

DFN-PKI

Jürgen Brauckmann

DFN-CERT Services GmbH

dfnpca@dfn-cert.de

Arbeitskreis Verzeichnisdienste ZKI

Frankfurt, 05.10.2005

- **Ziele der DFN-PKI**
- **Dienstleistungs-Modelle**
- **DFN-PKI-2**
- **Vorführung DFN-PKI-2**
- **Zusammenfassung**

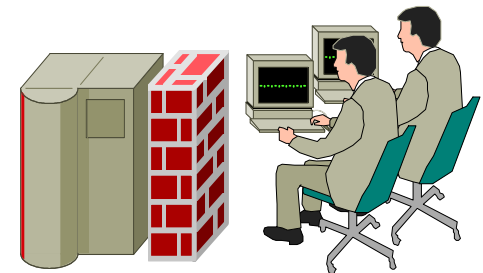
- Dienstleistungen rund um X.509 Zertifikate
 - Baustein für Identity Management
- Gemeinsamer Vertrauensanker /
gemeinsames Sicherheitsniveau für das
Deutsche Forschungsnetz
- Verschiedene Möglichkeiten der
Teilnahme für eine Hochschule
- Ausstellen von Zertifikaten für das D-Grid

- DFN-PKI-1:
 - Hochschule betreibt komplette Zertifizierungsstelle selbst
 - CA-Zertifikat vom DFN-Verein
 - Eigene Technik
 - Hoher Aufwand bei der Hochschule erforderlich

- Registrierungsstelle
 - Genehmigung von Zertifikatanträgen
 - Administrative Arbeiten
 - Verbleibt in der Hochschule



-
- Zertifizierungsstelle
 - Erzeugung der Zertifikate
 - Technisch aufwändige Arbeiten
 - Auslagerung an DFN möglich



- DFN-PKI-2:
 - Hochschule nimmt Aufgaben der Registrierungsstelle wahr
 - DFN-Verein erfüllt Aufgaben der Zertifizierungsstelle im Auftrag und Namen der Hochschule
 - Technik für Registrierung/Zertifizierung wird vom DFN-Verein betrieben
 - SSL-gesicherte Web-Schnittstellen für die Beantragung und Registrierung

- Organisatorisch:
 - Vertrauenswürdigen Personal
 - Entgegennahme, Prüfung und Freigabe von Anträgen
 - Identifizierung
- Technisch:
 - Abschließbarer Raum
 - PC mit Internetverbindung

