

# Die KIT Certification Authority Nutzerhandbuch

Tobias Dussa · Heiko Reese

# KIT CERTIFICATION AUTHORITY

P Bail Lors nop per sons de 51002	2++5kippins tercury mand in the statust last
TEC None-sche da trop 15 val 4500 Mail home	Dec 14 Out and the second and the second sec
ack 5272 ack 5272 ack son ) score of sonther sont de sunt ri	-14 04-00-16 Mercury -1-
win 108, option mobile raiot [ length of length of lags [	/1 = 1 and 10051 2549 zummel/ intproved
P second in the second	ute D Town/0=Thaute C SU62939280]; Upping 120070001
Succeec-mobilementor	The Presium Service Consulting country OK: depthet used 135615,437565 2009 to
n 1002 option 12121 home when it and	Dec 14 04:00.10 UR/email@decartification C. /C=2R/ST-Western C.
P score opcions [nop.nop.reliate.51983 ] hail	+14 04:00+10 Mercury sturnel (and premium servere) Services Division (Det
succeec-mobile-retor val 46221460 mail home.scht.de	alz/1=Hauth LU05[2548:302020000 antp=authroutonion aute.com
U, ack 30766	has 14 on tabaur /0=1 und 1 to 10001; VERIFY 0/ down 1280759616, 437610 mm
win 1002, options (e.51385 ) wail bons in length 0	A 14 04:00:17 mercine: AG/ONIzanto to Optimico, /Calle/STaBhalal
P	+0+1_accepted message geall: 1260759617 22Cert
F mail home adhe de	-accepted by meand in Kenote host said 200 H delivery 220; means and
survey su	Dec 14 04+00+17 -Kundenserver.de/
woolle-rz121 home when the process	20 revealed mercury qualt: 1000700001 and
Flags f	Ban 14 Advent
20 41 CC 34 CC 97	area 14 04:00:17 mercury gmails secondary of 10 remote 0/
av 41 66 74 65 72 20 3a 20 4a 64 6 a	9 44411; 1200/193617,226598 end and 204555000
20 32 30 31 32 20 47 41 40 48 61 66 20 32 31 20 31 76 7 70 70 7	meil/smtp-auth-outgoing: 1200760017 same
74 Z 00 15 1 10 11 10 14 04 04 00 20 20 20 20 20 20 20 20 20 20 20 20	1 06tage + T- 04 +
50 40 45 46 50 47 52 50 3 4b 40 51 20 20 20 53 75 62 6a 65 62	poto out 10/7 bytes sent to SSL
54 20 43 45 52 54 20 40 21 10 10 10 10 43 45 52 54 20 4F 55 21 11 10	2012 GHT . Subject d: 1260759644 949420 to
74 75 74 55 00 55 55 11 30 40 51 72 50 73 72 75 58 55 00 40 5 10 40	It: CN=GRP:KIT-CERT.OL=KII d: 1260759644 95004 topserver: status: 1/40
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	IT-CERT.0=Karlsruhe Instil
20 20 20 20 20 20 20 20 20 57 75 55 54 66 67 57 57 57 57 57 57 57 57 57 57 57 57 57	tute of Technology Cate 1 add 1200700014 prover
65 79 20 49 Ea EE EE 7 0 00 00 00 00 00 14 20 50 75 62 6c 69 63 20 4b	Cab task D. + 1
C C C C C C C C C C C C C C C C C C C	Jan Teles
DC 63 65 20 40 65 79 20 41 6c 67 6f 72 69 74 68 6d 74 20 70 72 ct 46 c	Publ 0: 1260/59644,966549 tcpserver: end 9516 status 0
63 72 79 70 74 69 6F 6a 0a 20 20 20 20 20 20 20 00 00 00 00 00 00	111C Key Algorithm: rsaEn[ M: 1200/53644.966659 topserver: status: 0/40
20 50 75 52 52 50 57 50 57 50 51 50 20 20 20 20 20 20 20 20 20 20 20 20 20	Icryption. RSA d: 1260759644.968772 tcpserver: status: 1/40
20 30 73 62 66 63 63 20 46 65 73 58 20 28 52 30 34 38 20 62 63 74 29 08	Public Key: (2048 bit),   d: 1260759644,977079 tcpserver: pid 9517 from 192
	Nodulue 1
28 22 20 24 28 20 52 59 74 29 24 04 20 20 20 20 20 20 20 20 20 20 20 20 20	1(2048 bit) + 1 dt 1260759644.977247 topserver: ok 9517 0:192.168
	0014-172-01-17-01 954
20 20 20 20 20 20 20 20 20 50 50 50 56 54 51 58 55 56 58 59 51 58 51 55 58 55	0010010110110101 etc. 1000759644 990919 topsequent and 9517 status 0
<b>329 32a</b> 61 66 <b>32a</b> 32 31 3a 38 36 3a 35 36 3a 31 32 3a 34 34 3a 62 63 3a 35	19:af:21:86:06:12:44:bc:51 44:toc:01 44:toc:0769644 901074 transmit statust 0/40
CT T C1 TT T 00 20 20 20 20 20 20 20 20 20 20 20 20	lc:a3:.
55 58 51 55 58 08 20 20 20 20 20 20 20 27 7, 77 77 72 72 74 70 F6 74 73	1 a0:95:d7:d5:d5:36:0f:31 mmail/001100mmail: 1200/33040.434403 recomment 4
20 20 61 30 3a 39 35 5a 64 5/ 5a 64 35 5a 64 55 5a 53 50 3a 50 60 7 6	14+95+23+6ftb4td3tdbtbft+1 46 2009
74 7 70 75 75 70 77 Xa 36 66 3a 62 34 3a 64 35 5a 64 62 5a 62 66 5a 0a	thmail/delivermail: 1260/53647.465/01 1 Message TV
54 58 55 55 58 58 58 58 58 58	a tehias@durta.de at pop.jundi.de (1568 octets).
to the 70207 > 192, 168, 1, 255, 30202; UDP, length 16	5 44 04:00:47 securu tstodt 1250759647 619435 tenseruer statut
P printserver.home.sons.de.succes are are are are 255 7202 Hill leadth 173	
D on interrupt hose, sdhs. de 7414 5 741 48 7414 19 19 19 19 19 19 19 19 19	
2 or intserver none suns.	

KIT – Universität des Landes Baden-Württemberg und

nationales Forschungszentrum in der Helmholtz-Gemeinschaft



#### 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.kit.edu/ca

#### 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 2013-02-04 (Revision 2527)

www.kit.edu

# Inhaltsverzeichnis

1	Einf	ührung	5
2	Bea	ntragung eines Zertifikats	5
	2.1	Nutzerzertifikat	5
		2.1.1 Zertifikatdaten	6
	2.2	Weitere Angaben	6
		2.2.1 Zertifikatantrag anzeigen und drucken	9
	2.3	Serverzertifikat	10
		2.3.1 Zertifikatdaten	11
		2.3.2   Weitere Angaben	12
3	Wei	tere Funktionen	13
-	3 1	Registerkarte Zertifikate	13
	5.1	3 1 1 Zertifikat sperren	13
		3.1.7 Zertifikat sychen	13
	2 2	Benisterkarte CA-Zortifikato	13
	J.Z	$3.2.1  \text{Murzelzertifikat}  \text{DEN_PCA_Zertifikat}  \text{KIT_CA_Zertifikat}$	13
		2.2.2. Zortifikatkotto anzoigon	17
	2 2	S.Z.Z Zertifikatkette anzeigen	14
	כ.כ	2.2.1. Zertifikatenereliete installieren	15
		3.3.1 Zertifikatsperniste installieren	10
	2.4	3.3.2 Zertifikatsperfilste anzeigen	15
	3.4	Registerkarte Policies	15
		3.4.1 DFN-PKI-POlicy	15
		3.4.2 Anwender-Policy	15
	3.5	Registerkarte Hilfe	15
	3.6	Registerkarte Beenden	15
4	Erst	ellen eines Requests für Serverzertifikate	15
	4.1	Allgemeines	15
	4.2	Internet Information Server	16
	4.3	Java Keystore	20
	4.4	OpenSSL	20
	4.5	Windows-Kommandozeile	20
5	Zusa	ammenführen von Zertifikatinformationen	21
	5.1	Nutzerzertifikate	21
	5.2	Serverzertifikate	22
		5.2.1 Internet Information Server	23
		5.2.2 Java Kevstore	24
		5.2.3 OpenSSI	24
		5.2.4 Windows-Kommandozeile	25
6	Exp	ortieren von Zertifikaten und geheimen Schlüsseln	25
	6.1	Internet Explorer	25
	6.2	Mozilla Firefox	30

# Revisionshistorie

Version	Inkrafttreten	Autor(en)	Änderung(en)
1	2009-08-19	Dussa, Tobias; Reese, Hei- ko	Initiale Revision.
2	2009-10-26	Dussa, Tobias	Anleitung für die Verwendung des Java Key- store ergänzt.
3	2010-08-17	Dussa, Tobias	Abschnitt zum Zertifikatexport eingefügt.
4	2011-11-16	Dussa, Tobias	Anleitung zu Windows-Server-Zertifikaten überarbeitet.
5	2012-07-17	Dussa, Tobias	Änderungen der DFN-Policy eingearbeitet.
6	2013-02-04	Dussa, Tobias	Hinweis zu privaten Schlüsseln in Firefox eingefügt; einige Passagen klarer formuliert.

