

Funktionsweise & Schnittstellen der DFN-PKI

Jürgen Brauckmann
brauckmann@dfn-cert.de

- Einführung
- Organisation und Technik
- Beispiele

Einführung

Warum PKI?

- Authentifizierung, Signatur, Verschlüsselung
- Dokumentiert nach außen eine Aussage über Zuverlässigkeit von Prozessen (Policy)
- Kann Aufwand sparen
- Sicherer als andere Verfahren

Warum Smartcards?

- Sicherheit: Besitz und Wissen
- Usability (PKI wird „versteckt“)

Was ist die DFN-PKI?

- PKI für DFN-Anwender
- Mehr als 320 teilnehmende Einrichtungen
- Root im Browser
- Organisatorisches Rahmenwerk durch DFN-PKI-Policy
- Anforderungen von Dritten, die eingehalten werden müssen

Wie hilft die DFN-PKI? 1. Sichere Webserver



DFN-PKI: Überblick DFN-PKI - Mozilla Firefox

https://www.pki.dfn.de/

DFN
Deutsches
Forschungsnetz

Überblick DFN-PKI

Überblick DFN-PKI

Der DFN-Verein organisiert mit dem Dienst DFN-PKI eine Public Key Infrastruktur, um digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Dabei werden fortgeschrittene Zertifikate auf Basis des X.509 Standards verwendet.

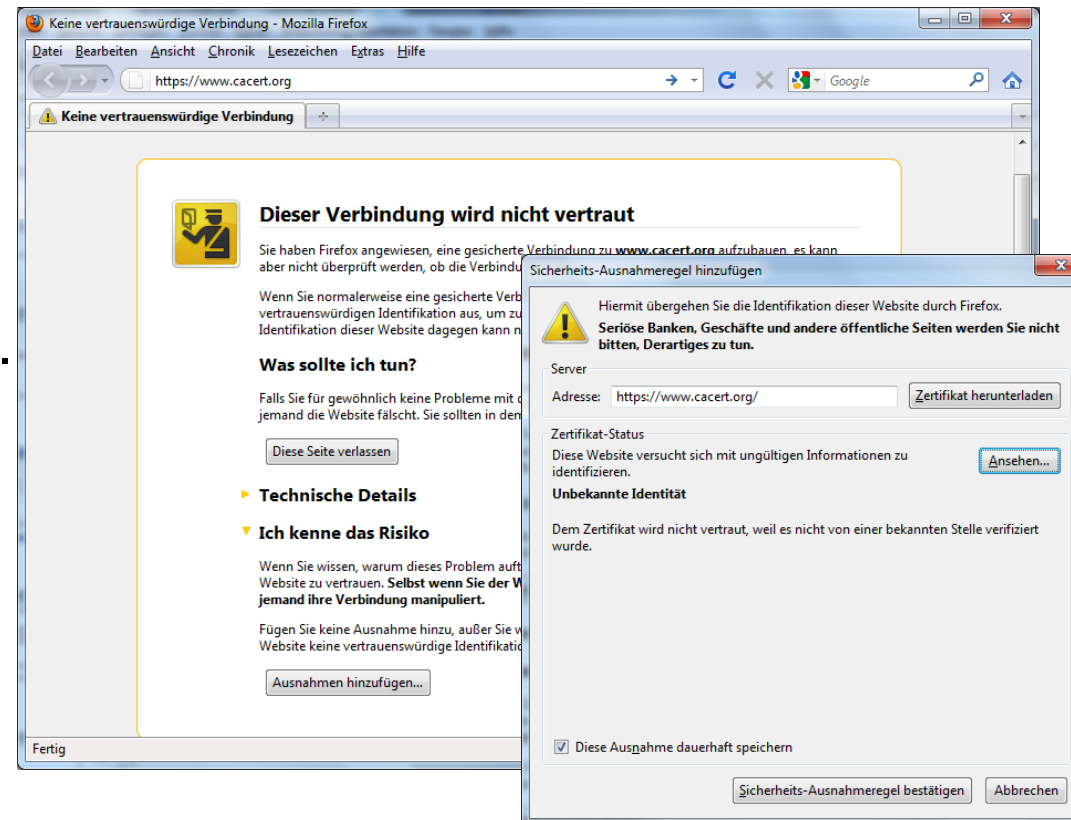
Viele Hochschulen und wissenschaftliche Einrichtungen setzen Zertifikate für eine sichere Kommunikation ein, dabei sind die Voraussetzungen und Anforderungen sehr unterschiedlich. Der Dienst DFN-PKI bietet deshalb folgende Möglichkeiten zur Lösung der technischen und organisatorischen Aufgaben an:

