policies Hilfe Beenden	=
	Schnittstelle für Nutzer und Administratoren - Policies Hier können Sie die Policy der DFN-PKI und Ihrer Zertifizierungsstelle herunterladen.	
<	Thermet	100% •

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 Ihre Arbeitsumgebung wie unten beschrieben.



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.



Es öffnet sich das nebenstehende Fenster. Wählen Sie **Öffnen**.



Zertifikatsimport-Assistent		X
To have	Willkommen	
	Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatsvertrauenslisten und -sperrlisten vom Datenträger in den Zertifikatspeicher.	
	Ein Zertifikat wird von einer Zertifizierungsstelle ausgestellt und dient der Bestätigung Ihrer Identität. Zertifikate enthalten Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich in dem Zertifikate gespeichert werden.	
	Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.	
	< <u>Zurück</u> <u>Weiter</u> > Abbreche	n

Das Zertifikat wird importiert. Wählen Sie Weiter.

Wählen Sie Zertifikat installieren.

Zertifikatsimport-Assistent	×
Zertifikatspeicher Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert	
Windows kann automatisch einen Zertifikatspeicher auswählen oder Sie können einen Pfad für die Zertifikate angeben.	
 Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend) 	
Alle Zertifikate in folgendem Speicher speichern	
Zerdrikatspeichen:	
< <u>Z</u> urück <u>Weiter</u> > Abbrechen)

Wählen Sie Zertifikatspeicher automatisch wählen und dann **Weiter**.

Zertifikatsimport-Assistent		\mathbf{X}
	Fertigstellen des Assistenten	
	Der Zertifikatsimport-Assistent für die wurde erfolgreich abgeschlossen.	
	Sie haben folgende Einstellungen ausgewählt:	
	Gewählter Zertifikatspeicher Auswahl wird vom Assisten Inhalt Zertifikat	
		_
	Zurück Fertig stellen Abbrecher	ī

Wählen Sie Fertig stellen.

Zertifikatsimport-Assistent

Der Importvorgang war erfolgreich.

OK

Bestätigen Sie mit OK.



Klicken Sie dann im PKI-Portal auf den Reiter **"DFN-PCA Zertifikat**". Dadurch wird das Zertifikat der DFN-Verein PCA Global in Ihren Browser importiert, nachdem Sie auch hier dem Installationsvorgang gefolgt sind wie oben für das Wurzelzertifikat im Detail beschrieben.



Verfahren Sie zuletzt ebenso mit dem Reiter **"UHH-CA Zertifikat"**. Dadurch wird das Zertifikat der CA der Universität Hamburg in Ihren Browser importiert, nachdem Sie auch hier dem Installationsvorgang gefolgt sind wie oben für das Wurzelzertifikat im Detail beschrieben.

🖉 UHH-CA - Windows Internet Explorer		
🔄 🕞 👻 👔 https://pki.pca.dfn.de/uni-hamburg-ca/cgi-bin/pub/pki	Yahoo! Sea	arch 🖉 🗸
😤 🛠 🌈 UHH-CA	👌 • 🔊 · (🖶 🔹 🔂 Seite 🔹 🎯 Extras 🔹 🍟
	Browserverlauf	löschen
	Popupblocker Phishingfilter Add-Ons verwa	alten
Universität Hamburg	Offinebetrieb	
Zertifikate CA-Zertifikate Gesperrte Zertif	Windows Updat Vollbid kate Po Symbolleisten	F11
Nutzerzertifikat Serverzertifikat Ze	Windows Messe Diagnose von V	enger 'erbindungsproblemen
	Internetoptione	:n
Willkommen bei der "CA der	Iniversität Hamburg	"
Bitte wählen Sie eine	Funktion aus.	

Nach der Installation der Zertifikate wird nun überprüft, ob diese richtig im Internet Explorer hinzugefügt wurden. Dazu öffnet man im Internet Explorer unter **Extras** die **Internetoptionen**.



Wählen Sie unter dem Reiter Inhalte Zertifikate aus.