# 1 Einführung

Die KIT-CA wird in Form einer Online-CA im Auftrag des KIT durch den DFN-Verein betrieben. Zertifikate werden direkt mittels einer Webschnittstelle beantragt, die durch den DFN-Verein zur Verfügung gestellt wird. Damit ein beantragtes Zertifikat ausgestellt werden kann, ist es danach notwendig, das von der Webschnittstelle generierte Antragsformular ausgefüllt in Papierform mit dem entsprechenden Ausweisdokument zu einer der Registrierungsstellen (RA) des KIT zu bringen, um sich gegenüber der KIT-CA zu identifizieren. Danach wird von den Mitarbeitern der entsprechenden RA der Zertifikatantrag freigeschaltet; die KIT-CA stellt daraufhin das beantragte Zertifikat aus.

Die Webschnittstelle der KIT-CA kann von allen Angehörigen einer Einrichtung ohne besondere Zugangsberechtigung genutzt werden. Sie ist unter dem URL https://pki.pca.dfn.de/kit-ca/ cgi-bin/pub/pki zu erreichen und wird in den nächsten Abschnitten beschrieben. In Abschnitt 2.1 wird die Beantragung eines Nutzerzertifikats, in Abschnitt 2.3 die Beantragung eines Serverzertifikats beschrieben. In den danach folgenden Abschnitten werden weitere Funktionen beschrieben, die über die Webschnittstelle zur Verfügung stehen. Schließlich wird in Abschnitt 6 vorgestellt, wie beantragte und ausgestellte Nutzerzertifikate exportiert werden können.

Dieser Anleitung liegt das entsprechende Dokument des DFN-Vereins zugrunde, das wir mit freundlicher Erlaubnis verarbeiten durften.

# 2 Beantragung eines Zertifikats

Zum Beantragen eines Zertifikats wählen Sie auf der Webseite die Registerkarte Zertifikate aus.

## 2.1 Nutzerzertifikat

Zum Beantragen eines Nutzerzertifikats wählen Sie den Reiter Nutzerzertifikat (Abbildung 1).



Abbildung 1: Startseite der Webschnittstelle.

Füllen Sie im folgenden Formular (Abbildung 2) alle mit einem Stern (\*) gekennzeichneten Felder aus.

Zertifikate         CA-Zertifikate         Gesperrte         Zertifikate         Policies         Hilfe         Beenden           Nutzerzertifikat         Serverzertifikat         Zertifikat sperren         Zertifikat suchen	Deutsches Forschungsnetz
Bitte geben Sie Ihre Daten ein. Felder mit einem Stern (*) müssen ausgefüllt werden.	
Zertifikatdaten         E-Mail *         Name *         Geben Sie hier Ihren Vor- und Nachnamen ein. Für Gruppenzertifikate stellen Sie das Kürzel "GRP:" voran. Verwenden Sie keine Umlaute.         Abteilung         Wenn Sie hier eine Abteilung angeben, wird diese in den Zertifikatnamen aufgenommen.	max.mustermann@kit.edu Max.Mustermann Institut fuer mustergueltige Beispiele
Weitere Angaben Diese Angaben werden nicht in das Zertifikat übernommen.	
PIN (Mindestens 8 beliebige Zeichen) *         Nochmalige Eingabe der PIN zur Bestätigung *         Die PIN wird von Ihnen benötigt, wenn Sie Ihr Zertifikat sperren wollen oder um dieses einzulesen, wenn Sie einer Veröffentlichung nicht zustimmen. Bitte notieren Sie sich die PIN.         Ich stimme der Zertifizierungsrichtlinie zu. *         Ich stimme der Veröffentlichung des Zertifikats mit meinem darin enthaltenen Namen und der E-Mail-Adresse zu.         Sie können diese Einwilligung jederzeit mit Wirkung für die Zukunft durch eine E-Mail an pki@dfn.de	······································
widerrufen. Weiter	

Abbildung 2: Beantragen eines Clientzertifikats – Schritt 1.

### 2.1.1 Zertifikatdaten

Diese Angaben werden in das Zertifikat übernommen. Die hier eingegebene E-Mail-Adresse wird von der KIT-CA zur Auslieferung des Zertifikats genutzt. Verwenden Sie bei der Eingabe Ihres Namens keine Umlaute; umschreiben Sie statt dessen ä als ae, ö als oe und so weiter. Ihr Name darf keine Zusätze beinhalten, die nicht auch in Ihrem Personalausweis oder Reisepass enthalten sind; beispielsweise wird ein Doktortitel häufig in den Personalausweis aufgenommen, die Bezeichnung »Professor« hingegen nicht. Im Feld Abteilung sollten Sie nur dann Angaben machen, wenn die Abteilung im OU=–Feld des Zertifikats erscheinen soll. Auch hier dürfen keine Umlaute verwendet werden. Beachten Sie außerdem, dass Sie die Zugehörigkeit zu einer Abteilung beispielsweise durch einen Institutsstempel oder ähnliches auf dem Antrag belegen müssen.

Beachten Sie ferner, dass lediglich solche E-Mail-Adressen zulässig sind, die auf

- fzk.de,
- kit.edu,
- uka.de oder
- uni-karlsruhe.de

enden.

### 2.2 Weitere Angaben

Diese Einträge werden nicht in das Zertifikat übernommen. Trotzdem möchten wir Sie auf einige Punkte explizit hinweisen.

- Achtung! Die PIN benötigen Sie als Passwort beim Importieren Ihres Zertifikats, wenn Sie einer Veröffentlichung nicht zugestimmt haben, oder wenn Sie Ihr Zertifikat sperren wollen. Sie sollten sich deshalb die PIN unbedingt notieren.
- Wenn Sie der Zertifizierungsrichtlinie nicht zustimmen, kann Ihr Antrag nicht bearbeitet werden. Mit anderen Worten, um ein Zertifikat zu erhalten, **müssen** Sie der Zertifizierungsrichtlinie zustimmen.
- Wenn Sie einer Veröffentlichung nicht zustimmen, steht Ihr Zertifikat nicht im öffentlichen Verzeichnisdienst zur Verfügung; es wird dann auch nicht automatisch in das globale KIT-AD-Adressbuch übernommen. In der Regel ist dies aber gewollt, so dass wir empfehlen, der Veröffentlichung zuzustimmen.
- Wenn Sie einer Veröffentlichung nicht zustimmen, benötigen Sie zum Import Ihres Zertifikats die oben eingetragene PIN.

Wenn Sie auf Weiter klicken, werden Ihnen Ihre Angaben noch einmal angezeigt (Abbildung 3).

Zertifikate CA-Zertifikate Nutzerzertifikat Serverze Die folgenden Daten wurden eing	Gesperrte Zertifikat ertifikat Zertifi jetragen:	e Policies Hilfe ikat sperren i	Beenden Zertifikat sucher Nutze	Deutsches Forschungsnetz
	Zertifikatdaten E-Mail n Name M Abteilung In Weitere Angaben Veröffentlichen Ja	nax.mustermann@l lax.Mustermann nstitut fuer musterg a	kit.edu gueltige Beispiel	e
		Andern Bestätigen		

Abbildung 3: Beantragen eines Clientzertifikats – Schritt 2.

Hier können sie die eingegebenen Daten nochmals überprüfen und, falls erforderlich, noch ändern. Wenn die Daten korrekt eingegeben wurden, klicken Sie auf Bestätigen. Ihr Webbrowser wird daraufhin das Schlüsselpaar für Sie erzeugen; die Schlüssellänge beträgt immer 2048 Bit. Von Mozilla Firefox wird Ihnen dieser Vorgang nur kurz angezeigt (Abbildung 4).



Abbildung 4: Beantragen eines Clientzertifikats – Schritt 3, Mozilla Firefox.

Beim Internet Explorer müssen Sie möglicherweise zunächst zustimmen, dass ein Add-on zur Schlüsselgenerierung ausgeführt wird (Abbildung 5). Diese Zustimmung ist nicht notwendig, wenn Sie die Seite der KIT-CA in die Zone der vertrauenswürdigen Sites aufgenommen haben.

🔞 This website wants to run the following add-on: 'Microsoft Certificate Enrolln	nent Control' from 'Microsoft Corp	oration'. If you trust the website a	and the add-on and want to allow it t	o run, click here	×
				DEUTSCHES Forschungsnetz	
Zertifikate CA-Zertifikate	Gesperrte Zertifi	ikate Policies Hi	ilfe Beenden		
Nutzerzertifikat         Serve	rzertifikat Ze	rtifikat sperren	Zertifikat suchen		
				Nutzerzertifikat beantra	gen - Bestätigen
Die folgenden Daten wurden eingetragen:					
	Zertifikatdaten E-Mail Name Abteilung Weitere Angaben Veröffentlichen Erweiterte Optionen>>	max.mustermann@ Max Mustermann Institut fuer Muste Ja	⊉kit.edu ergueltige Beispiele		
		Ändern Bestätigen	]		

Abbildung 5: Beantragen eines Clientzertifikats – Schritt 3, Internet Explorer – Ausführen des Add-ons genehmigen; der entsprechende Hinweis ist am oberen Bildrand zu sehen und sehr unscheinbar.