- [Auslagerung einer Zertifizierungsstelle an den DFN-Verein](#)
- [Ausstellung von Grid Zertifikaten](#)
- [Ausstellung von Zertifikaten für die DFN-AAI](#)

Für alle Lösungen übernimmt der DFN-Verein im Rahmen von DFN-PKI den technischen Betrieb zentraler Komponenten und bietet für die lokalen Komponenten technische und organisatorische Unterstützung an.

DFN-PKI ist im Dienst DFNInternet enthalten und kann damit von DFN-Anwendern ohne zusätzliches Entgelt genutzt werden.

VS.



Keine vertrauenswürdige Verbindung - Mozilla Firefox

https://www.cacert.org/

Keine vertrauenswürdige Verbindung

Dieser Verbindung wird nicht vertraut

Sie haben Firefox angewiesen, eine gesicherte Verbindung zu www.cacert.org aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung eine Sicherheits-Ausnahmeregel hinzufügen

Wenn Sie normalerweise eine gesicherte Verbindung mit vertrauenswürdiger Identifikation aus, um zu identifizieren, diese Website dagegen kann nicht

Was sollte ich tun?

Falls Sie für gewöhnlich keine Probleme mit der Verbindung haben, können Sie diese Seite verlassen. Falls Sie jemand die Website fälscht, Sie sollten in den

Technische Details

Ich kenne das Risiko

Wenn Sie wissen, warum dieses Problem auftritt, können Sie diese Website zu vertrauen. **Selbst wenn Sie der Website keine vertrauenswürdige Identifikation**

Fügen Sie keine Ausnahme hinzu, außer Sie wissen, dass die Website keine vertrauenswürdige Identifikation

Hiermit übergehen Sie die Identifikation dieser Website durch Firefox.
Seriöse Banken, Geschäfte und andere öffentliche Seiten werden Sie nicht bitten, Derartiges zu tun.

Server

Adresse:

Zertifikat-Status

Diese Website versucht sich mit ungültigen Informationen zu identifizieren.

Unbekannte Identität

Dem Zertifikat wird nicht vertraut, weil es nicht von einer bekannten Stelle verifiziert wurde.

Diese Ausnahme dauerhaft speichern

Wie hilft die DFN-PKI?

2. Anmeldung an Portalen

Kartenauthentisierung - Mozilla Firefox

tu-berlin.de https://aagw.tubit.tu-berlin.de/unsafe/Karte.html?APP=t3portal

Kartenauthentisierung

Technische Universität Berlin

TUB-Chipkarten-Authentisierung

Impressum

Anmeldevorgang

Impressum

Anmeldung mit Chipkarte

Legen Sie bitte die Karte in das Lesegerät und klicken den folgenden Link:

[Anmelden mit Chipkarte](#)

Hinweise zum persönlichen Portal:

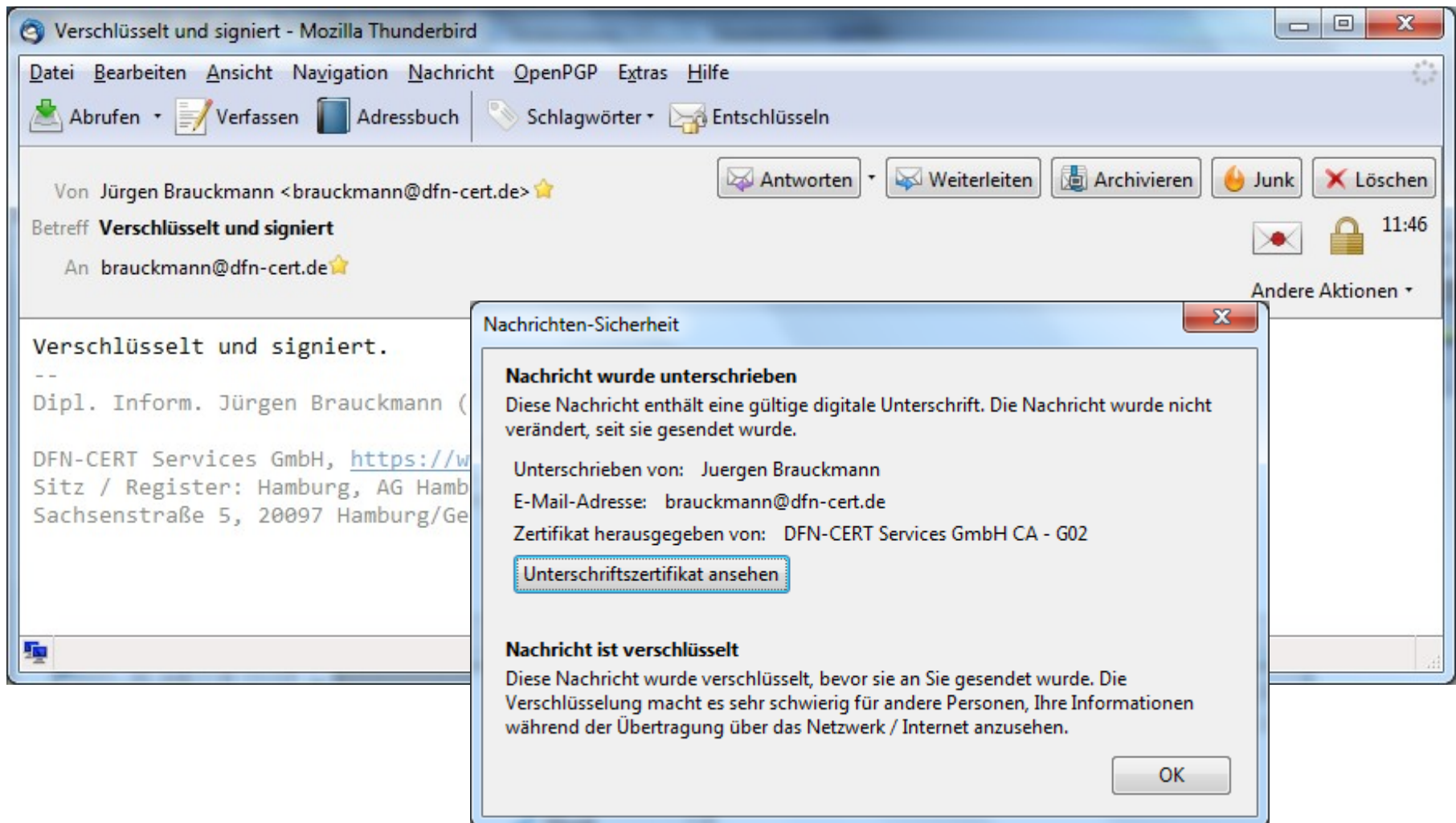
Sie benötigen zur Anmeldung am persönlichen Portal ein tubIT-Nutzerkonto. Diese werden im Rahmen des Provisioning vergeben. Weitere Informationen zum Provisioning finden Sie unter http://www.tubit.tu-berlin.de/menu/dienste/konto_karte/provisioning/.

Um Hinweise des Browser (insbesondere des Internet Explorers) auf ungültige Zertifikate zu unterbinden, installieren Sie bitte die benötigten Zertifikate im Browser, indem Sie auf die folgenden Links klicken: <https://pki.pca.dfn.de/tu-berlin-ca/pub/cacert/cacert.crt> und <https://pki.pca.dfn.de/tu-berlin-ca/pub/cacert/rootcert.crt>. Informationen zu diesen Zertifikaten erhalten Sie unter der URL <http://ca.tu-berlin.de/>.