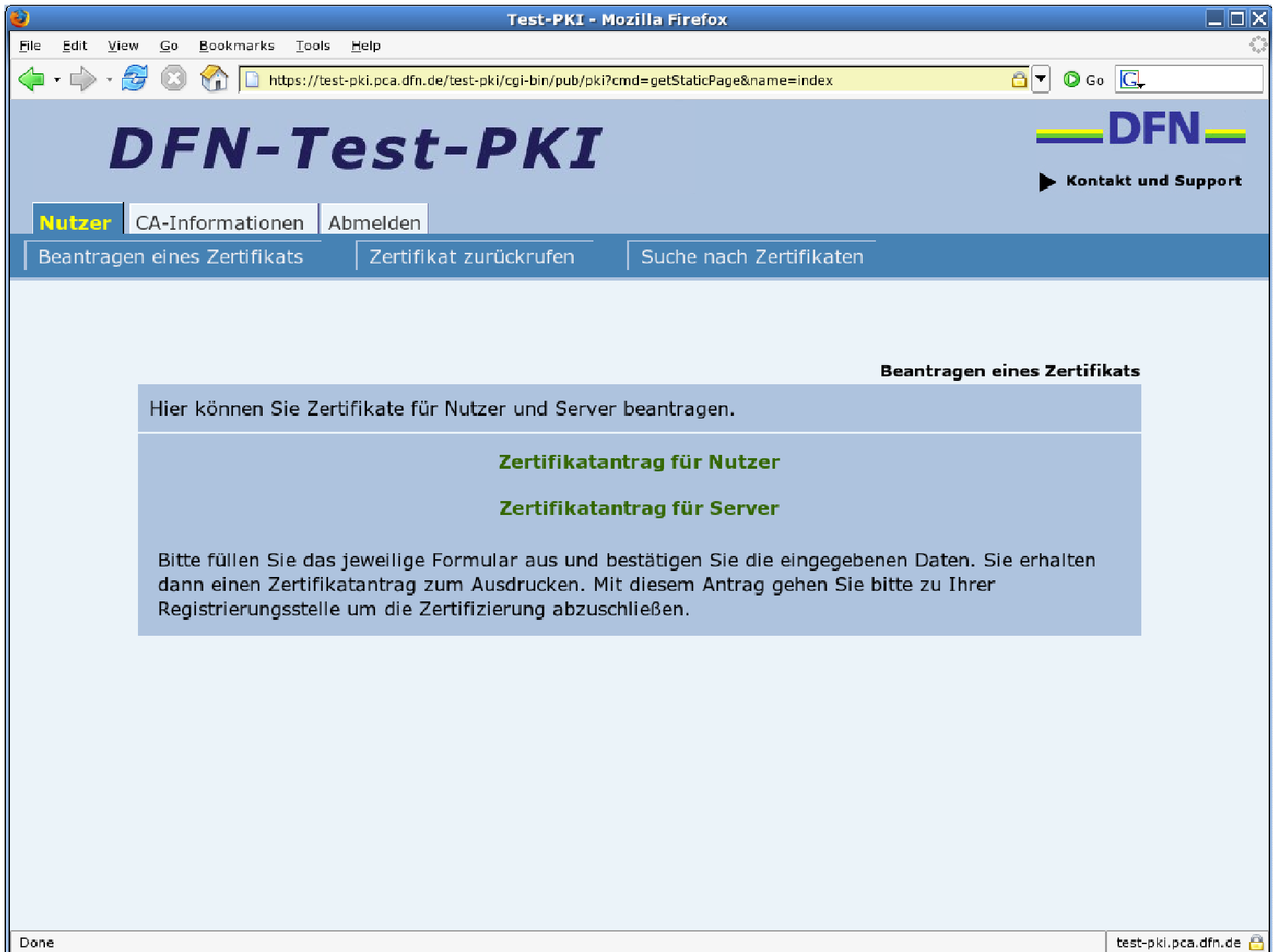
- Beauftragung durch Vertreter der Einrichtung
- Abstimmung der technischen Details
- Persönliche Identifizierung eines Mitarbeiters der Einrichtung durch die DFN-PCA
- Aufsetzen der Zertifizierungsstelle inkl. Erzeugung des CA-Zertifikats

Vorführung der DFN-PKI-2

Schritt 1

Nutzer beantragt Zertifikat







Test-PKI - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://test-pki.pca.dfn.de/test-pki/cgi-bin/pub/pki?cmd=getStaticPage&name=index