Beim Internet Explorer werden Sie noch mehrfach aufgefordert, der Zertifikatanforderung beziehungsweise der Schlüsselgenerierung zuzustimmen (Abbildungen 6 und 7).

	DEFN Deutsches Forschungsnetz	
Zertifikate CA-Zertifikate Gesperrte Zertifikate Policies Hilfe Beenden		
Nutzerzertifikat Serverzertifikat Zertifikat sperren Zertifikat suchen		
	zertifikat beantragen -	Restätigen
Nuze	zerunkat beantragen -	Bestatigen
Die folgenden Daten wurden eingetragen:		
Zertifikatdaten         E-Mail       max.mustermann@kit.edu         Name       Max Mustermann         Abteilung       Institut fuer Mustergueltige Beispiele         Weitere Angaben       Max Mustermann         Potential Scripting Violation       X         This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.       No		

Abbildung 6: Beantragen eines Clientzertifikats – Schritt 3, Internet Explorer – .

			DEN Deutsches Forschungsnetz	
Zertifikate CA-Zertifikate Ges Nutzerzertifikat Serverzertifi	sperrte Zertifikate Policies ikat Zertifikat sperren	Hilfe Beenden Zertifikat such	nen	
			Nutzerzertifikat beantra	gen - Bestätigen
Die folgenden Daten wurden eingetragen:	Creating a new RSA exchange key	×		
Zertif E-Mail Name Abteil <b>Weite</b> Veröff Erweiten	An application is creating a CuptoAPI Private Key Security level set to Medium	Protected item. D	iele	
	ОК	Cancel Details		

Abbildung 7: Beantragen eines Clientzertifikats – Schritt 3, Internet Explorer – Stufe 3.

### 2.2.1 Zertifikatantrag anzeigen und drucken

Abschließend werden Sie aufgefordert, sich Ihren Zertifikatantrag anzeigen zu lassen und ihn auszudrucken (Abbildung 8).

Zertifikate CA-Zertifikate Gesperrte Zertifikate Policies Hilfe Beenden
Zertifikatantrag
Abschließend müssen Sie Ihren Zertifikatantrag ausdrucken.
<ul> <li>Bitte betätigen Sie die Schaltfläche "Zertifikatantrag anzeigen". Daraufhin wird der Zertifikatantrag geöffnet.</li> <li>Bitte drucken Sie den Zertifikatantrag aus, unterschreiben ihn und legen ihn bei Ihrer Registrierungsstelle vor, um die Antragsstellung abzuschließen.</li> <li>Bitte beachten Sie, daß der geheime Teil Ihres Schlüsselpaares in Ihrem Webbrowser gespeichert wird. Um das von der CA ausgestellte Zertifikat nutzen zu können, muss es daher zwingend mit diesem Brower abgeholt werden! Wenn Sie in</li> </ul>
der Zwischenzeit den Browser wechseln, Ihr System neu installieren oder auf einen anderen Rechner wechseln, können Sie Ihr Zertifikat nicht korrekt importieren!
Nachdem Sie den Zertifikatantrag ausgedruckt haben, können Sie diese Schnittstelle über die Registerkarte "Beenden" verlassen.
Zertifikatantrag anzeigen

Abbildung 8: Beantragen eines Clientzertifikats – Schritt 4.

Bei diesem Antragsformular handelt es sich um ein PDF-Formular, das Sie beispielsweise mit dem Adobe Reader bereits am Bildschirm ausfüllen können, bevor Sie es ausdrucken; selbstverständlich können Sie ebenso das Formular ausdrucken und mit der Hand ausfüllen. Haben Sie eine Abteilungsoder Institutszugehörigkeit oder ähnliches angegeben, so lassen Sie das Formular als Bestätigung von zuständiger Stelle beglaubigen, beispielsweise durch einen Institutsstempel. Bringen Sie anschließend das Formular **persönlich** zur nächstgelegenen RA des KIT (HelpDesk des SCC im Campus Nord, BIT8000 des SCC im Campus Süd oder die RA des Campus Alpin). Bringen Sie außerdem **das auf dem Formular angegebene Ausweisdokument sowie Ihren KIT-Ausweis** oder einen sonstigen Nachweis Ihrer KIT-Zugehörigkeit mit. Bitte beachten Sie, dass Zertifikatanträge, für die nicht innerhalb von drei Monaten das zugehörige Formular ausgefüllt bei uns eingegangen ist, verworfen werden! Sie müssen also das zugehörige Formular innerhalb von drei Monaten bei einer Registrierungsstelle der KIT-CA einreichen!

Wenn Sie Mozilla Firefox zum Beantragen des Zertifikats verwendet haben, so beachten Sie bitte, dass Ihr geheimer Schlüssel zwar beim Beantragen erzeugt und in der Schlüsselablage des Browsers gespeichert wurde, aber **nicht** in der Übersicht Ihrer eigenen Zertifikate geführt wird, solange kein dazu passendes Zertifikat ausgestellt und eingespielt wurde.

## 2.3 Serverzertifikat

Im Folgenden wird erläutert, wie ein Serverzertifikat beantragt werden kann. Wählen Sie dafür im KIT-CA-Webinterface den Reiter Serverzertifikate.

Füllen Sie im angezeigten Webformular (Abbildung 9) alle mit einem Stern (\*) gekennzeichneten Felder aus.



Abbildung 9: Beantragen eines Serverzertifikats – Schritt 1.

### 2.3.1 Zertifikatdaten

Die Zertifikatdaten werden bei Serverzertifikaten nicht über die Webschnittstelle eingegeben, sondern sind als Datei im sogenannten PKCS#10-Format zur Webschnittstelle hochgeladen. Die PKCS#10-Datei muss vorher erzeugt werden. Beispiele, wie Sie eine solche Antragsdatei unter Windows und Linux erzeugen können, finden Sie in Abschnitt 4. Mit Hilfe des Zertifikatprofils wird festgelegt, für welche Anwendung das beantragte Zertifikat verwendet werden soll. Beim Ausstellen des Zertifikats wird durch die KIT-CA der entsprechende Verwendungszweck als sogenannte Extension in das Zertifikat eingetragen; der Zweck ist im Nachhinein nicht mehr änderbar. Sollte Ihr Anwendungsfall nicht als Profil zur Verfügung stehen, so setzen Sie sich bitte mit den Mitarbeitern der KIT-CA in Verbindung, um die Lage zu klären. Eine nähere Beschreibung der verfügbaren Profile finden Sie auf den Webseiten der DFN-PKI.

Sowohl für Rechnernamen wie auch für E-Mail-Adressen gilt wie bei Nutzerzertifikaten, dass nur solche Namen beziehungsweise Adressen zulässig sind, die auf

- fzk.de,
- kit.edu,
- uka.de oder
- uni-karlsruhe.de

enden.

#### 2.3.2 Weitere Angaben

Diese Einträge werden nicht in das Zertifikat übernommen. Bei der Beantragung eines Serverzertifikats müssen Sie hier Ihren Namen und Ihre E-Mail-Adresse angeben, damit die Zertifizierungsstelle das Serverzertifikat einem Ansprechpartner zuordnen kann. Als E-Mail-Adresse sollte eine Adresse verwendet werden, bei der sichergestellt ist, dass jederzeit während der Gültigkeit des Zertifikats ein kompetenter Ansprechpartner erreicht wird. Hierfür empfiehlt es sich beispielsweise, für Serverzertifikate nicht die direkte E-Mail-Adresse eines Administrators anzugeben, sondern vielmehr eine entsprechende **Mailingliste** oder einen entsprechenden **Mailverteiler**. Auf diese Weise kann elegant sichergestellt werden, dass auch bei Abwesenheit des beantragenden Administrators ein Vertreter erreichbar ist. Achtung! Die PIN benötigen Sie, wenn Sie das Zertifikat sperren wollen. Sie sollten sich deshalb die PIN unbedingt notieren. Wenn Sie der Zertifizierungsrichtlinie nicht zustimmen, kann Ihr Antrag nicht bearbeitet werden. Wenn Sie einer Veröffentlichung nicht zustimmen, steht Ihr Zertifikat nicht im öffentlichen Verzeichnisdienst zur Verfügung. Wenn Sie auf Weiter klicken, werden Ihnen Ihre Angaben noch einmal angezeigt. Sie können sie nun ändern oder die Richtigkeit bestätigen (Abbildung 10).