Fertig

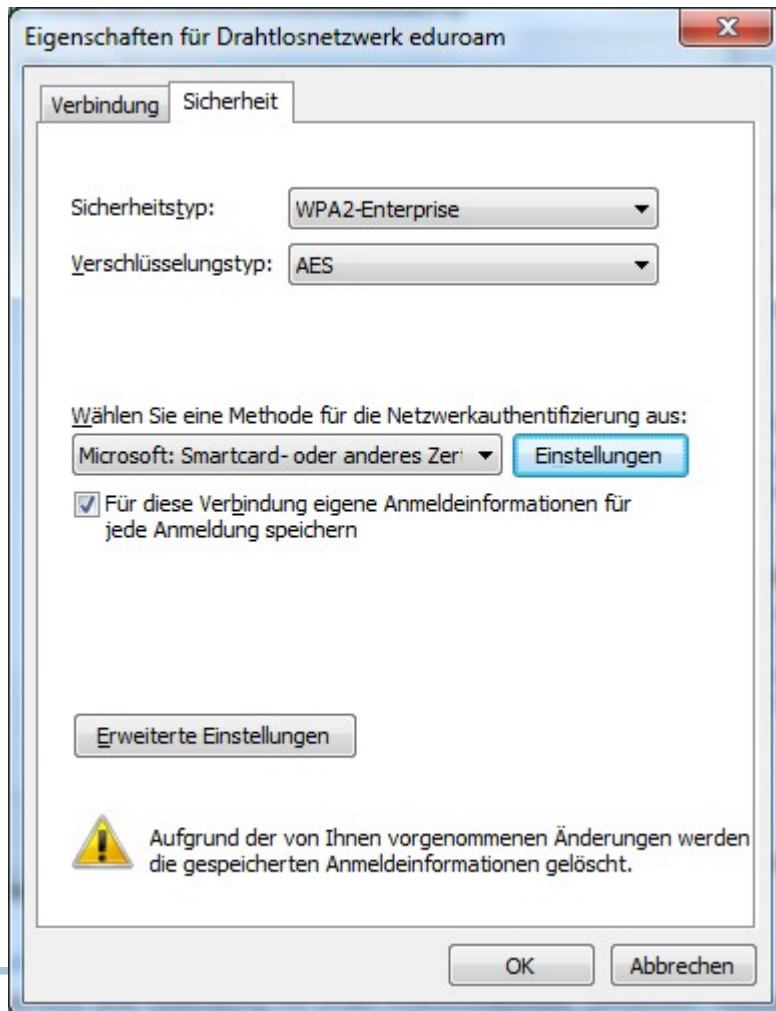
Wie hilft die DFN-PKI?

3. Email-Signatur und -Verschlüsselung



Wie hilft die DFN-PKI?

4. Authentifizierung am WLAN (802.1X) und am Betriebssystem



Organisation und Technik

Erstellung von Zertifikaten zentral bei DFN-PCA in Hamburg:

- CA-Schlüssel im HSM
- Datenbank mit Zertifikatdaten
- Sperrlistenerzeugung und OCSP

Registrierungsstelle in der Hochschule:

- Identifizierung von Zertifikatnehmern
- Ggf. Erzeugung von Schlüsseln
- Prüfung und Genehmigung von Zertifikatanträgen
- Archivierung

Aufgabenteilung zwischen RA/CA:

- Zertifizierung in der DFN-PKI ist **Funktionsübertragung an den DFN-Verein**
- Daher evtl. Ergänzung der Studienordnung o.ä. nötig

Verpflichtung:

- Einhaltung der DFN-PKI Policy

„Überwacher“:

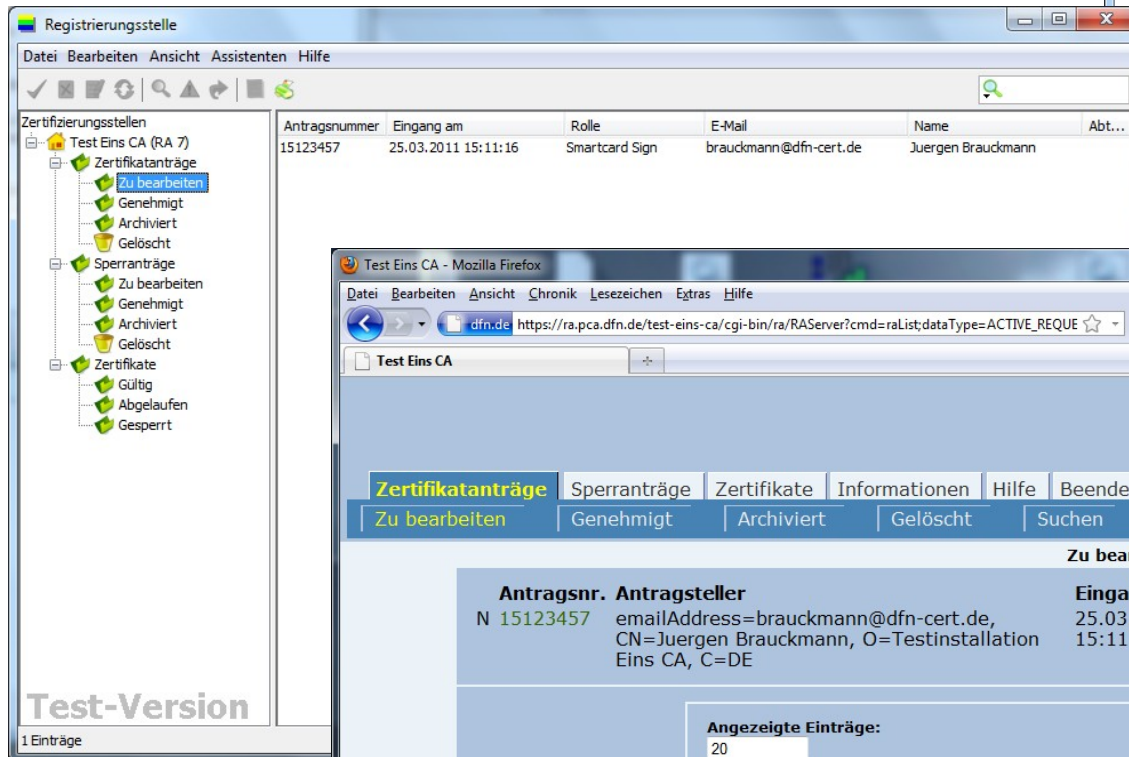
- DFN-PCA
- T-Systems
- Browserhersteller (Mozilla...)

Kernpunkte:

- Persönliche Identifizierung des Zertifikatnehmers
- Email-Adressen und Webservernamen nachweisbar korrekt
- Missbrauch der geheimen Schlüssel verhindern
=> Sichere Übergabe von Smartcards, PIN-Schutz und sichere PIN-Briefe
- Archivierung von Unterlagen
- Sperrung von Zertifikaten