Zertifikate			? 🗙
Beabsichtigter Zweck: <alle></alle>			~
Zwischenzertifizierungsstellen Vertrauenswi	ürdige Stammzertifizierungs	stellen Vertr	aute I 🔸 🕨
Ausgestellt für	Ausgestellt von	Gültig bis	Ang 🔨
Beutsche Telekom Root CA 1	Deutsche Telekom Ro	10.07.19	Deu
Deutsche Telekom Root CA 2	Deutsche Telekom Ro	10.07.19	Deu
DFN Toplevel Certification Authority	DFN Toplevel Certifica	31.01.10	DFN
DFN-Verein PCA Classic - G01	DFN-Verein PCA Class	28.04.13	DFN
🖼 DigiCert Assured ID Root CA	DigiCert Assured ID R	10.11.31	Digi
🖼 DigiCert Global Root CA	DigiCert Global Root CA	10.11.31	Digi
🖼 DigiCert High Assurance EV Root CA	DigiCert High Assuran	10.11.31	Digit
🖼 DigiNotar Root CA	DigiNotar Root CA	31.03.25	Digil 🤜
			>
Importieren) Exportieren) Entfernen		E	r <u>w</u> eitert
Beabsichtigte Zwecke des Zertifikats			
Sichere E-Mail, Serverauthentifizierung			zeigen
			<u>S</u> chließen

Unter dem Reiter Vertrauenswürdige Stammzertifizierungsstellen sollte das Zertifikat der Deutschen Telekom Root CA 2 stehen.

Unter **Anzeigen** können Sie sich die Zertifikatsinformationen anzeigen lassen.



Unter dem Reiter **Zwischenzertifi**zierungsstellen finden Sie das Zertifikat des **DFN-Verein PCA Global – G01** und das Zertifikat der **UHH CA – G02** Mit dem Button **Anzeigen** können Sie sich die Zertifikatsinformationen ansehen.





Fingerabdruck der DFN-Verein PCA Global

3 Beantragen eines persönlichen Nutzer-Zertifikates

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 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 der Veröffentlichung ihres Zertifikats zugestimmt haben.



۰.	Windows Internet	Explorer			Wonn
• [🔊 https://pki.pca.dfr	.de/uni-hamburg-ca/cgi-bin/pub/pki	💌 🔒 🐓 🗙 Yahoo! Search	P •	vvenn
Ø	UHH-CA		🟠 • 🔂 · 🖶 • 🗗 s	sjte • 🕥 Extyras • 🎇	tigen
H	ti Univers	sität Hamburg		Deut Forsc	U
i fik erz	cate CA-Zer certifikat	tifikate Gesperrte Zertif Serverzertifikat Ze	ikate Policies Hilfe Beenden ertifikat sperren Zertifikat suchen		
			Nutzerzertifikat beantragen - Bestätige	n	
	Die folgend	len Daten wurden eingetra	gen:		
		Zertifikatdaten E-Mail Name Abteilung 1 (optional) Abteilung 2 (optional) Weröffentlichen Erweitet Oppionen>>	Olaf, Gellert@rrz.uni-hamburg.de Olaf Gellert Regionales Rechenzentrum Kommunikationsnetze Ja		

u 😜 🥫

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

Wenn alle Angaben korrekt sind, **bestä**tigen Sie.

 Mögliche Skriptingverletzung
 Image: Second Sec

Ändern Bestätigen

Bestätigen Sie mit JA.

Ein neuer RS/	A-Austauschschlüssel wird erstellt. 🛛 🛛 🚺
	Eine Anwendung erstellt ein geschütztes Objekt.
	Privater Schlüssel des Cry
	Sie haben die mittlere Sicherheitsstufe gewählt OK Abbrechen Details

Im Dialog "Ein neuer RSA-Austauschschlüssel wird erstellt" sollte zunächst die Sicherheitsstufe eingestellt werden: Automatisch wird eine mittlere Sicherheitsstufe gewählt. Über den Button Sicherheitsstufe kann die Sicherheitsstufe geändert werden.