								_	_DFN_
									Deutsches
Zertifikato CA	Zortifikato	Connerto 7	artifikata	Policion	Hilfo	Roondon	1		Forschungshetz
Nutzerzertifikat	Serverz	ortifikat	Zortifika	tenerren		Zortifikat s	uchon		
		ertinkat		it sperren	1		uchen ur joursoutifi	kathaantuu	non Dootätigung
						36	rverzerun	kat beantrag	gen - bestaugung
Die folgenden Date	en wurden ei	ngetragen:							
PKCS#10- Zertifikatantrag	BEGIN CF MITDITCCAHUCA GC5LZRUXIFAAB VQQLF2JDnNDG AlUEChMM52Fyb EwlIXXJsc3J16 BhMCRUuggEL mRZJQ5dm6pvds gSgCsB7rc10C MgD1bXrd4d46 OH6/MW7EXUwFF Khdk05FpAgHBA sV3U74003cU aPUEEJ79Q)GC1 JNGRcPuitTDN 9q23++XvQK0IF /tTlvAucd2DT Eg== END CERT	RTIFICATE REQUE QAugecxJTAjBgko gWVBANTGAJLAXM XRIdCEmdWVJELI HNydWhlIELuc3Rg GUXGZAZBgNVBAg1 ALOGCSGST b3DgH c52UXOGCAJLAJRE c52UXOGCAJLAJRE SWUWGVXAUX SWUWGVXAUX SWUGVXAUX SWUWGVXAUX	ST hhtg9wDBcOE hhtg9wDBcOE seWSs2VydnV c3RLcmd120k, dHV02Sbv21b Ek7L26VuLVd AQUAA1BDbA kGEu+cDe7LB HMC0x2GWPT kGEu+cDe7LB IS2w0A2 L0XDE 9wDBAQUFAAC 32BLwC7CuOO 13Ln16H51bk ZM/nf+92Lvc AwM60Y+zwyH 	WFm1heC5tdX 'yLmltY15raX Oawd11EJ1ax UZWNobm9sb2 UZWNobm9sb2 UZWNobm9sb2 Woqu6CbgnRu 60J4Xctunfva ApmONKnmb9d 4P5s1UnWAt 4P5s1UnWAt 4P5s1UnWAt CAQEAYf5tL WAQqMEx7JEF rITO/rmO4E2 6E7/1xDmKa pK9UaEzEVTX k2d5fmAMbrz	NOZXJEYY QuZWRIM: MwaWW3Z d5MRIwE/ WyZzELM (6xeTbz) ndHwq6q RFC2J+r: rYXUUY4 zuw8HKT mPcrfQzI vEnVQ9/ qwdpVf21 qwdpVf21 qwdpVf21 qwdpVf21 qwdpVf21 x1FVQ9/ qwdpVf21 x1FVQ9/ qwdpVf21 x1FVQ9/ gwdpVf21 x1FVQ9/ gwdpVf21 x1FVQ9/ gwdpVf21 x1FVQ9/ gwdpVf21 x1FVQ9/ gwdpVf21 x1FVQ9/ yyc+tL1 yTFSB16 x1FVQ9/ yyc+tL1	NSUQGtp SRuDQTD FEqMCGG AYDVQQH KKGAIUE KumbBv7 HKbaKvq KumbBv7 HKbaKvq KuMbWs7 HKbaKvq KuMV HKbaKvq HKbaKv			
Zertifikatsprofil	Web Serve	r							
Algorithmus des öffentlichen Schlüssels	rsa Encrypti	on							
Schlüssellänge	2048								
Eindeutiger Name	emailAddre Musterguelt Wuerttemb	ss=max.mus tige Beispiele erg,C=DE	termann@ .0=Karlsri	kit.edu,C uhe Institu	N=beis ute of T	pielserver. echnology,	.imb.kit.eo ,L=Karlsru	du,OU=Insti uhe,ST=Bad	itut fuer en-
Veröffentlichen	Ja	-							
Name (Vor- und Nachname)	Max Muster	mann							
E-Mail	max.muste	rmann@kit.e	du						
Abteilung	Institut fuer	r Musterguelt	ge Beispie	ele					
			Änd	ern Bestät	igen				

Abbildung 10: Beantragen eines Serverzertifikats – Schritt 2.

Wenn Sie Ihre Angaben bestätigen, werden Sie wie bei der Beantragung eines Nutzerzertifikats aufgefordert, sich Ihren Zertifikatantrag anzeigen zu lassen und auszudrucken (Abbildung 8). Zusätzlich zu den bereits oben und in Abschnitt 4 zu findenden Hinweisen ist es wichtig, dass für die RA-Mitarbeiter erkennbar ist, dass Sie berechtigt sind, für den jeweiligen Rechnernamen ein Zertifikat zu beantragen; wenn Sie beispielsweise ein Zertifikat für einen Institutswebserver beantragen, wäre etwa der entsprechende Institutsstempel hilfreich. Außerdem müssen Sie ein von der KIT-CA ausgestelltes und gültiges Nutzerzertifikat besitzen, um ein Serverzertifikat zu beantragen.

Bitte beachten Sie, dass Zertifikatanträge, für die nicht innerhalb von drei Monaten das zugehörige Formular ausgefüllt bei uns eingegangen ist, verworfen werden! Sie müssen also das zugehörige Formular innerhalb von drei Monaten bei einer Registrierungsstelle der KIT-CA einreichen!

Bitte beachten Sie weiter, dass es nicht ausreicht, Zertifikatanträge per Fax zu übermitteln. Es werden die Originalanträge benötigt!

Schicken Sie das ausgedruckte Formular an die KIT-CA (KIT-CA, Steinbuch Centre for Computing/Campus Süd) oder geben Sie es persönlich bei einer Registrierungsstelle ab.

# 3 Weitere Funktionen

Außer der Beantragung von Zertifikaten stehen Ihnen über diese Webschnittstelle noch weitere Funktionen zur Verfügung.

## 3.1 Registerkarte Zertifikate

#### 3.1.1 Zertifikat sperren

Hier können Sie bereits ausgestellte Zertifikate wieder sperren lassen. Dazu benötigen Sie die Seriennummer des Zertifikats, die Sie mit Ihrem Zertifikat erhalten haben, und die PIN, die Sie in Ihrem Zertifikatantrag angegeben haben. Sie müssen Ihr Zertifikat beispielsweise sperren, wenn der geheime Teil des zum Zertifikat gehörenden Schlüsselpaares in falsche Hände geraten ist.

### 3.1.2 Zertifikat suchen

Hier können Sie nach Zertifikaten suchen, die durch die KIT-CA ausgestellt wurden und deren Eigentümer der Veröffentlichung zugestimmt haben. So können Sie beispielsweise das Zertifikat eines Kommunikationspartners, dem Sie verschlüsselte E-Mails schicken möchten, suchen und, falls Sie fündig geworden sind, herunterladen. Als Suchkriterium kann der Name oder die E-Mail-Adresse verwendet werden.

### 3.2 Registerkarte CA-Zertifikate

### 3.2.1 Wurzelzertifikat, DFN-PCA-Zertifikat, KIT-CA-Zertifikat

Hier können Sie das Wurzelzertifikat der Deutschen Telekom, das Zertifikat der DFN-PKI sowie das Zertifikat der KIT-CA herunterladen. Für die meisten Anwendungen sollte es nicht nötig sein, eines der Zertifikate herunterzuladen beziehungsweise zu installieren, da das Wurzelzertifikat der Deutschen Telekom bereits in den aktuellen Versionen gängiger Browser sowie im Windows-Zertifikatspeicher mitgeliefert wird. Sollte ein manueller Import tatsächlich nötig sein, so wird es in den meisten Fällen genügen, das Wurzelzertifikat der Deutschen Telekom herunterzuladen. Die übrigen Zertifikate (DFN-PKI und KIT-CA) müssen nur in den seltensten Fällen vom Benutzer manuell installiert werden.

Die Vorgehensweise beim Herunterladen ist bei allen drei Zertifikaten gleich. Je nach verwendetem Browser werden Sie möglicherweise zu weiteren Aktionen aufgefordert.

Wenn Sie in Mozilla Firefox eine der Registerkarten anklicken, wird das entsprechende Zertifikat direkt in Ihren Browser geladen. Sie können dann wählen, für welche Zwecke Sie der entsprechenden Zertifizierungsstelle vertrauen wollen (Abbildung 11). In der Regel sollten Sie alle Kästchen ankreuzen. Wenn Sie die Zertifikate auch in andere Anwendungen (beispielsweise Mozilla Thunderbird) importieren möchten, klicken Sie mit der rechten Maustaste auf die entsprechende Registerkarte und wählen Sie »Ziel speichern unter«. Das Zertifikat wird dann im Zielordner abgelegt und kann in andere Programme importiert werden. Beachten Sie, dass Sie von Mozilla Firefox keine Bestätigungsmeldung bekommen, dass die Installation des Zertifikats erfolgreich war. Korrekt installierte Zertifikate sind jedoch im Einstellungsmenü unter »Erweitert«/»Zertifikate anzeigen«/»Zertifizierungsstellen« aufgelistet.



Abbildung 11: Importieren eines CA-Zertifikats in Mozilla Firefox.

Der Internet Explorer fordert Sie in mehreren Schritten auf, das Zertifikat zu importieren (Abbildung 12). Öffnen Sie das Zertifikat, wenn Sie es nur im Windows-Zertifikatspeicher installieren wollen. Sie können das Zertifikat auch speichern und dann in den Windows-Zertifikatspeicher und in andere Programme importieren. Wenn Sie das Zertifikat installieren, werden Sie durch einen Assistenten geführt; die erfolgreiche Installation wird Ihnen bestätigt.

Certificate ?
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s): •All application policies
Issued to: DFN-Verein PCA Global - G01
Issued by: Deutsche Telekom Root CA 2
Valid from 19.12.2006 to 01.07.2019
Install Certificate Issuer Statement
OK

Abbildung 12: Importieren eines CA-Zertifikats in den Internet Explorer.