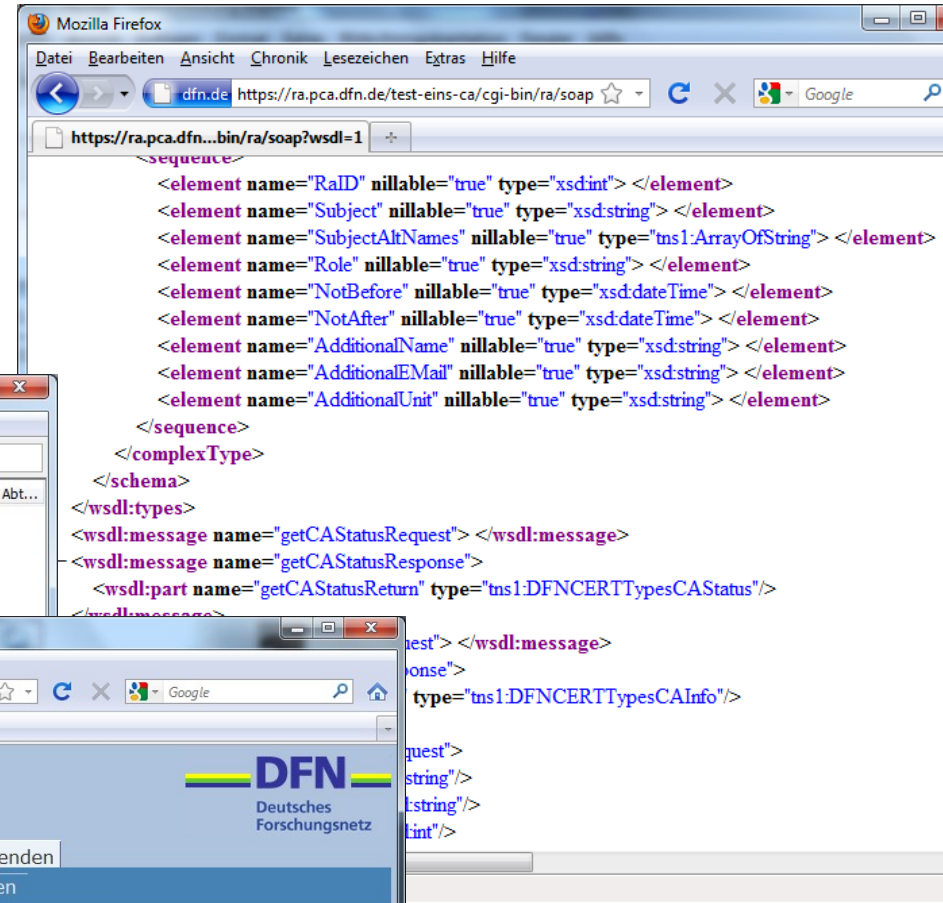
Schnittstellen für die Registrierungsstelle:

- Webseiten
- Java RA-Oberfläche
- WebServices (SOAP)



The screenshot shows the 'Registrierungsstelle' web application. It features a navigation tree on the left with categories like 'Zertifizierungsstellen', 'Zertifikatanträge', 'Sperranträge', and 'Zertifikate'. The main area displays a table of certificate requests. Below the table, there are tabs for 'Zertifikatanträge', 'Sperranträge', 'Zertifikate', 'Informationen', 'Hilfe', and 'Beenden'. A detailed view of a certificate request is shown below the table, including fields for 'Antragsnr.', 'Antragsteller', 'Eingangsdatum', and 'Rolle'. The interface is labeled 'Test-Version' and '1 Einträge'.

Antragsnummer	Eingang am	Rolle	E-Mail	Name	Abt...
15123457	25.03.2011 15:11:16	Smartcard Sign	brauckmann@dfn-cert.de	Juergen Brauckmann	



The screenshot shows a Mozilla Firefox browser window displaying SOAP XML data. The URL is `https://ra.pca.dfn.de/test-eins-ca/cgi-bin/ra/soap`. The XML content includes a sequence of elements such as `RaID`, `Subject`, `SubjectAltNames`, `Role`, `NotBefore`, `NotAfter`, `AdditionalName`, `AdditionalEMail`, and `AdditionalUnit`. The XML is structured as follows:

```
<sequence>
  <element name="RaID" nillable="true" type="xsd:int"> </element>
  <element name="Subject" nillable="true" type="xsd:string"> </element>
  <element name="SubjectAltNames" nillable="true" type="tns1:ArrayOfString"> </element>
  <element name="Role" nillable="true" type="xsd:string"> </element>
  <element name="NotBefore" nillable="true" type="xsd:dateTime"> </element>
  <element name="NotAfter" nillable="true" type="xsd:dateTime"> </element>
  <element name="AdditionalName" nillable="true" type="xsd:string"> </element>
  <element name="AdditionalEMail" nillable="true" type="xsd:string"> </element>
  <element name="AdditionalUnit" nillable="true" type="xsd:string"> </element>
</sequence>
</complexType>
</schema>
<wsdl:types>
  <wsdl:message name="getCAStatusRequest"> </wsdl:message>
  <wsdl:message name="getCAStatusResponse">
    <wsdl:part name="getCAStatusReturn" type="tns1:DFNCERTTypesCAStatus"/>
  </wsdl:message>
  <wsdl:message name="getCAInfoRequest"> </wsdl:message>
  <wsdl:message name="getCAInfoResponse">
    <wsdl:part name="getCAInfoReturn" type="tns1:DFNCERTTypesCAInfo"/>
  </wsdl:message>
</wsdl:types>
```