DFN-Test-PKI

 **DFN**

 **Kontakt und Support**

Nutzer CA-Informationen Abmelden

Beantragen eines Zertifikats | Zertifikat zurückrufen | Suche nach Zertifikaten

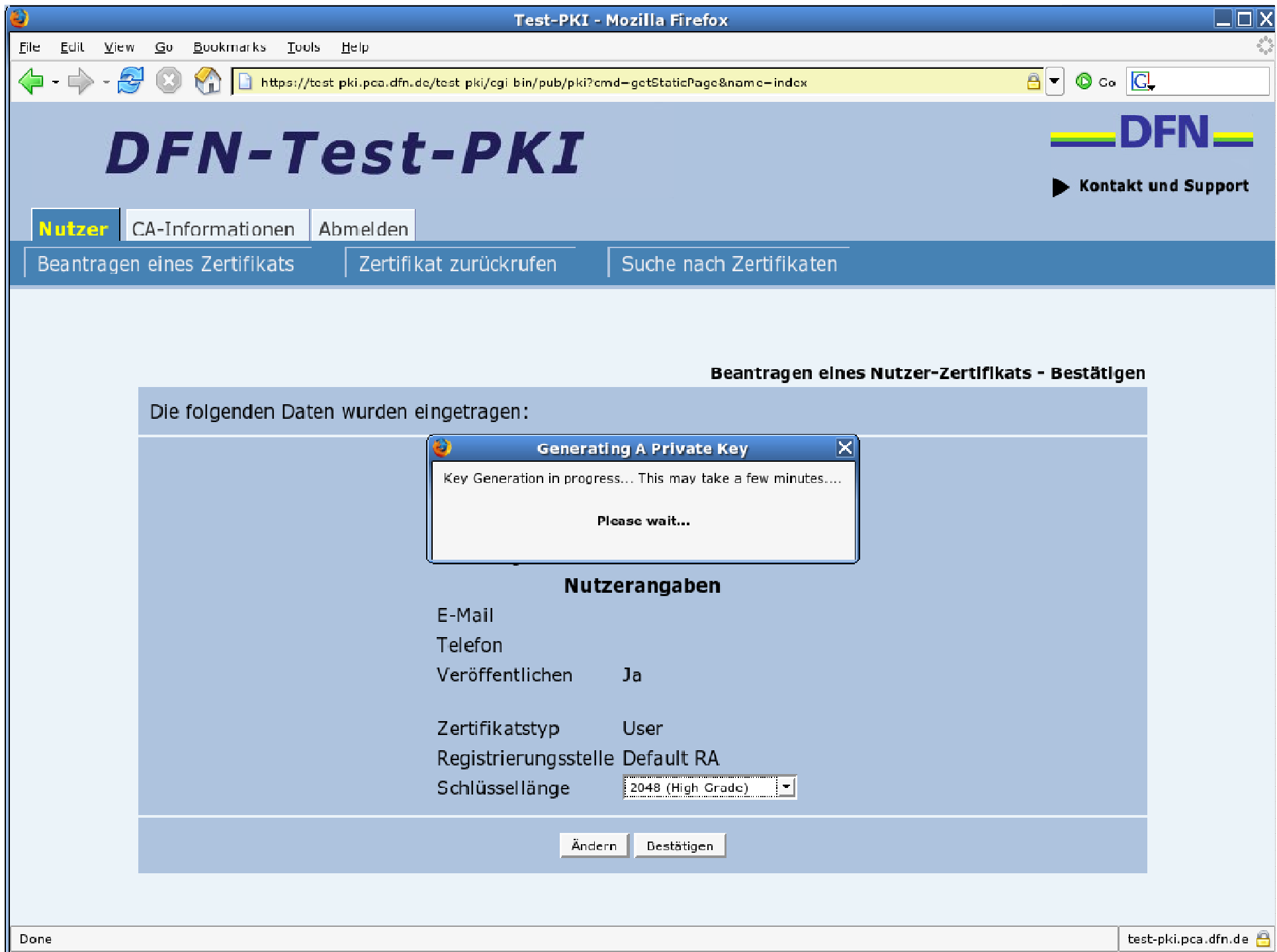
Beantragen eines Nutzer-Zertifikats

Bitte geben Sie Ihre Daten ein. Felder, die mit einem Stern (*) markiert sind, müssen ausgefüllt werden.

Zertifikatsdaten	
E-Mail *	<input type="text" value="brauckmann@dfn-cert.de"/>
Name *	<input type="text" value="Juergen Brauckmann"/>
Abteilung	<input type="text"/>

Nutzerangaben	
Bitte geben Sie hier zusätzliche Kontaktdaten ein:	
E-Mail	<input type="text"/>
Telefon	<input type="text"/>
PIN (Mindestens 8 beliebige Zeichen) *	<input type="password" value="*****"/>
Nochmalige Eingabe der PIN zur Bestätigung *	<input type="password" value="*****"/>
Die PIN wird von Ihnen benötigt, um sich gegenüber dem Zertifizierungssystem zu autorisieren, z.B. wenn Sie Ihr Zertifikat sperren wollen. Bitte notieren Sie sich die PIN.	
Ich stimme den AGB zu (Zertifizierungsrichtlinie) *	<input checked="" type="checkbox"/>
Ich stimme der Veröffentlichung des Zertifikats zu.	<input checked="" type="checkbox"/>
Wenn Sie der Veröffentlichung nicht zustimmen, wird Ihr Zertifikat nicht im Verzeichnisdienst zur Verfügung stehen.	