Ein neuer RSA-Austau	schschlüssel wird erstellt.	\times
	 Wählen Sie eine passende Sicherheitsstufe für dieses Objekt. ● Hoch Bevor Objekt verwendet werden kann, muss meine Zustimmung mit einem Kennwort eingeholt werden. ○ Mittel Bevor Objekt verwendet werden kann, muss meine Zustimmung eingeholt werden. 	
	< Zurück Weiter > Abbrechen	

Wählen Sie **Hoch** und klicken Sie dann auf **Weiter**.

Ein neuer RSA-Austau	schschlüssel wird erstellt.	×
	Erstellen Sie ein Kennwort, um dieses Objekt zu schützen.	
	Neues Kennwort für dieses Objekt erstellen Kennwort für: Privater Schlüssel des Cr	
Ť	Kennwort:	
	Bestätigen:	J
	< Zurück Eertig stellen Abbrech	nen

Zum Schutz Ihres Schlüssels werden Sie zur Eingabe eines **Schlüssel-Kennwortes** aufgefordert. Nachdem Sie dieses eingegeben und bestätigt haben, wählen Sie **Fertig stellen**.

Ein neuer R	SA-Austausch	schlüssel wird erstellt.	
	Eine Anwend	ung erstellt ein geschütztes Objekt.	
	Privater Schlü	issel des Cry	
	Sie haben die Sicherheitsstu	hohe <u>S</u> icherheitsst	ufe
		OK Abbrechen Det	ails
C UHH-CA - Windows Internet E	xplorer		
CUFFLCA - Windows Internet E	xplorer de/uni-hamburg-ca/cg-bin/pub/pik	▼ ▲ (∱) ×) Tobal Seach	Sete v ^{os} Extra v ^{os}
C UBH CA. Windows Internet I C UBH CA. WINDOWS INTERNET C UBH CA. WINDOWS INTERNET C UBH CA. WINDOWS INTERNET U UDI VIENTIAL IN	xplorer deturshamburg-catog-bei(pob)(si	V A value Search	Contraction of the second
C UBH CA. Windows Internet I C UBH CA. Windows Internet I D UBPS//skpcadnu C UBPS//skpcadnu C UBPS//skpcadnu UBPS//skpcadnu UDPS//skpcad	xplorer felure-handwar-cator-knipobijski ität Hamburg	V A video Search	Sete C Betras C
CURICA Windows Internet L C C C C C C C C C C C C C C C C C C C	eplarer dejuri-hamburg-cargetingschijdel ität Hamburg ifikate Gesperite Zertifik	ate Policies Hilfe Beenden	Pettsches Forschungsnetz
2001CA Windows Internet I C C + 2 Inter(blace dhu ★ ★ Øuteca Universi Zertifikate CA-Zert Nutzerzetfikat	Aplarer dejuri handurg calog tenjadajali ität Hamburg iffikate Gesperite Zertlfik Serverzertlfikat Zert	ate Policies Hilfe Beenden jikat sperren Zertifikat suchen	
2001CA. Windows Internet 1 Constructions Construc	Aplorer dejuri-handurg celog-brijskeljel ität Hamburg iffikate Gesperite Zertlifik Server zertlifikat Zert	ate Policies Hilfe Beenden j jífkat speren Zertifikat suchen	
2UBICA. Windows Internet 1 Image: State of the office and the offi	Anjorer dejuri-handorg celog brigodopti ität Hamburg ifikate Gesperrte Zertlifik Serverzertlifikat Zert nd müssen Sie Ihren Zertlifi	ate Policies Hilfe Beenden fifkat sperren Zertifikat suchen Zertifikatantrag ausdrucken.	Solo Contraction Contraction
2 UBICA. Windows Internet I Image: Constraint of the state of t	Anglarer delari-handarg celegi telejastajali ität Hamburg iffikate Gesperrte Zertlifik Serverzertlifikat Zert nd müssen Sie Ihren Zertlifi petätigen Sie die Schalffläc katantarg geöffnet.	ate Policies Hilfe Beenden iffkat sperren Zertifikat suchen Ertifikat suchen Zertifikat suchen Ertifikatantrag ausdrucken. he "Zertifikatantrag anzelgen". Daraufhin wird der trag aus, unterschreiben ihn und legen ihn bei Ihrer intragsstellung abzuschließen.	C C C C C C C C C C C C C C C C C C C
Image: Second	Alphrer Alphrendorg calge Angelagia Ität Hamburg Ifikate Gesperrte Zertlifik Serverzertlifikat Zert nd müssen Sie Ihren Zertlifi petätigen Sie die Schaltfläct katantrag geöffnet. Internogsstelle vor, um die A ie den Zertlifikatantrag auss rkarte "Beenden" verlassen	ate Policies Hilfe Beenden fikat sperren Zertifikat suchen Zertifikatantrag ausdrucken. he "Zertifikatantrag ausdrucken. he "Zertifikatant	Control of the second s
2 UBICA. Windows Internet 1 Image: Constraint of the state of the stat	Apperer dejuri-handrog sakg krigtstøjde it ät Hamburg ifikate Gesperrte Zertifik Serverzertifikat Zert ind müssen Sie Ihren Zertifikatar rierungsstelle vor, um de A irerungsstelle vor	ate Policies Hilfe Beenden fifkat sperren Zertifikat suchen Zertifikat suchen Zertifikatantrag ausdrucken. he "Zertifikatantrag ausdrucken. he "Zertifikatantrag ausdrucken. he "Zertifikatantrag ausdrucken. he "Zertifikatantrag ausdrucken. gedruckt haben, können Sie diese Schnittstelle über - endmatsmag anzeigen.	Contraction of the second seco
2 UIICA Windows Internet I	eplerer deprivhendung-cargethripskipel ität Hamburg ifikate Gesperrte Zertfirk Serverzertfirkat Zert nd müssen Sie Ihren Zertfi bestättnanga gestfinkt. frucken Sie den Zertfirkatar rierungsstelle vor, um die A ie den Zertfirkatartrag aus- rkarte "Beeenden" verlassen	ate Policies Hilfe Beenden fifkat sperren Zertifikat suchen Zertifikatantrag ausdrucken. he "Zertifikatantrag anzeigen". Daraufhin wird der trag aus, unterschreiben ihn und legen ihn bei Ihrer hirragsstellung abzuschließen. gedruckt haben, können Sie diese Schnittstelle über	Control of the second s