### 3.2.2 Zertifikatkette anzeigen

Hier können Sie alle drei Zertifikate – Wurzelzertifikat der Deutschen Telekom, DFN-PKI-Zertifikat und KIT-CA-Zertifikat – auf einmal anzeigen lassen und herunterladen.

## 3.3 Registerkarte Gesperrte Zertifikate

#### 3.3.1 Zertifikatsperrliste installieren

Hier können Sie die aktuelle Zertifikatsperrliste in Ihren Browser laden; dies sollte, wann immer möglich, auch getan werden. Der Internet Explorer bietet Ihnen zusätzlich die Möglichkeit, die Zertifikatsperrliste zu speichern, um sie auch in andere Anwendungen zu importieren.

#### 3.3.2 Zertifikatsperrliste anzeigen

Hier können Sie sich die aktuelle Zertifikatsperrliste anzeigen lassen und in einer Datei speichern.

### 3.4 Registerkarte Policies

#### 3.4.1 DFN-PKI-Policy

Hier können Sie die Policy (Zertifizierungsrichtlinie) der DFN-PKI herunterladen.

#### 3.4.2 Anwender-Policy

Hier können Sie die Policy der KIT-CA herunterladen.

### 3.5 Registerkarte Hilfe

Hier können Sie diese Nutzeranleitung herunterladen.

### 3.6 Registerkarte Beenden

Hier können Sie die Webschnittstelle verlassen.

# 4 Erstellen eines Requests für Serverzertifikate

### 4.1 Allgemeines

Um ein Serverzertifikat beantragen zu können, muss zunächst ein entsprechender Request generiert werden, der mit Hilfe des Webinterfaces an die KIT-CA geschickt werden kann. Beispielhaft ist unten das Vorgehen bei Benutzung von OpenSSL sowie dem Internet Information Server beschrieben. Unabhängig von der verwendeten Software sind jedoch einige Rahmenbedingungen einzuhalten, die in den Policies der DFN-PKI und der KIT-CA näher beschrieben sind. Die wichtigsten einzuhaltenden Eckpunkte sind:

- Der DN muss mindestens die Zeichenketten C=DE, ST=Baden-Wuerttemberg, L=Karlsruhe und O=Karlsruhe Institute of Technology enthalten.
- Der Name des Servers muss ein vollqualifizierter Rechnername (Fully-qualified host name, FQHN), der auf eine der Domains

```
- fzk.de,
```

- kit.edu,
- uka.de oder

```
- uni-karlsruhe.de
```

endet.

- Neben dem Namen des Servers muss im Zertifikatantrag eine E-Mail-Adresse angegeben sein, mit der ein verantwortlicher Administrator erreicht werden kann. Diese kann entweder als emailAddress-Feld im DN oder als Subject alternative name (SaN) angegeben werden und muss ebenfalls auf eine der vier angegebenen Domains enden. Es bietet sich an, eine Gruppenmailingliste oder einen Mailverteiler anzugeben, um elegant sicherstellen zu können, dass auch bei Krankheit oder Urlaub einzelner Mitarbeiter stets ein kompetenter Ansprechpartner erreicht wird.
- Im DN sind die folgenden Attribute zulässig; in eckigen Klammern angegebene Attribute können weggelassen werden, Argumente in spitzen Klammern müssen entsprechend ersetzt werden:
  - C=DE,
  - ST=Baden-Wuerttemberg,
  - L=Karlsruhe,
  - O=Karlsruhe Institute of Technology,
  - [OU=<Abteilung, Institut, Organisationseinheit etc.>],
  - CN=<Servername (FQHN) > und
  - [emailAddress=<E-Mail-Adresse>].
- Die verwendete Schlüssellänge muss mindestens 2048 Bit betragen; derzeit werden Schlüssellängen von 2048 Bit gemeinhin als hinreichend sicher angesehen.

#### 4.2 Internet Information Server

Zertifikatanträge können unter Windows mit Hilfe des Internet Information Server (IIS) erzeugt werden. Hierfür öffnen Sie die Verwaltungskonsole des IIS (Abbildung 13). Im Dialogfenster der Eigenschaften einer Webseite können Sie unter dem Punkt »Verzeichnissicherheit« den Wizard zur Erzeugung eines Requests mit der Schaltfläche »Serverzertifikat« starten.

Default Web	Site Prope	rties						?	×	
Web Site Directory S	Performa Security	Ho Cus	me Directory tom Errors	Docum ASP.N	ents JET					
Authentication and access control Enable anonymous access and edit the authentication methods for this resource. Edit										
IP address	IP address and domain name restrictions Grant or deny access to this resource using IP addresses or Internet domain names. Edit									
Secure communications Require scure communications and enable clenk certificates when this resource is accessed. <u>yiew Certificate</u> Egit										
		0	к	Can	cel	Apply	н	elp		

Abbildung 13: Verwaltungskonsole des IIS.

Wählen Sie »Neues Zertifikat erstellen« aus und klicken Sie dann auf Weiter (Abbildung 14).



Abbildung 14: Erzeugen eines Zertifikatantrags mit dem IIS – Schritt 1.

Wählen Sie im nächsten Schritt »Request vorbereiten und später senden« aus und klicken Sie auf Weiter.



Abbildung 15: Erzeugen eines Zertifikatantrags mit dem IIS – Schritt 2.

Im nächsten Dialogfenster ist es wichtig, die richtige Schlüssellänge auszuwählen. Wählen Sie mindestens 2048 Bit. Der anzugebene Name ist nur für den internen Gebrauch bestimmt und kann von Ihnen frei gewählt werden. Klicken Sie auf Weiter.

Certificate Wizard					×
Vame and Security Se Your new certificate m	<b>ittings</b> iust have a name	and a specific bit I	length.		Ì
Type a name for the n remember. Name:	iew certificate. Th	ie name should be	easy for you to r	efer to and	
Default Web Site					
The bit length of the e The greater the bit len decrease performance	ncryption key del ngth, the stronger a.	ermines the certific the security. How	ate's encryption ever, a greater b	strength. it length may	
Bit lengt <u>h</u> :	1024	•			
🔲 Select cryptograp	512 1024 2048	(SP) for this ce	rtificate		
	4096 8192 16384				
		2 Deels	News	Coursel	

Abbildung 16: Erzeugen eines Zertifikatantrags mit dem IIS – Schritt 3.

Im nächsten Schritt muss als Organisationsname Karlsruhe Institute of Technology eingegeben werden. Der Abteilungs- oder Institutsname (Organizational Unit, OU) ist im Prinzip frei wählbar, muss aber nachvollziehbar sein und im Zweifel belegt werden. Die in Abbildung 17 zu sehende Zeichenkette <OE> ist als Platzhalter zu verstehen und entsprechend zu ersetzen oder leer zu lassen. Bestätigen Sie mit Weiter.

anization Information	
Your certificate must include information distinguishes it from other organizations.	n about your organization that
Select or type your organization's name legal name of your organization and the	and your organizational unit. This is typically to name of your division or department.
For further information, consult certificat	tion authority's Web site.
Organization:	
Karlsruhe Institute of Technology	•
Organizational unit:	
<0E>	•
,	_

Abbildung 17: Erzeugen eines Zertifikatantrags mit dem IIS – Schritt 4.

Im nächsten Schritt muss der vollqualifizierte DNS-Hostname des Rechners, von dem das Zertifikat später verwendet werden soll, eingegeben werden. Wiederum ist <FQDN> in Abbildung 18 als Platzhalter zu verstehen und entsprechend zu ersetzen. Klicken Sie auf Weiter.

S Certificate Wizard	
Your Site's Common Name Your Web site's common name is its fu	ully qualified domain name.
Type the common name for your site. I name. If the server is on the intranet, y name.	If the server is on the Internet, use a valid DNS you may prefer to use the computer's NetBIDS
If the common name changes, you wil	Il need to obtain a new certificate.
Common name:	
<fqdn></fqdn>	
	< Back Next> Lancel

Abbildung 18: Erzeugen eines Zertifikatantrags mit dem IIS – Schritt 5.

Als nächstes müssen die geographischen Kenndaten eingegeben werden: Land DE, Bundesland Baden-Wuerttemberg und Stadt Karlsruhe. Bestätigen Sie mit Weiter.

IIS Certificate Wizard 🛛 🗙
Geographical Information The certification authority requires the following geographical information.
Country/Region: DE (Germany)
Baden-Wuerttemberg
,
State/province and City/locality must be complete, official names and may not contain abbreviations.
< <u>B</u> ack <u>N</u> ext > Cancel

Abbildung 19: Erzeugen eines Zertifikatantrags mit dem IIS – Schritt 6.

Im nächsten Schritt wird der Name der Datei abgefragt, in der der Zertifikatantrag gespeichert werden soll. Geben Sie einen geeigneten Namen ein und klicken Sie auf Weiter.

rtificate Request File Name			
Your certificate request is saved as a te specify.	xt file with the file r	ame you	
Enter a file name for the certificate requ	est.		
<u>File name:</u>			
c:\certreg.txt			Browse
,			
			-

Abbildung 20: Erzeugen eines Zertifikatantrags mit dem IIS – Schritt 7.

Schließlich wird in einer letzten Dialogbox zusammengefasst, was bisher eingegeben wurde. Bestätigen Sie diese Einstellungen.