Done test-pki.pca.dfn.de




Test-PKI - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://test-pki.pca.dfn.de/test-pki/cgi-bin/pub/pki?cmd=getStaticPage&name=index

Go

DFN-Test-PKI


Kontakt und Support

Nutzer

CA-Informationen

Abmelden

Beantragen eines Zertifikats

Zertifikat zurückrufen

Suche nach Zertifikaten

Bitte drucken Sie diese Seite aus, unterschreiben Sie sie und legen Sie diese bei Ihrer Registrierungsstelle vor, um die Antragsstellung abzuschließen. Der Druckdialog sollte sich automatisch in wenigen Sekunden öffnen.

DFN-Test-PKI

Ich versichere, dass sämtliche Angaben im Antrag vollständig sind und der Wahrheit entsprechen.

Ich kenne die gültigen Zertifizierungs-Richtlinien und die Erklärung zum Zertifizierungsbetrieb und stimme ihnen zu.

Ich stimme der Verarbeitung und Speicherung der bei der Zertifizierung anfallenden Daten zu. Die Daten werden gemäß den geltenden Datenschutzbestimmungen vertraulich behandelt.

Seriennummer des Antrags: 28704

Eindeutiger Name: emailAddress=brauckmann@dfn-cert.de,CN=Juergen Brauckmann,O=Test-PKI,C=DE

Public Key Fingerprint: 1D:46:70:D6:6D:50:5A:01:6D:F2:1A:B1:4D:7C:26:A5:7A:62:B0:95

Schlüssellänge: 2048

Veröffentlichen: Ja

Datum und Ort: _____

Eigenhändige Unterschrift: _____

Art des Ausweises: _____

Ausweis gültig bis: _____

Ausweis geprüft:

Datum, Unterschrift RA-Administrator(in): _____

Done

test-pki.pca.dfn.de

Schritt 2

Registrierungsstelle (RA)



Test-PKI - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

←

→

↻

✕

🏠

📄

https://test-pki.pca.dfn.de/test-pki/cgi-bin/ra/RAServer?cmd=getStaticPage&name=index

🔒

Go

🔍

DFN-Test-PKI

DFN

▶ Kontakt und Support

Zertifikatanträge

Rückrufanträge

Zertifikate

CA-Zertifikate

Zertifikat-Sperrlisten

Hilfsmittel

Abmelden

Neu

Erneuert

In Bearbeitung

Genehmigt

Archiviert

Gelöscht

Neue Zertifikatanträge

Mittwoch, den 28. September 16:26:32

Antragsnummer	Antragssteller	Übermittelt am	Beantragte Rolle
28704	emailAddress=brauckmann@dfn-cert.de,CN=Juergen Brauckmann,O=Test-PKI,C=DE	Wed Sep 28 14:20:56 2005 UTC	User

https://test-pki.pca.dfn.de/test-pki/cgi-bin/ra/RAServer?cmd=raList;dataType=NEW_REQUEST


test-pki.pca.dfn.de

Test-PKI - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://test-pki.pca.dfn.de/test-pki/cgi-bin/ra/RAserver?cmd=getStaticPage&name=index

DFN-Test-PKI

 **Kontakt und Support**

Zertifikatanträge Rückrufanträge Zertifikate CA-Zertifikate Zertifikat-Sperrlisten Hilfsmittel Abmelden

Neu Erneuert In Bearbeitung Genehmigt Archiviert Gelöscht

Neuer Zertifikatantrag

Mittwoch, den 28. September 16:27:20

Feld	Wert
Antragsnummer	28704
Veröffentlichen	Ja
Name	Juergen Brauckmann
E-Mail	brauckmann@dfn-cert.de
Alternativer Name des Zertifikats	email.0=brauckmann@dfn-cert.de
Zertifikatstyp	User
Gültigkeit (Tage)	nicht vorhanden
Gültigkeitsbeginn	nicht vorhanden
Gültigkeitsende	nicht vorhanden
Gültigkeitsprüfung	Gültigkeit wäre OK
Eindeutiger Name	CN=Juergen Brauckmann,O=Test-PKI,C=DE
Übermittelt am	Wed Sep 28 14:20:56 2005 UTC
Benutzte PIN zur Identifizierung	016b4cd38218617dae472b59f68d9cddf10e5a6c
Schlüssellänge	2048
Algorithmus des öffentlichen Schlüssels	rsaEncryption