Internet Explorer 7 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. Bestätigen Sie mit **OK**.

Sie werden nun 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 (RA) im RRZ auf:

Herr Olaf Gellert Regionales Rechenzentrum der Universität Hamburg Schlüterstraße 70 20146 Hamburg Telefon: 040 - 42838 4694 Terminabsprachen sind für den Vertretungsfall auch unter -3095 und -3050 möglich!

Folgendes ist mitzubringen:

- 1. Der vollständig ausgefüllte Zertifikatantrag,
- 2. der Personalausweis oder Pass,
- 3. ein Dokument, das die Zugehörigkeit zur Universität bestätigt (z.B. gültiger Studierendenausweis).

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 Antwort E-Mail und Zertifikat in den Browser importieren

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



6 Sicherungskopie des privaten Schlüssels

Für die folgenden Schritte wird ein USB-Stick oder eine leere Diskette benötigt (oder ein anderer externer Datenträger).

Internetoptioner	1				? 🛛
Verbindunge	n Sicherh	Progra	mme Datensd	hutz	Erweitert Inhalte
Inhaltsratgeber Filter I diesen	nelfen Ihnen n Computer a	bei der Kon angezeigt w A <u>k</u> tiviere	ntrolle der i erden kön	Internetin nen. Einst	halte, die auf ellungen
Zertifikate Zertifi Q Identi	kate werden fizierung ver	für verschli wendet.	üsselte Ve	rbindunge	n und zur
SL-Status	löschen	<u>Z</u> ertifik	ate	<u>H</u> era	usgeber
AutoVervollständi AutoV vorhe und so	gen ervollständig rige Eingaber hlägt Überei	en speicher n auf Webs nstimmunge	t eiten en vor.	Einst	ellungen
Feeds Feeds Websi ander könne	bieten aktua tes, die in In en Programm n.	ilisierte Inhi ternet Expl en gelesen	alte von orer und werden	Ei <u>n</u> st	ellungen
		ОК	Ab	brechen	Ü <u>b</u> ernehmen