### 4.3 Java Keystore

Zunächst muss ein Schlüsselpaar aus privatem und öffentlichem Schlüssel generiert werden. Dies kann mit der folgenden Kommandozeile erfolgen, wobei die Platzhalter sinnvoll ersetzt werden müssen:

```
keytool -genkey \
-alias <Schluesselname> \
-dname "C=DE,ST=Baden-Wuerttemberg,L=Karlsruhe,O=Karlsruhe Institute of Technology,CN=<FQHN>" \
-keyalg RSA \
-keysize 2048 \
-keystore <Keystoredatei>
```

Aus diesem Schlüsselpaar kann dann der Zertifikatantrag mit der folgenden Kommandozeile generiert werden:

```
keytool -certreq \
-alias <Schluesselname> \
-file <Antragsdatei> \
-keystore <Keystoredatei>
```

Es kann hilfreich sein, die CA-Zertifikate der DFN-PCA und der KIT-CA in den Java-Keystore aufzunehmen. Dies erfolgt mit der folgenden Kommandozeile, wobei die Platzhalter durch die entsprechenden Dateinamen der Zertifikate zu ersetzen sind:

```
keytool -import -trustcacerts \
  -alias dfnca \
  -file <DFN-CA-Zertifikat> \
  -keystore <Keystoredatei>
keytool -import -trustcacerts \
  -alias kitca \
  -file <KIT-CA-Zertifikat> \
  -keystore <Keystoredatei>
```

## 4.4 OpenSSL

Mit OpenSSL kann ein Zertifikatantrag leicht mit der folgenden Kommandozeile erstellt werden. In spitzen Klammern stehende Argumente müssen entsprechend ersetzt werden:

```
openssl req \
  -newkey rsa:2048 \
  -out <Antragsdatei> \
  -keyout <Schluesseldatei> \
  -subj '/C=DE/ST=Baden-Wuerttemberg/L=Karlsruhe/O=Karlsruhe Institute of Technology/CN=<FQHN>'
```

Aus Platzgründen wird im Beispiel auf die Angabe der (optionalen) Felder OU und emailAddress verzichtet. Sie können einfach an den entsprechenden Stellen eingefügt werden; die oben angegebene Attributreihenfolge muss dabei eingehalten werden. Die Antrags- und die Schlüsseldatei werden dabei von OpenSSL überschrieben; die Antragsdatei ist danach im Webinterface hochzuladen.

Beachten Sie, dass Sie bei Aufruf der obigen Kommandozeile ein Passwort für den geheimen Schlüssel eingegeben werden muss. Dies ist für viele Serveranwendungen hinderlich. Durch Angabe der zusätzlichen Option –nodes wird der geheime Schlüssel nicht chiffriert, so dass auch die Angabe eines Passworts entfällt.

Die Schlüsseldatei ist später für den tatsächlichen Betrieb des Servers in Verbindung mit dem Ihnen dann zugeschickten Zertifikat nötig.

### 4.5 Windows-Kommandozeile

Requests können unter Windows auch auf der Kommandozeile erstellt werden. Hierfür muss zunächst eine Datei <Eingabedatei> mit folgenden Inhalt erstellt werden. Die Platzhalter <Eingabedatei> und <Antragdatei> sind hierbei durch beliebige Dateinamen zu ersetzen:

```
[RequestAttributes]
SAN = "email=<E-Mail-Adresse>"
[NewRequest]
Exportable = TRUE
KeyLength = 2048
MachineKeySet = TRUE
Subject = "C=DE,ST=Baden-Wuerttemberg,L=Karlsruhe,O=Karlsruhe Institute of Technology,CN=<FQDN>"
RequestType = PKCS10
UserProtected = FALSE
```

Angaben in spitzen Klammern sind entsprechend zu ersetzen. Der eigentliche Request kann danach mit dem folgenden Aufruf erstellt werden:

certreq -new <Eingabedatei> <Antragdatei>

Hierbei wird die Datei <Antragdatei> mit dem neu generierten Request überschrieben und muss über das Web-Interface am die KIT-CA geschickt werden. Details Ihres Requests können Sie mit folgendem Befehl ansehen:

certutil -dump <Antragdatei>

# 5 Zusammenführen von Zertifikatinformationen

Wenn die KIT-CA auf Ihren Zertifikatantrag hin das beantragte Zertifikat ausstellt, werden Sie mit Hilfe einer E-Mail informiert, dass das beantragte Zertifikat bereitsteht. Das ausgestellte Zertifikat wird auch als Anhang dieser E-Mail in Form einer .pem-Datei mitgeschickt. Dieses Zertifikat müssen Sie mit dem geheimen Schlüssel, den Sie beim Beantragen erzeugt haben, zusammenführen, um das Zertifikat nutzen zu können.

### 5.1 Nutzerzertifikate

Zum Zusammenführen Ihres Nutzerzertifikats mit Ihrem geheimen Schlüssel müssen Sie mit **demselben** Webbrowser, mit dem Sie das Zertifikat beantragt haben, auf **demselben Rechner** unter **demselben** Benutzerprofil das ausgestellte Zertifikat laden. Hierfür öffnen Sie den in der E-Mail angegebenen Link öffnen (Abbildung 21).

								_	DEN Deutsches Forschungsnetz
Zer	tifikate CA-Ze	ertifikate	Gesperrte Ze	ertifikate	Policies H	lilfe	Beenden		
Nutz	zerzertifikat	Server:	zertifikat	Zertifik	at sperren		Zertifikat suchen		
							Laden des	s beantragten Z	ertifikats
	Benutzen Sie	den Butto	n, um Ihr Zerf	ifikat in 1	(hren Browse	r zu	importieren.		
	Bitte beachte	n Sie, da	ss einige Brov	wser eine	en erfolgreid	hen	Import nicht ges	ondert melder	٦.
	Wenn Sie bei so werden Sie	der Antra nach der	gsstellung bes PIN gefragt, (	stimmt ha die Sie in	iben, dass Ih Ihren Zertifil	r Ze <ata< td=""><td>rtifikat nicht veröfi ntrag eingegeben l</td><td><sup>r</sup>entlicht werde naben.</td><td>n soll,</td></ata<>	rtifikat nicht veröfi ntrag eingegeben l	<sup>r</sup> entlicht werde naben.	n soll,
				Zei	rtifikat importieren				
								Im	pressum

Abbildung 21: Zusammenführen eines Nutzerzertifikats – Schritt 1.

Wenn Sie der Veröffentlichung des Zertifikats beim Beantragen nicht zugestimmt haben, so ist die von Ihnen gewählte PIN nötig, um das Zertifikat mit Hilfe des angegebenen Links laden zu können (Abbildung 22); dieser Schritt wird übersprungen, wenn Sie der Veröffentlichung zugestimmt haben.

Zertif	ikate CA	-Zertifikate	Gesperrte Z	ertifikate	Policies Hilf	e Beenden		DF Deutsch Forschu	N _ nes ingsnet
Nutzei	rzertifikat	Server:	zertifikat	Zertifika	at sperren	Zertifikat s	uchen		
_							P	IN-geschützter Inha	lt
	Der gewün des Zugan	schte Inhalt gs ein.	ist durch eine	PIN gesch	hützt. Bitte gel	oen Sie die b	enötigte F	PIN zur Erlangung	
			PIN für d	en Zugriff	auf die Seite				
				OK	Zurücksetzen				
								Impressur	n

Abbildung 22: Zusammenführen eines Nutzerzertifikats – Schritt 2.

Firefox bestätigt danach direkt den erfolgreichen Import mit einer entsprechenden Hinweisbox (Abbildung 23).



Abbildung 23: Zusammenführen eines Nutzerzertifikats – Rückmeldung von Mozilla Firefox.

Der Internet Explorer dagegen fordert zunächst eine Bestätigung an, dass Sie der Webseite vertrauen und das von dort stammende Zertifikat tatsächlich installieren möchten (Abbildung 24).

Mögliche	Skriptingverletzung
♪	Diese Website fügt ein oder mehrere Zertifikate zu diesem Computer hinzu. Es besteht ein Sicherheitsrisiko, wenn Sie nicht vertrauenswürdigen Websites das Aktualisieren von Zertifikaten gestatten. Die Website kann Zertifikate installieren, denen Sie nicht vertrauen, durch die wiederum nicht vertrauenswürdige Programme auf dem Computer ausgeführt werden können, die Zugriff auf Ihre Daten haben.
	Soll dieses Programm jetzt die Zertifikate hinzufügen? Klicken Sie auf "Ja", wenn Sie dieser Website vertrauen. Andernfalls klicken Sie auf "Nein".
	Ja Nein

Abbildung 24: Zusammenführen eines Nutzerzertifikats – Rückfrage des Internet Explorer.

Wenn Sie den Vorgang bestätigen, wird direkt im Webbrowser eine entsprechende Bestätigung dargestellt (Abbildung 25).

					DEutsches Forschungsnetz
Zertifikat	e CA-Zer	tifikate Gesperrte	Zertifikate Policies	Hilfe Beenden	
Nutzerzer	tifikat	Serverzertifikat	Zertifikat sperren	Zertifikat suchen	
				Zertifikatsinstallation für In	ternet Explorer
	Das Zertifi	ikat wurde erfolgrei	ch installiert.		
					Impressum

Abbildung 25: Zusammenführen eines Nutzerzertifikats – Bestätigung des Internet Explorer.