Done test-pki.pca.dfn.de

Test-PKI - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://test-pki.pca.dfn.de/test-pki/cgi-bin/ra/RA_Server?cmd=getStaticPage&name=index

DFN-Test-PKI

DFN

Kontakt und Support

Zertifikatanträge Rückrufanträge Zertifikate CA-Zertifikate Zertifikat-Sperrlisten Hilfsmittel Abmelden

Neu Erneuert In Bearbeitung Genehmigt Archiviert Gelöscht

Gültigkeitsprüfung	Gültigkeit wäre OK
Eindeutiger Name	CN=Juergen Brauckmann,O=Test-PKI,C=DE
Übermittelt am	Wed Sep 28 14:20:56 2005 UTC
Benutzte PIN zur Identifizierung	016b4cd38218617dae472b59f68d9cddf10e5a6c
Schlüssellänge	2048
Algorithmus des öffentlichen Schlüssels	rsaEncryption
Public Key Fingerprint	1D:46:70:D6:6D:50:5A:01:6D:F2:1A:B1:4D:7C:26:A5:7A:62:B0:95
Öffentlicher Schlüssel	Öffentlichen Schlüssel ansehen
Signaturalgorithmus	nicht vorhanden
Zertifikate mit demselben DN	123337441
Name (Vor- und Nachname)	nicht vorhanden
E-Mail	nicht vorhanden
Abteilung	nicht vorhanden
Telefon	nicht vorhanden