Unter **Extras-Internetoptionen** finden Sie den Reiter **Inhalte**. Klicken Sie hier bitte **Zertifikate** an.

Zertifikate					?×
Beabsichtigter Zwec	k: <alle></alle>				~
Eigene Zertifikate	Andere Personen	Zwischenzertif	izierungsstellen	Vertrauenswürdige	< >
Ausgestellt für	Ausges	tellt von	Gültig bis	Angezeigter Name	
🕮 Olaf Gellert	UHH CA	- G02	16.09.2010	Olaf Gellert's Uni	
Importieren	portieren	atfernen		Er <u>w</u> eit	ert
Beabsichtigte Zwei	tke des Zertifikats -				
Clientauthentifizier	ung, Sichere E-Mail	l, Smartcard-Ann	neldung	Anzeige	n.
				<u>S</u> chlie	eßen

Unter **Eigene Zertifikate** sollte das eigene, von der UHH CA ausgestellte Zertifikat vorhanden sein. Wählen Sie Ihr neues Zertifikat von der UHH-CA aus und klicken Sie auf **Exportieren**.





Zertifikatsexport-Assistent
Exportdateiformat Zertifikate können in verschiedenen Dateiformaten exportiert werden.
Wählen Sie das gewünschte Format:
O DER-codiert-binär X.509 (.CER)
○ B <u>a</u> se-64-codiert X.509 (.CER)
O Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
Privater Informationsaustausch - PKCS #12 (.PFX)
Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
☑ ⊻erstärkte Sicherheit aktivieren (IE 5.0, NT 4.0 SP4 oder höher erforderlich)
Privaten Schlüssel nach erfolgreichem Export löschen
< <u>Z</u> urück <u>Weiter</u> Abbrechen

Es öffnet sich der Zertifikatsexport-Assistent. Wählen Sie **Weiter**.

Wählen Sie "Ja" und bestätigen Sie mit Weiter.

Setzen Sie bitte die beiden Haken. Bestätigen Sie mit **Weiter**.

Zertifikatsexport-Assistent] Da in d
Kennwort	sel abo
Der private Schlüssel muss mit einem Kennwort geschützt werden, um die Sicherheit zu gewährleisten.	einem
Geben Sie ein Kennwort ein und bestätigen Sie dieses.	Sie nui stätigei
<u>N</u> eninwort: ******	
' K <u>e</u> nnwort bestätigen:	erinner
*****	einen a
	importi
	<u> </u>
< <u>Z</u> urück <u>W</u> eiter > Abbrechen	

Da in dem Backup auch der private Schlüssel abgelegt wird, muss das Backup mit einem Kennwort gesichert werden. Geben Sie nun ein Backup-Kennwort ein und bestätigen Sie dieses noch einmal.

Das Kennwort ist frei wählbar. Sie müssen es unbedingt aufbewahren bzw. sich daran erinnern, wenn Sie Ihr Zertifikat später in einen anderen Browser oder E-Mail-Client importieren möchten.

Zertifikatsexport-Assistent	×
Exportdatei Geben Sie die den Namen der zu exportierenden Datei an.	
Dateiname:	
Durchsuchen	
	_
< <u>Z</u> urück <u>W</u> eiter > Abbrechen	

Drücken Sie Durchsuchen.

