

# **Erklärung zum Zertifizierungsbetrieb der Uni-Lübeck CA in der DFN-PKI**

- Sicherheitsniveau: Global -



## 1 Einleitung

Die Uni-Lübeck CA ist eine Zertifizierungsstelle des DFN-Anwenders Universität zu Lübeck innerhalb der DFN-PKI. In der DFN-PKI wird eine Zertifizierungshierarchie verwendet, bei der das Zertifikat der Uni-Lübeck CA von der DFN-PCA ausgestellt wird.

Für den Betrieb der Uni-Lübeck 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 Uni-Lübeck CA sind in Kapitel 3 dieses Dokuments beschrieben.

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

## 2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der Uni-Lübeck CA in der DFN-PKI"
- Version: 2.1

## 3 Abweichungen vom CPS der DFN-PCA

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

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

Die Anschrift der Uni-Lübeck CA lautet:

Universität zu Lübeck	Telefon: +49 451 500-5640
IT-Service-Center	
Uni-Lübeck CA	Telefax: +49 451 500-5613
Ratzeburger Allee 160	E-Mail: pki@uni-luebeck.de
23562 Lübeck	WWW: www.pki.uni-luebeck.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 Uni-Lübeck 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 Uni-Lübeck 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 verantwortliche Person für das CPS der Uni-Lübeck CA ist:

Universität zu Lübeck	Dipl.-Inf. Helge Illig
IT-Service-Center	
Uni-Lübeck CA	Telefon: +49 451 500-5640
Ratzeburger Allee 160	Telefax: +49 451 500-5613
23562 Lübeck	E-Mail: illig@itsc.uni-luebeck.de
GERMANY	

### **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 DNs aller Zertifikatnehmer unterhalb der Uni-Lübeck CA enthalten die Attribute "C=DE" und "O=Universitaet zu Luebeck".

Wenn das optionale Attribut "ST=Schleswig-Holstein" aufgenommen wird, dann muss auch das Attribut "L=Luebeck" aufgenommen werden.

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=Schleswig-Holstein
L=Luebeck ]
O=Universitaet zu Luebeck
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

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

Die Uni-Lübeck CA bietet ihre Dienstleistungen allen Angehörigen und Mitarbeitern des DFN-Anwenders Universität zu Lübeck an.

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

Die Uni-Lübeck CA wird durch den DFN-Verein im Auftrag des DFN-Anwenders Universität zu Lübeck bei der DFN-PCA betrieben. Daher sind für die Uni-Lübeck 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 Uni-Lübeck CA ausgestellten Serverzertifikate haben standardmäßig eine Laufzeit von fünf Jahren, die Nutzerzertifikate von drei Jahren.