Operationen

Antrag **genehmigen** und digital signieren

Antrag **genehmigen** ohne ihn digital zu signieren

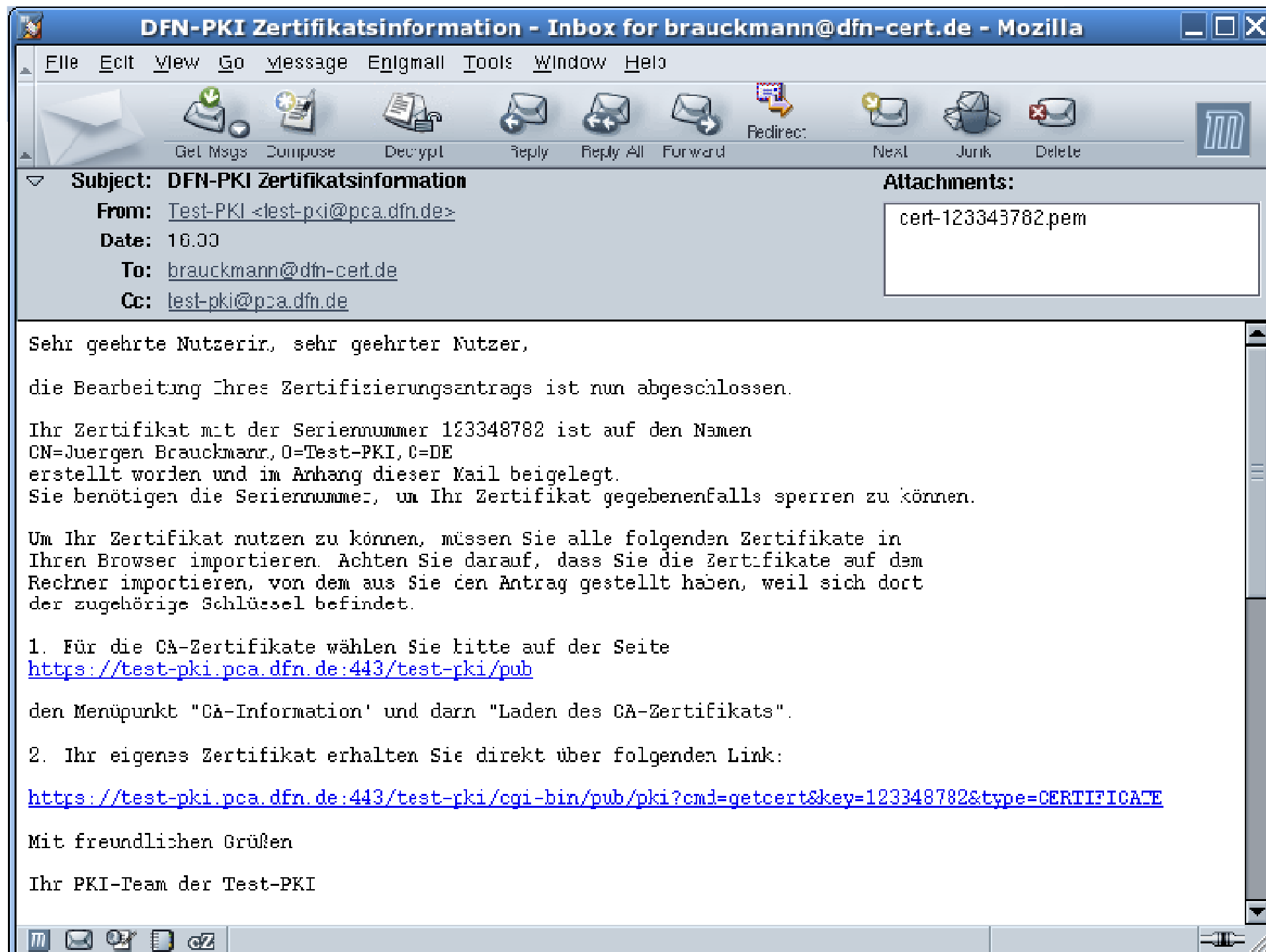
Bearbeiten des Antrags

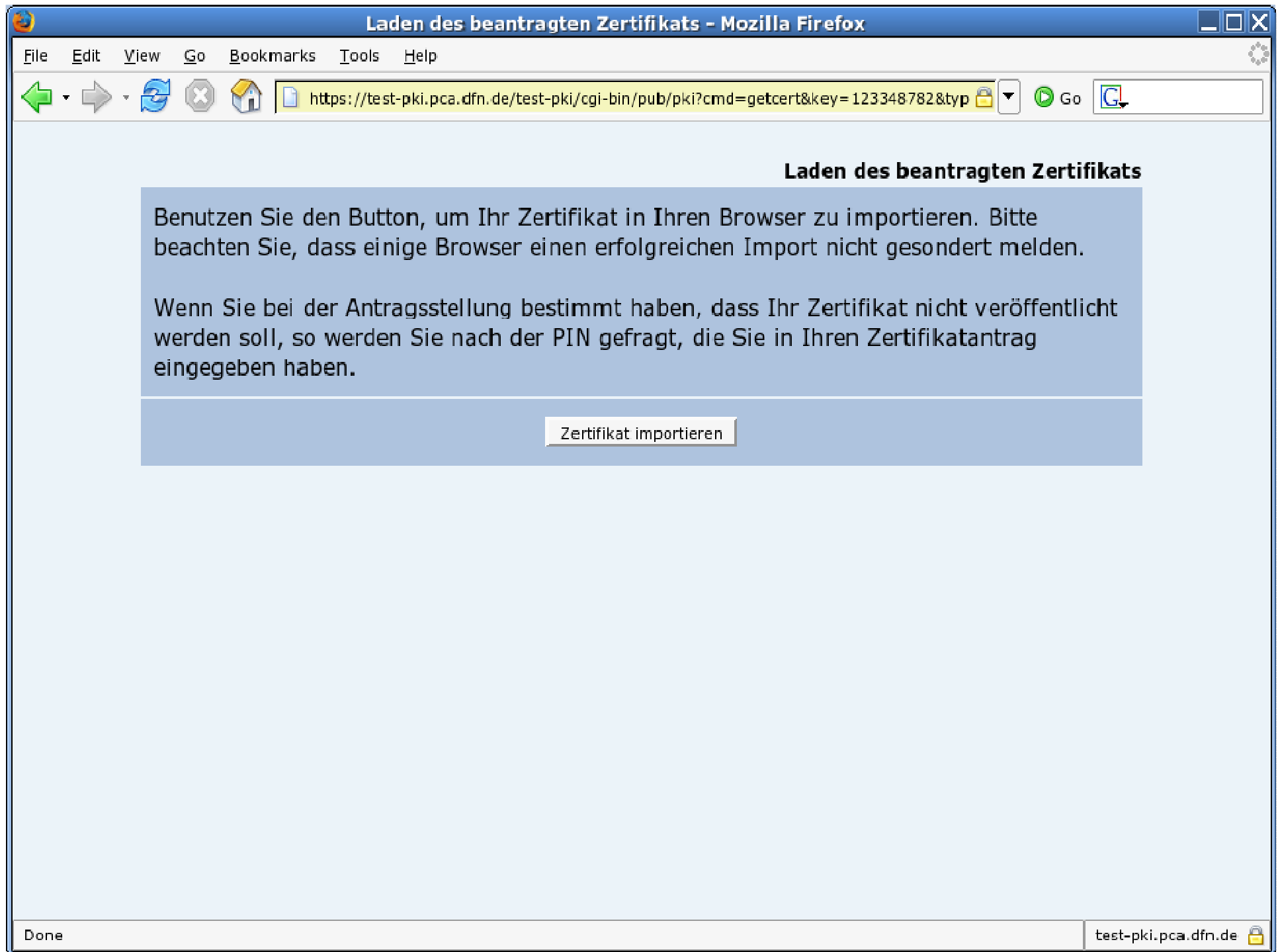
Lösche Antrag

Done test-pki.pca.dfn.de

Schritt 3

Nutzer erhält sein Zertifikat





Laden des beantragten Zertifikats - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://test-pki.pca.dfn.de/test-pki/cgi-bin/pub/pki?cmd=getcert&key=123348782&typ