Es wird empfohlen, dass Sie umgehend eine Sicherheitskopie Ihres Zertifikats inklusive geheimem Schlüssel anlegen, damit der geheime Schlüssel nicht so einfach versehentlich verloren gehen kann. Siehe hierzu auch Abschnitt 6, in dem das Exportieren von Zertifikat und geheimem Schlüssel beschrieben wird.

## 5.2 Serverzertifikate

Je nach Serveranwendung kann es notwendig sein, den geheimen Schlüssel mit dem von der CA ausgestellten Zertifikat in einer Datenbank oder in einer gemeinsamen Datei zusammenzuführen. Für andere Anwendungen kann es aber auch ausreichend sein, geheimen Schlüssel und Zertifikat in zwei unterschiedlichen Dateien abzulegen.

#### 5.2.1 Internet Information Server

Das Zusammenführen von geheimem Schlüssel und Zertifikat wird analog zum Erstellen eines Zertifikatantrags mit Hilfe der IIS-Konsole durchgeführt. Öffnen Sie hierzur die Konsole und klicken Sie im Bereich »Verzeichnissicherheit« auf Serverzertifikat (Abbildung 13). Beachten Sie, dass sich der dann folgende Wizard von dem in Abschnitt 4.2 beschriebenen unterscheidet, da bereits ein Zertifikatantrag generiert wurde.

Klicken Sie im folgenden Wizard auf Ausstehende Anforderung verarbeiten (Abbildung 26).



Abbildung 26: Zusammenführen eines Zertifikats mit dem passenden geheimen Schlüssel im IIS – Schritt 1.

Wählen Sie im nächsten Dialogfeld die Datei mit dem von der KIT-CA ausgestellten Zertifikat aus, das Sie beispielsweise in der Antwortmail der KIT-CA erhalten haben, und klicken Sie auf Weiter.

IIS Certificate Wizard	×
Process a Pending Request Process a pending certificate request by retrieving the file that contains the certification authority's response.	
Enter the path and file name of the file containing the certification autho	rity's response.
Path and file name:	
c:\*.cer	Browse
	<b>_</b>
< <u>B</u> ack <u>N</u> ext>	Cancel

Abbildung 27: Zusammenführen eines Zertifikats mit dem passenden geheimen Schlüssel im IIS – Schritt 2.

Im nächsten Schritt geben Sie den Port ein, auf dem der IIS HTTPS-Anfragen entgegennimmt. In der Regel ist der Port 443 korrekt. Klicken Sie anschließend auf Weiter.

IIS Certificate Wizard		×
SSL Port Specify the SSL port for this web site.		
SSL port this web site should use: 또한		
	< Back Next >	Cancel

Abbildung 28: Zusammenführen eines Zertifikats mit dem passenden geheimen Schlüssel im IIS – Schritt 3.

Schließlich wird nochmals eine Zusammenfassung der im Zertifikat enthaltenen Daten angezeigt. Der Vorgang wird mit einem Klick auf Weiter abgeschlossen.

ertificate Summary You have chosen to	install a certificate from a response file.	
To install the following	ig certificate, click Next.	
File name:	D:\certreq-templates\sccsec-ts-02.cer	
Certificate details: Issued To Issued By Expiration Date Intended Purpose Friendly Name Country/Region State / Province City Organization Organizational Unit	secsec-ts-02.soc.kit.edu KIT-CA 13.09.2012 Server Authentication Request from IIS DE Baden-Vuerttemberg Katrauhe Katrauhe Katrauhe Institute of Technology SCC	
	< Back Next> Can	el :

Abbildung 29: Zusammenführen eines Zertifikats mit dem passenden geheimen Schlüssel im IIS – Schritt 4.

#### 5.2.2 Java Keystore

Bei Venwendung des Java Keystore muss abschließend das von der KIT-CA generierte Zertifikat in den Keystore importiert werden. Dies geschieht mit der folgenden Kommandozeile:

```
keytool -import -trustcacerts \
  -alias <Schluesselname> \
  -file <Zertifikatdatei> \
  -keystore <Keystoredatei>
```

#### 5.2.3 OpenSSL

Unter Linux können geheimer Schlüssel und Zertifikat mit einem einfachen cat-Befehl zusammengeführt werden, wenn Sie im .pem-Format vorliegen:

cat <Zertifikatdatei> <Schluesseldatei> > <Ausgabedatei>

Unter Windows können die . pem-Dateien ebenfalls einfach zusammengefügt werden:

copy <Zertifikatdatei> +<Schluesseldatei> <Ausgabedatei>

Liegen die Dateien nicht im .pem-Format vor, so können sie in der Regel mit Hilfe von OpenSSL in das .pem-Format konvertiert werden. Die Kombinationsmöglichkeiten sind recht vielfältig, so dass hier nur auf die Dokumentation von OpenSSL verwiesen werden kann.

Für manche Anwendungen ist es hilfreich oder sogar notwendig, auch die Zertifikate aller Zwischen-CAs in die Ausgabedatei zu integrieren. Die gesamte Zertifikatkette, bestehend aus den Zertifikaten der KIT-CA, der DFN-CA und der Root-CA der Deutschen Telekom, kann in der Webschnittstelle der KIT-CA heruntergeladen werden (siehe Abschnitt 3.2.2). Es empfiehlt sich in der Regel, die Zertifikatkette zwischen dem eigentlichen Zertifikat und dem geheimen Schlüssel einzufügen:

cat <Zertifikatdatei> <Zertifikatkettendatei> <Schluesseldatei> > <Ausgabedatei>

Obwohl die obige Reihenfolge für die meisten Anwendungen funktionieren dürfte, kann es sein, dass einzelne Anwendungen die Zertifikat- und Schlüsseldaten in einer anderen Reihenfolge in der Gesamtdatei erwarten. In einem solchen Fall muss der cat- oder copy-Befehl entsprechend angepasst werden.

#### 5.2.4 Windows-Kommandozeile

Zusätzlich kann auch bei Windows ein Zertifikat mit Hilfe der Kommandozeile mit dem entsprechenden geheimen Schlüssel zusammengeführt werden. Hierfür geben Sie die folgende Kommandozeile ein:

certreq -accept <Zertifikatdatei>

Hierbei ist <Zertifikatdatei> durch den Namen der Datei zu ersetzen, die das von der KIT-CA ausgestellte Zertifikat enthält. Wird das Zertifikat über die Weboberfläche heruntergeladen, so ist zu beachten, dass es im .pem-Format benötigt wird.

Details des heruntergeladenen Zertifikats können Sie mit folgendem Befehl ansehen:

certutil -dump <Zertifikatdatei>

# 6 Exportieren von Zertifikaten und geheimen Schlüsseln

Wenn Sie Ihr beantragtes Zertifikat erhalten und in Betrieb genommen haben, ist es gerade bei Nutzerzertifikaten sehr ratsam, vom geheimen Schlüssel eine Sicherungskopie anzulegen. Dies ist in mehrerer Hinsicht sinnvoll:

- 1. Sollte aus irgendeinem Grund der geheime Schlüssel verlorengehen oder nicht mehr zugreifbar sein, so existiert eine Sicherung, mit der weiterhin auf verschlüsselte Daten zugegriffen werden kann.
- 2. Das Zertifikat mitsamt zugehörigem geheimen Schlüssel kann mit Hilfe der Kopie auch auf andere Rechner oder in andere Anwendungen importiert werden.

Die genaue Vorgehensweise beim Exportieren hängt davon ab, ob Sie Ihr Zertifikat mit dem Internet Explorer oder mit Mozilla Firefox beantragt und abgeholt haben. Aus diesem Grund werden im folgenden beide Verfahren beschrieben.

#### 6.1 Internet Explorer

Der Internet Explorer legt Nutzerzertifikate nicht in einem eigenen Archiv ab, sondern bedient sich des Windows-Zertifikatspeichers. Wenn Sie Ihr Nutzerzertifikat also mit dem Internet Explorer beantragt und abgeholt haben, werden Ihr Zertifikat und der dazugehörige geheime Schlüssel im Windows-Zertifikatspeicher abgelegt. Um sie von dort zu exportieren, öffnen Sie den Zertifikatmanager, indem Sie das Programm certmgr.msc ausführen; dies kann entweder mit Hilfe einer Kommandozeile oder mit Hilfe des »Ausführen«-Eintrags im Windows-Startmenü erfolgen.

Bitte beachten Sie, dass Serverzertifikate in der Regel nicht in Ihrem persönlichen Zertifikatspeicher, sondern im Zertifikatspeicher für Computerzertifikate abgelegt werden. Auf diesen Zertifikatspeicher kann nicht durch direkten Aufruf von certmgr.msc zugegriffen werden; vielmehr muss hierfür mittels des Zertifikat-Snap-Ins in der Microsoft Management Console (MMC) der entsprechende Zertifikatspeicher ausgewählt werden. Die weiteren Schritte zum Exportieren bleiben jedoch gleich.

Abbildung 30 zeigt den Windows-Zertifikatmanager.

Abbildung 30: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 1.

Erweitern Sie den Punkt »Eigene Zertifikate« und klicken Sie auf Zertifikate.