Speichern unte	er				? 🗙
Spejchern in:	Sechseldater	nträger (F:)) 🛛 🖉) 📂 🛄 -	
Zuletzt verwendete D	Documents				
Desktop					
igene Dateien					
Arbeitsplatz					
S	Dateiname:	Zertifikat.pfx			<u>S</u> peichern
Netzwerkumgeb	Dateityp:	Privater Informationsaustausch (*	.pfx)	*	Abbrechen

Wählen Sie den Wechseldatenträger (USB-Stick) oder das Floppylaufwerk bzw. einen anderen externen Datenträger, geben Sie einen Dateinamen ein und drücken Sie **Speichern**. Sie gelangen zurück zum vorigen Dialog, den Sie mit **Weiter** fortsetzen.



Der private A	ustauschschlüssel wird exportiert.	X
	Eine Anwendung erfordert Zugriff auf ein geschütztes Objekt.	
	Privater Schlüssel des Cry	
	OK Abbrechen Details	

Wenn Sie die hohe Sicherheitsstufe für Ihren Schlüssel gewählt haben, erscheint eine Kennwort-Abfrage. Geben Sie das Schlüssel-Kennwort für den Schlüssel ein und bestätigen Sie mit **OK**.

Zertifikatsexport-Assistent
Der Exportvorgang wurde erfolgreich abgeschlossen.
ОК

Bestätigen Sie mit OK.

Wählen Sie Fertig Stellen.

7 Wichtiger Hinweis zum Einstellen der Sicherheitsstufe

Für den Fall, dass Sie beim Erstellen des Zertifikatantrages für den privaten Schlüssel <u>nicht</u> die hohe Sicherheitstsufe eingestellt haben (wobei es Ihnen grundsätzlich freigestellt ist, ob Sie die hohe, mittlere oder niedrige Sicherheitsstufe wählen), wird beim Signieren einer E-Mail kein Kennwort abgefragt.

Es besteht somit die Gefahr, dass ein Virus mit eigener SMTP-Engine (versendet eigenständig Mails an z.B. die Einträge im Adressbuch) nun möglicherweise auch signierte Mails verschicken kann.

Darum sollte <u>unbedingt immer die hohe Sicherheitsstufe</u> eingestellt werden, um zu gewährleisten, dass für signierte Mails immer ein Kennwort abgefragt wird, so dass der oben beschriebene Fall nach Virusbefall, oder ähnlich gelagerter Missbrauch, verhindert wird.

So ändern Sie die Sicherheitsstufe für Ihren privaten Schlüssel: Windows hat keinen Mechanismus vorgesehen, um die Sicherheitsstufe zu verändern. Zum Ändern der Sicherheitsstufe wird der Schlüssel einfach erneut von der Sicherheitskopie importiert. Sie benötigen den USB-Stick oder die Diskette, auf der Sie ihren privaten Schlüssel gespeichert haben.

Zertifikate					?×
Beabsichtigter Zwecł	a <alle></alle>				~
Eigene Zertifikate	Andere Personen	Zwischenzertifiz	zierungsstellen	Vertrauenswürdige	< >
Ausgestellt für	Ausgeste	llt von	Gültig bis	Angezeigter Name	
🔛 Olaf Gellert	UHH CA -	G02	16.09.2010	Olaf Gellert's Uni	
Importieren Ex	portieren Entf	rernen		Er <u>w</u> eit	ert
Beabsichtigte Zwee	ke des Zertifikats —				
				Anzeige	en
				<u>S</u> chlie	эßen

Wählen Sie im Menü des Internet Explorers unter **Extras** die **Internetoptionen**. Unter dem Reiter **Inhalte** wählen Sie den Button **Zertifikate**.

Unter **Eigene Zertifikate** sollte das eigene von der Universität Hamburg ausgestellte Zertifikat vorhanden sein. Der rot markierte Schalter **Importieren** wird erst nach der Auswahl des eigenen Zertifikates verfügbar.



Es öffnet sich der Zertifikatsimport-Assistent. Drücken Sie **Weiter**.