Laden des beantragten Zertifikats

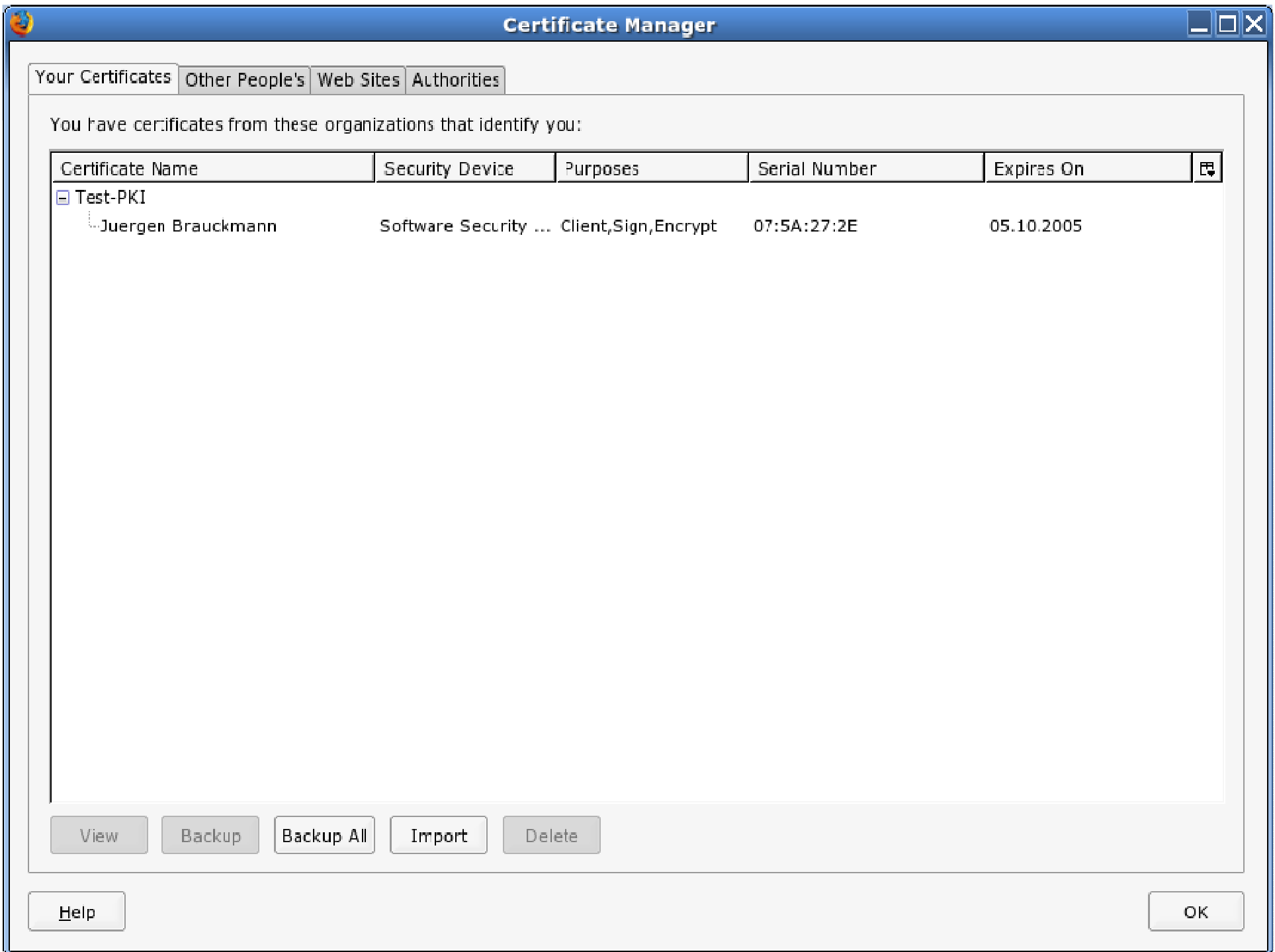
Benutzen Sie den Button, um Ihr Zertifikat in Ihren Browser zu importieren. Bitte beachten Sie, dass einige Browser einen erfolgreichen Import nicht gesondert melden.

Wenn Sie bei der Antragsstellung bestimmt haben, dass Ihr Zertifikat nicht veröffentlicht werden soll, so werden Sie nach der PIN gefragt, die Sie in Ihren Zertifikatantrag eingegeben haben.

Zertifikat importieren

Done

test-pki.pca.dfn.de



- Zum Ausprobieren der Prozesse
- DFN-Test-PKI steht allen Anwendern zur Verfügung
- Bei Interesse Zugangskennung unter:

pki@dfn.de

- Hohe Qualität / Sicherheit
- Auslagerung der Zertifizierungsstelle
 - Keine eigene Spezial-Technik erforderlich
 - Lokaler Aufwand deutlich reduziert
 - Webschnittstelle anpassbar
 - Entgelt im DFNInternet enthalten
- Regelbetrieb ab 1.1.2006 mit Übergang auf das X-WiN (www.dfn.de/pki)

- DFN-PKI-1:
 - Regelbetrieb läuft
- DFN-PKI-2:
 - Pilotbetrieb läuft
 - Test-PKI als Demo-System verfügbar
- Zertifikate für D-Grid

- DFN-PKI-2:
 - Regelbetrieb ab 1.1.2006
 - Erweiterung im nächsten Jahr:
 - Schnittstelle für hohe Zertifikatzahlen („Alle Studenten“)
 - Laufzeit Zertifikatausstellung < 1 Stunde
 - Hardware Token bei Benutzern
- Wurzelzertifikat in Browser:
 - Thema wird bearbeitet – aber schwierig

- Dienstleistungsangebote DFN-PKI-1 und DFN-PKI-2
- Auslagerung von technisch aufwändigen Systemen und Vorgängen an den DFN-Verein in der DFN-PKI-2
- DFN-Test-PKI zum Ausprobieren:

pki@dfn.de

Danke für Ihre Aufmerksamkeit!

Jürgen Brauckmann
DFN-CERT Services GmbH
dfnpca@dfn-cert.de