🐕 certmgr - [Zertifikate - Aktueller	r Benutzer\Eigene Zertifikate\Zertil	ìkate]	
Datei Aktion Ansicht ?			
	3 🖬		
🗐 Zertifikate - Aktueller Benutzer	Ausgestellt für 🔺	Ausgestellt von	Gült
Gigen Zertifikate     Gertüfikate     Ger	PN: Tobies Dussa/Testzertifikat	KIT-CA	21.0
		1	•
Der Speicher Eigene Zertifikate" enthalt 1	Zercirikac.		

Abbildung 31: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 2.

Doppelklicken Sie auf Ihr Zertifikat. Die Zertifikateigenschaften werden angezeigt.

Zertifikat	? ×
Allgemein Details Zertifizierungspfad	
Zertifikatinformationen Dieses Zertifikat ist für folgende Zwecke beabsichtigt: •Schützt E-Mail-Nachrichten	
Ausgestellt für: PN:Tobias Dussa/Testzertifikat	
Ausgestellt von: KIT-CA	
Gültig von 22.04.2010 bis 21.04.2013	
Ausstellerenklärung	
ОК	

Abbildung 32: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 3.

Klicken Sie auf den Reiter Details.

nzeigen: <alle></alle>	•
Feld	Wert
Version	V3
Seriennummer	Of ef ec 94
Signaturalgorithmus	sha1RSA
Aussteller	ca@kit.edu, KIT-CA, Steinbuc
🚍 Gültig ab	Donnerstag, 22. April 2010 17
Gültig bis	Sonntag, 21. April 2013 17:45
Antragsteller	PN:Tobias Dussa/Testzertifikat
Öffentlicher Schlüssel	RSA (2048 Bits)

Abbildung 33: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 4.

Klicken Sie auf In Datei kopieren. Der Export-Wizard öffnet sich.

Zertifikatexport-Assistent	×
	Willkommen
	Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und -sperrlisten vom Zertifikatspeicher auf den Datenträger.
	Ein Zertifikat wird von einer Zertifizierungsstelle ausgestellt und dient der Beetätigung Ihrer Identiktä. Zertifikate enthalten Informationen für den Datenschutz oder für den Aufbau sichterer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichtert werden.
	Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
	Zarick Weiter Mahrechen
	< 20100X Weiter > Abbrechen

Abbildung 34: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 5.

Klicken Sie auf Weiter.



Abbildung 35: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 6.

Markieren Sie die Option »Ja, privaten Schlüssel exportieren« und klicken Sie auf Weiter.



Abbildung 36: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 7.

Setzen Sie die Haken bei

- »Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen« und
- »Verstärkte Sicherheit aktivieren«.

Klicken Sie auf Weiter.



Abbildung 37: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 8.

Geben Sie ein Kennwort ein, mit dem der exportierte geheime Schlüssel geschützt werden soll. Geben Sie es erneut zur Bestätigung ein. Klicken Sie auf Weiter.

Wichtig: Beachten Sie, dass Sie ein Zertifikat mit geheimem Schlüssel nur dann wieder in einen Windows-Keystore importieren können, wenn Sie zuvor beim Exportieren auch ein Kennwort gesetzt haben.

ertifikatexport-Assistent		×
Exportdatei Geben Sie die den Namen der zu exportiere	enden Datei an.	
Dateiname:		
Zertifikat		Durchsuchen
	< Zurück Weiter	> Abbrechen

Abbildung 38: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 9.

Geben Sie einen Dateinamen ein, unter dem das exportierte Zertifikat gespeichert werden soll. Klicken Sie auf Weiter; es erscheint ein Dialog, der alle gewählten Optionen und Einstellungen nochmal zusammenfasst. Klicken Sie auf »Fertig stellen«.

Zertifikatexport-Assistent		×
	Fertigstellen des Assistenten	
	Der Zertifikatexport-Assistent wurde erfolgreich abgeschlossen.	
	Sie haben folgende Einstellungen ausgewählt:	
	Exportschlüssel Ja	
	Alle Zertifikate im Zertifizierungspfad einbeziehen Ja Dateiformat Priv	
1000		
	< Zurück Fertig stellen Abbrech	en

Abbildung 39: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 10.

Der erfolgreiche Export Ihres Zertifikats und Ihres geheimen Schlüssels wird bestätigt.



Abbildung 40: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Windows-Zertifikatspeicher – Schritt 11.

Kopieren Sie die Datei mit Ihrem Zertifikat und geheimem Schlüssel an einen sicheren Ort.

### 6.2 Mozilla Firefox

Wenn Sie Ihr Nutzerzertifikat mit dem Mozilla Firefox beantragt und abgeholt haben, ist es in Ihrem Firefox-Benutzerprofil abgelegt und kann von dort exportiert werden. Klicken Sie hierzu auf den Menüpunkt Einstellungen im Menü Extras.

🥹 Mozilla Firefox			
Datei Bearbeiten Ansicht ⊆hronik Lesezeichen	E <u>x</u> tras <u>H</u> ilfe		
CD-CXA	Web-Syche	Strg+K	→ • Google
🔎 Meistbesuchte Seiten 🌪 Erste Schritte 🔝 Aktuelle	Downloads Add-ons	Strg+J	
(Unbenannt) ÷	Java Console		-
	Fehlerkonsole Str Seiteninformationen	rg+Umschalt+J	
	Privaten Modus starten Str. Neueste Chronik löschen Strg+	g+Umschalt+P Umschalt+Entf	
	Einstellungen		

Abbildung 41: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Mozilla Firefox – Schritt 1.

Klicken Sie auf das Feld Erweitert und dann auf den Reiter Zertifikate anzeigen.

Einstellungen	1						×
		۵. ج		90		i.	
Allgemein	Tabs	Inhalt	Anwendungen	Datenschutz	Sicherheit	Erweitert	
Allgemein N	letzwerk	Update	Verschlüsselung				
Protokolle							
🔽 55L 3	.0 verweni	den		TLS 1.0 verwer	nden		
Zertifikate							
Wenn eine	e Website r	nach dem	persönlichen Sicher	heitszertihikat ve	rlangt:		
C Autor	natisch ein:	s <u>w</u> ählen	Jedes Mal fra	igen			
		_					
Zertifikat	e anzeiger	Zert	fikatsperrliste	alidierung K	ryptographie	-Module	
				ОК 4	Abbrechen	Hilfe	

Abbildung 42: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Mozilla Firefox – Schritt 2.

Wählen Sie Ihr Zertifikat aus und klicken Sie auf Sichern.

Zertifikat-Mar	nager					
Ihre Zertifikate	Personen	Server 2	ertifizierungsstellen	Andere		
Sie haben Zerti	ifikate dieser	r Organisati	onen, die Sie identifiz	ieren:		
Zertifikatsnam	ne		Kryptographie	Seriennummer	Läuft ab am	EŞ.
🖃 Karlsruhe In	stitute of Te	echnology				
PN: Tobi	as Dussa/Te	stzertifikat	Software-Sicherh	0F:EF:EC:94	21.04.2013	
Ansehen	Sichern.	<u>A</u> lle	sichern Importi	eren Löschen		
						ОК

Abbildung 43: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Mozilla Firefox – Schritt 3.

Geben Sie einen Dateinamen ein, unter dem Ihr Zertifikat und Ihr geheimer Schlüssel gespeichert werden sollen. Klicken Sie auf Speichern.

Dateiname für E	lackup					? ×
Speichern in	🞯 Desktop		•	3 🕫	بي 🥲	
Zuletzt verwendete D Desktop Eigene Dateien	Eigene Dateier	bung				
Netzwerkumge	, Dateiname:	Zertifikat			•	Speichern
Бung	Dateityp:	PKCS12-Dateien			-	Abbrechen

Abbildung 44: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Mozilla Firefox – Schritt 4.

Geben Sie ein Kennwort ein, mit dem Ihr exportierter geheimer Schlüssel geschützt werden soll. Geben Sie es erneut zur Bestätigung ein. Im unteren Bereich gibt ein Statusbalken grob die Güte des von Ihnen

eingegebenen Passwortes an; der Balken sollte so breit wie möglich sein, mindestens aber drei Viertel der Breite ausfüllen. Klicken Sie auf OK.

Wählen Sie ein Zertifikats-Backup-Passwort	×
Das Zertifikats-Backup-Passwort, das Sie hier festlegen, schützt die Ba erstellen. Sie müssen dieses Passwort festlegen, um mit dem Backup fe	ckup-Datei, die Sie im Moment ortzufahren.
Zertifikats-Backup-Passwort:	
Zertifikats-Backup-Passwort (nochmals):	
Wichtig: Wenn Sie Ihr Zertifikats-Backup-Passwort vergessen, können wiederherstellen. Bitte schreiben Sie es an einem sicheren Platz nieder	Sie dieses Backup später nicht
Passwort-Qualitätsmessung	
	OK Abbrechen

Abbildung 45: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Mozilla Firefox – Schritt 5.

Der erfolgreiche Export wird mit einer separaten Dialogbox gemeldet.

Warnung	) ×
1	Ihre Sicherheits-Zertifikate und privaten Schlüssel wurden erfolgreich gesichert.
	ОК

Abbildung 46: Exportieren eines Zertifikats mit geheimem Schlüssel aus dem Mozilla Firefox – Schritt 6.

Kopieren Sie die Datei mit Ihrem Zertifikat und geheimem Schlüssel an einen sicheren Ort.