🕑 🗿 🤌 🛄 -Documents Zertifikat Ò Zuletzt rwendete D.. Desktop Eigene Dateier **Si** Arbeitsplatz Dateiname: Öffnen Zertifikat < Abbrechen Dateityp: Privater Informationsaustausch (*.pfx;*.p12) ~ Netzwerkumgeb

Wählen Sie unter "**Suchen in:**" den Datenträger mit Ihrem Zertifikat (USB-Stick oder Diskette). Wählen Sie Ihr Zertifikat an und klicken Sie auf **Öffnen**.

Zert	ifikatsimport-Assistent 🛛 🗙	Wählen Sie "Weiter".
I	mportdateiname Geben Sie die zu importierende Datei an.	
—		
	Dateiname:	
	F:\Zertifikat.pf×	
	Hinweis: Es können mehrere Zertifikate in einer einzigen Datei in folgenden Formaten gespeichert werden:	
	Privater Informationsaustausch - PKCS #12 (.PFX,.P12)	
	Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)	
	Microsoft Serieller Zertifikatspeicher (.SST)	
-	< <u>Z</u> urück Weiter > Abbrechen	

Zertifikatsimport-Assistent	×
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 f ür den privaten Schl üssel aktivieren. Immer wenn der private Schl üssel 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.	
< <u>Z</u> urück <u>Weiter</u> > Abbrechen	

Zertifikatspeicher sind Systembereich	ne, in denen Zertifikate gespeichert	
Windows kann automatisch einen Zer Pfad für die Zertifikate angeben.	rtifikatspeicher auswählen oder Sie können eine	n
 Zertifikatspeicher automatisch 	auswählen (auf dem Zertifikattyp basierend)	
◯ <u>A</u> lle Zertifikate in folgendem Sp	peicher speichern	
Zertifikatspeicher:		
Eigene Zertifikate	Durchsucher	n)

Setzen Sie das Häkchen für Hohe Sicherheit und für Schlüssel als exportierbar markieren. Geben Sie dann das Backup-Kennwort für Ihren privaten Schlüssel an, das Sie zuvor beim Exportieren benutzt haben.

Dieses Kennwort ist nicht zu verwechseln mit dem Schlüssel-Kennwort für die hohe Sicherheitsstufe für Ihr Zertifikat.

Mit diesem Kennwort hatten Sie Ihren privaten Schlüssel auf der Diskette vor missbräuchlichen Zugriff geschützt.

Drücken Sie Weiter.

Wählen Sie Zertifikatsspeicher automatisch auswählen. Weiter

Zertifikatsimport-Assistent		×
Fertigstellen des Assistenten		Assistenten
	Der Zertifikatsimport-Assistent für die wurde erfolgreich abgeschlossen.	
	Sie haben folgende Einstellungen ausgewählt:	
	Gewählter Zertifikatspeicher Inhalt Dateiname	Auswahl wird vom Assisten PFX F:\Zertifikat.pfx
	< <u> </u>	
	< <u>Z</u> urück	Fertig stellen Abbrechen

Wählen Sie Fertig Stellen.

Ein neuer pri	vater Austauschschlüssel wird importiert. 🛛 🔀
	Eine Anwendung erstellt ein geschütztes Objekt.
	Privater Schlüssel des Cry
	Sie haben die mittlere Sicherheitsstufe gewählt OK Abbrechen Details





Jetzt können und sollen Sie die Sicherheitsstufe ändern.

Hier sollten Sie die **Sicherheitsstufe ein**stellen wählen.

Wählen Sie jetzt Hoch.

Sie werden nun zur Eingabe eines **Schlüssel-Kennwortes** aufgefordert. Damit wird der Kryptospeicher auf Ihrem Computer, der das eigene Zertifikat und den zugehörigen privaten Schlüssel beinhaltet, geschützt. Überlegen Sie sich ein Kennwort und bestätigen Sie dieses noch einmal. Dieses Kennwort wird bei jeder zu signierenden Mail abgefragt werden.

Drücken Sie Fertig Stellen.



Die Sicherheitsstufe wurde geändert. Bestätigen Sie mit **OK**.

ΟΚ

Zertifikatsimport-Assistent		
(į)	Der Importvorgang war erfolgreich.	
	ОК	