

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

- Sicherheitsniveau: Global -

## 1 Einleitung

Die BTU-CA ist eine Zertifizierungsstelle des DFN-Anwenders Brandenburgische Technische Universität Cottbus innerhalb der DFN-PKI. In der DFN-PKI wird eine Zertifizierungshierarchie verwendet, bei der das Zertifikat der BTU-CA von der DFN-PCA ausgestellt wird.

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

- CP der DFN-PKI: "Zertifizierungsrichtlinie der DFN-PKI – Sicherheitsniveaus: Global, Classic und Basic -", Version 2.2, April 2009, OID 1.3.6.1.4.1.22177.300.1.1.5.2.2
- 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 BTU-CA sind in Kapitel 3 dieses Dokuments beschrieben.

Die BTU-CA stellt Zertifikate im Sicherheitsniveau "Global" aus.

## 2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der BTU-CA in der DFN-PKI"
- Version: 2.5

## 3 Abweichungen vom CPS der DFN-PCA

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

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

Die Anschrift der BTU-CA lautet:

Brandenburgische Technische Universität Cottbus	Telefon: +49 355 692875
Universitätsrechenzentrum	Telefax: +49 355 692421
BTU-CA	
Konrad-Wachsmann-Allee 1	E-Mail: ca-btu@tu-cottbus.de
03046 Cottbus	WWW: www.rz.tu-cottbus.de
GERMANY	

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

Die ausgezeichneten Registrierungsstellen für die zuvor genannten Zertifizierungsstellen befinden sich in den Räumen der BTU-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 BTU-CA erfolgt durch:

DFN-Verein	Telefon: +49 30 884299-955
Alexanderplatz 1	Telefax: +49 30 884299-70
10178 Berlin	E-Mail: pki@dfn.de
GERMANY	WWW: www.pki.dfn.de

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

Die verantwortlichen Personen für das CPS der BTU-CA sind:

Brandenburgische Technische Universität Cottbus	Thomas Pawell
	Elgin Lorenz
Universitätsrechenzentrum	Telefon: +49 355 692874
BTU-CA	+49 355 693573
Konrad-Wachsmann-Allee 1	Telefax: +49 355 692421
03046 Cottbus	E-Mail: pawell@tu-cottbus.de
GERMANY	lorenz@tu-cottbus.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>

Für unter Dienstanweisung der BTU Cottbus stehende Zertifikatnehmer der BTU-CA werden alle erforderlichen Informationen, unabhängig von ihrer Entscheidung ihr Zertifikat über den Verzeichnisdienst der DFN-PKI zu veröffentlichen oder nicht, auf dem zentralen LDAP-Server der BTU Cottbus veröffentlicht.

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

Die DNSs aller Zertifikatnehmer unterhalb der BTU-CA enthalten die Attribute "C=DE" und "O=Brandenburgische Technische Universitaet Cottbus".

Das Attribut "OU=<Organisationseinheit>" muss einmal angegeben werden.

Eine gültige E-Mail Adresse der BTU Cottbus muss über das Attribut "emailAddress" in den Namen aufgenommen werden. Die E-Mail Adresse kann außerdem in der Zertifikat-erweiterung "subjectAlternativeName" aufgenommen werden. Die E-Mail Adresse muss auf "tu-cottbus.de" enden.

Damit entspricht der Name jedes Zertifikatnehmers dem folgenden Schema:

C=DE  
ST=Brandenburg  
L=Cottbus  
O=Brandenburgische Technische Universitaet Cottbus  
OU=<Organisationseinheit>  
CN=<Eindeutiger Name>  
emailAddress=<E-Mail Adresse> (in der Form \*tu-cottbus.de)

### **Zu CPS der DFN-PCA: "3.3 Identifizierung und Authentifizierung bei einer Zertifikaterneuerung"**

Die BTU-CA bietet keine Zertifikaterneuerung an.

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

Die BTU-CA bietet ihre Dienstleistungen allen Angehörigen und Mitarbeitern des DFN-Anwenders Brandenburgische Technische Universität Cottbus an. Gegen Gebühr können Zertifikate für externe Zertifikatnehmer, die in vertraglichen oder anderen dienstlichen Verbindungen zur BTU Cottbus oder anderen Einrichtungen der BTU Cottbus stehen, ausgestellt werden. Die Namensvergabe für Externe erfolgt entsprechend Punkt 3.1.2 CP.

Ebenso können gegen Gebühr Zertifikate für externe Serversysteme, die nicht in den Namens- oder Adressraum der BTU Cottbus fallen, deren Betreiber nachweislich in vertraglichen oder anderen dienstlichen Verbindungen zur BTU Cottbus stehen, ausgestellt werden.

#### **Zu CPS der DFN-PCA: "4.6 Zertifikaterneuerung ohne Schlüsselwechsel"**

Dieser Dienst wird von der BTU-CA grundsätzlich nicht angeboten.

#### **Zu CPS der DFN-PCA: "4.7 Zertifikaterneuerung mit Schlüsselwechsel"**

Dieser Dienst wird von der BTU-CA grundsätzlich nicht angeboten. Es ist grundsätzlich wie bei einem Neuantrag vorzugehen.

#### **Zu CPS der DFN-PCA: "4.8 Zertifikatmodifizierung"**

Dieser Dienst wird von der BTU-CA nicht angeboten.

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

Die BTU-CA wird durch den DFN-Verein im Auftrag des DFN-Anwenders Brandenburgische Technische Universität Cottbus bei der DFN-PCA betrieben. Daher sind für die BTU-CA dieselben infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen umgesetzt, wie für die DFN-PCA (siehe CPS der DFN-PCA).

#### **Zu CPS der DFN-PCA: "6.1.1 Schlüsselerzeugung" und "6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatnehmer"**

Die BTU-CA bietet eine optionale Schlüsselerzeugung bei der Registrierungsstelle an. Dabei wird technisch gewährleistet, dass die Registrierungsstelle nicht in Besitz oder Kenntnis des privaten Schlüssels gelangen kann. Es wird keine Sicherheitskopie des privaten Schlüssels erstellt.

Die Speicherung des privaten Schlüssels und des Zertifikats erfolgen direkt auf einem nur für den Zertifikatnehmer bestimmten mobilen Datenträger. Der private Schlüssel wird mit einer Zufalls-Passphrase geschützt, die dem Zertifikatnehmer in Form eines PIN-Briefs zusammen mit dem Datenträger ausgehändigt wird.

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

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

#### **Zu CPS der DFN-PCA: "9.1 Gebühren"**

Für Zertifikatnehmer, die nicht Angehörige der Brandenburgischen Technischen Universität Cottbus sind, fallen für ein Zertifikat Gebühren lt. Gebührenordnung der BTU Cottbus an.

Für Zertifikate für externe Serversysteme fallen ebenfalls Gebühren lt. Gebührenordnung der BTU Cottbus an.