

# **Erklärung zum Zertifizierungsbetrieb der FHWF-CA in der DFN-PKI**

- Sicherheitsniveau: Global -

**Fachhochschule Braunschweig/Wolfenbüttel**

**CPS der FHWF-CA**

**V1.2**

**8. Oktober 2007**



## 1 Einleitung

Die FHWF-CA ist eine Zertifizierungsstelle des DFN-Anwenders Fachhochschule Braunschweig/Wolfenbüttel innerhalb der DFN-PKI. In der DFN-PKI wird eine Zertifizierungshierarchie verwendet, bei der das Zertifikat der FHWF-CA von der DFN-PCA ausgestellt wird.

Für den Betrieb der FHWF-CA gelten die folgenden Dokumente:

- CP der DFN-PKI: "Zertifizierungsrichtlinie der DFN-PKI – Sicherheitsniveaus: Global, Classic und Basic -", Version 2.1, Dezember 2006, OID 1.3.6.1.4.1.22177.300.1.1.5.2.1
- CPS der DFN-PCA: "Erklärung zum Zertifizierungsbetrieb der obersten Zertifizierungsstelle der DFN-PKI – Sicherheitsniveaus: Global, Classic und Basic -", Version 2.1, Dezember 2006, OID 1.3.6.1.4.1.22177.300.2.1.5.2.1

Die vom CPS der DFN-PCA abweichenden Regelungen für die FHWF-CA sind in Kapitel 3 dieses Dokuments beschrieben.

Die FHWF-CA stellt ausschließlich Zertifikate im Sicherheitsniveau "Global" aus.

## 2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der FHWF-CA in der DFN-PKI"
- Version: 1.2
- Object Identifier (OID): 1.3.6.1.4.1.17379.100.1.1.2
- Zusammensetzung der OID:

Internet Assigned Numbers Authority (IANA)	1.3.6.1.4.1
Fachhochschule Braunschweig/Wolfenbüttel	17379
FHWF-CA	100
Erklärung zum Zertifizierungsbetrieb	1
Hauptversion	1
Nebenversion	2

## 3 Abweichungen vom CPS der DFN-PCA

Nachfolgend sind die Abschnitte des CPS der DFN-PCA aufgeführt, in denen für die FHWF-CA abweichende Regelungen getroffen werden.

### Zu CPS der DFN-PCA: "1.3.1 Zertifizierungsstellen"

Die Anschrift der FHWF-CA lautet:

Fachhochschule Braunschweig/Wolfenbüttel	Telefon: +49 5331 939-1900
Rechenzentrum	Telefax: +49 5331 939-1902
FHWF-CA	
Salzdahlumer Str. 46-48	E-Mail: pki@fh-wolfenbuettel.de
D - 38302 Wolfenbüttel	WWW: pki.fh-wolfenbuettel.de

### **Zu CPS der DFN-PCA: "1.3.2 Registrierungsstellen"**

Die ausgezeichneten Registrierungsstellen für die zuvor genannten Zertifizierungsstellen befinden sich in den Räumen der FHWF-CA.

Darüber hinaus sind keine weiteren Registrierungsstellen verfügbar.

### **Zu CPS der DFN-PCA: "1.5.1 Organisation"**

Die Verwaltung dieses CPS erfolgt durch die in Abschnitt 1.3.1 genannte Einrichtung.

Der Betrieb der FHWF-CA erfolgt durch:

DFN-Verein	Telefon: +49 30 884299-24
	Telefax: +49 30 884299-70
Stresemannstr. 78	E-Mail: pki@dfn.de
D - 10963 Berlin	WWW: www.pki.dfn.de

### **Zu CPS der DFN-PCA: "1.5.2 Kontaktperson"**

Die verantwortliche Person für das CPS der FHWF-CA ist:

Fachhochschule Braunschweig/Wolfenbüttel	Thorsten Ludewig
Rechenzentrum	Telefon: +49 5331 939 1940
FHWF-CA	
Salzdahlumer Str. 46-48	Telefax: +49 5331 939 1902
D - 38302 Wolfenbüttel	E-Mail: t.ludewig@fh-wolfenbuettel.de

### **Zu CPS der DFN-PCA: "2.2 Veröffentlichung von Informationen"**

Alle gemäß CP, Abschnitt 2.2, erforderlichen Informationen werden bereitgestellt unter:

<http://www.pki.dfn.de/teilnehmer>

### **Zu CPS der DFN-PCA: "3.1.1 Namensform"**

Die DNSs aller Zertifikatnehmer unterhalb der FHWF-CA enthalten die Attribute "C=DE" und "O=Fachhochschule Braunschweig/Wolfenbuettel".