The screenshot shows the 'Test Eins CA' web application interface. It features a navigation bar with tabs for 'Zertifikatanträge', 'Sperranträge', 'Zertifikate', 'Informationen', 'Hilfe', and 'Beenden'. Below the navigation bar, there are sub-tabs for 'Zu bearbeiten', 'Genehmigt', 'Archiviert', 'Gelöscht', and 'Suchen'. The main content area displays a table of certificate requests. Below the table, there are fields for 'Antragsnr.', 'Antragsteller', 'Eingangsdatum', and 'Rolle'. The interface is labeled 'DFN Deutsches Forschungsnetz' and 'Impressum'.

Antragsnr.	Antragsteller	Eingangsdatum	Rolle
N 15123457	emailAddress=brauckmann@dfn-cert.de, CN=Juergen Brauckmann, O=Testinstallation Eins CA, C=DE	25.03.2011 um 15:11	Smartcard Sign

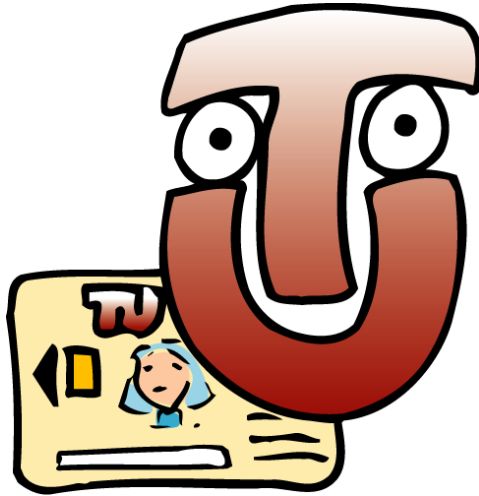
WebServices (SOAP):

- Einfaches API
- Noch einfachere Bibliothek verfügbar
 - Schritte zum Zertifikat: `newRequest()`, `approveRequest()`, `getCertificate()`
- Wenig Aufwand zur Integration für Entwickler
- Dadurch Technik der Zertifizierung „Detail“ bei der Smartcard-Produktion

Beispiele

Beispiele (1)

Aktuell 9 Einrichtungen mit Smartcards für alle Studierende,
Auswahl:



TU Berlin



Ruhr-Universität Bochum



JLU Gießen



FH Gelsenkirchen



TU Dortmund

Unterschiedliche Arten der Ausgabe:

- Mehrere Arbeitsplätze zur Immatrikulation und gleichzeitigen Chipkartenproduktion
- Arbeitsplätze zur Chipkartenproduktion nach Immatrikulation
- Immatrikulation, Ausgabe von Chipkarten, Zertifikaterstellung durch Zertifikatnehmer selbst

Verwendung:

- Selbstbedienungsterminals
- Nutzung der Smartcard von zu Hause mit eigenem CardReader

Fazit

Checkliste für Smartcard-Ausgabe mit DFN-PKI:

- Kapazitätenplanung Smartcard-Ausgabe
- Verschlüsselung? Konzept, evtl. Keybackup!
- PIN-Briefe, Vorbereitung, Druck, Ausgabe
- Persönliche Identifizierung!
- Archivierung von Anträgen (auch digital möglich)
- Wirksames Sperrmanagement!
- Funktionsübertragung, daher evtl. Ergänzung der Studienordnung o.ä. nötig

- DFN-PKI ist ein Angebot für alle DFN-Anwender
- Vielfältige Nutzungsszenarien
- Integration der Zertifizierung in Studiausweis-Ausgabe einfach möglich
- Rollout von Zertifikaten für Studierende wird zur „Routine“

pki@dfn.de
<https://www.pki.dfn.de>