Das optionale Attribut "OU=<Organisationseinheit>" kann mehrfach angegeben werden.

Wenn eine E-Mail Adresse angegeben wird, so kann diese über das Attribut "emailAddress" in den Namen aufgenommen werden. Die E-Mail Adresse sollte allerdings bevorzugt in der Zertifikaterweiterung "subjectAlternativeName" aufgenommen werden.

Damit entspricht der Name jedes Zertifikatnehmers dem folgenden Schema:

```
C=DE
[ ST=Niedersachsen
L=Braunschweig | Salzgitter | Wolfenbuettel | Wolfsburg ]
O=Fachhochschule Braunschweig/Wolfenbuettel
[ OU=<Organisationseinheit> ]
CN=<eindeutiger Name>
[ emailAddress=<E-Mail-Adresse> ]
```

Das Attribut "CN=" ist für alle Endteilnehmer obligatorisch und kommt genau einmal vor. Es enthält den vollständigen Namen des Benutzers.

Es wird empfohlen, über das Attribut "emailAddress=" eine gültige Emailadresse in den Namen aufzunehmen.

Für Endteilnehmer der FHWF-CA lautet der Name:

C=DE  
O=Fachhochschule Braunschweig/Wolfenbuettel  
OU=<Institut/Einrichtung>  
CN=<eindeutiger Name>  
emailAddress=<E-Mail-Adresse>

*Beispiel:*

C=DE  
O=Fachhochschule Braunschweig/Wolfenbuettel  
OU=Musterinstitut  
CN=Erich Mustermann  
emailAddress=mustermann@fh-wolfenbuettel.de

### **Zusätzliche Regeln für die Wahl eines Namens für Server:**

Zertifikate für WWW-Server müssen im Attribut "CN=" einen eindeutigen voll qualifizierten Hostnamen einer offiziell registrierten Domain enthalten.

Dieses Attribut darf keine Platzhalter ("Wildcards") und keine numerischen IP-Adressen enthalten.

Das optionale Attribut "emailAddress=" sollte eine gültige, vorzugsweise funktionsbezogene E-Mail-Adresse, beispielsweise die des Server-Administrators, enthalten.

Für Server im Bereich der FHWF-CA lautet der Name:

C=DE  
[ ST=Niedersachsen  
L=Braunschweig | Salzgitter | Wolfenbuettel | Wolfsburg ]  
O=Fachhochschule Braunschweig/Wolfenbuettel  
OU=<Institut/Einrichtung>  
CN=<voll qualifizierter Rechnername (Domainname)>  
emailAddress=<E-Mail-Adresse des Server-Admin>

*Beispiel (ohne optionale Attribute):*

C=DE  
O=Fachhochschule Braunschweig/Wolfenbuettel  
OU=Rechenzentrum  
CN=studip.fh-wolfenbuettel.de  
emailAddress=webmaster@fh-wolfenbuettel.de

#### **Zu CPS der DFN-PCA: "4.1.1 Wer kann ein Zertifikat beantragen"**

Die FHWF-CA bietet ihre Dienstleistungen allen Angehörigen und Mitarbeitern des DFN-Anwenders Fachhochschule Braunschweig/Wolfenbüttel an. Die FHWF-CA behält sich grundsätzlich das Recht vor, Zertifizierungsanträge *nicht* entgegen zu nehmen.

#### **Zu CPS der DFN-PCA: "5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen" und "6 Technische Sicherheitsmaßnahmen"**

Die FHWF-CA wird durch den DFN-Verein im Auftrag des DFN-Anwenders Fachhochschule Braunschweig/Wolfenbüttel bei der DFN-PCA betrieben. Daher sind für die FHWF-CA dieselben infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen umgesetzt, wie für die DFN-PCA (siehe CPS der DFN-PCA).

#### **Zu CPS der DFN-PCA: "6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren"**

Die durch die FHWF-CA ausgestellten Serverzertifikate haben standardmäßig eine Laufzeit von fünf Jahren, die Nutzerzertifikate von drei Jahren.