DFN-PKI

Erklärung zum Zertifizierungsbetrieb der UH-CA in der DFN-PKI

- Sicherheitsniveau: Global -

Leibniz Universität Hannover

CPS der UH-CA

V2.1

13.03.2007

1 Einleitung

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

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

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

2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der UH-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 UH-CA abweichende Regelungen getroffen werden.

Zu CPS der DFN-PCA: "1.3.1 Zertifizierungsstellen"

Die Anschrift der UH-CA lautet:

Leibniz Universität Hannover	Telefon: +49 511/762-799042
Zertifizierungsstelle der Leibniz Universität Hannover	Telefax: +49 511/762-3003
RRZN (Regionales Rechenzentrum für Niedersachsen)	
Schloßwender Str. 5	E-Mail: uh-ca@ca.uni-hannover.de
D – 30159 Hannover	WWW: http://www.rrzn.uni-hannover.de/zertifizierung.html

Zu CPS der DFN-PCA: "1.3.2 Registrierungsstellen"

Die ausgezeichneten Registrierungsstellen für die zuvor genannten Zertifizierungsstellen befinden sich in den Räumen der UH-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 UH-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 UH-CA ist:

Leibniz Universität Hannover	Birgit Gersbeck-Schierholz
Zertifizierungsstelle der Leibniz Universität Hannover	Telefon: +49 511/762- 19789
RRZN (Regionales Rechenzentrum für Niedersachsen)	
Schloßwender Str. 5	Telefax: +49 511/762-3003
D – 30159 Hannover	E-Mail: gersbeck@rrzn.uni-hannover.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 DNs aller Zertifikatnehmer unterhalb der UH-CA enthalten die Attribute "C=DE" und "O=Leibniz Universitaet Hannover".

Das Attribut "ST=Niedersachsen" kann optional aufgenommen werden; in diesem Fall muss zusätzlich ein Attribut "L=Hannover" eingetragen 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=Niedersachsen,
L=Hannover,]
O=Leibniz Universitaet Hannover,
[OU=<Organisationseinheit>,]
[CN=<Eindeutiger Name>,]
[emailAddress=<E-Mail Adresse>]
```

Für Endteilnehmer der UH-CA lautet der Name:

```
C=DE,
O=Leibniz Universitaet Hannover,
OU=<Institut/Einrichtung der Leibniz Universitaet Hannover>,
CN=<eindeutiger Name>,
emailAddress=<E-Mail-Adresse>
```

Beispiel:

```
C=DE,
O=Leibniz Universitaet Hannover,
OU=Musterinstitut,
CN=Erich Mustermann,
emailAddress=mustermann@mi.uni-hannover.de
```

Zusätzliche Regeln für die Wahl eines Namens für Server:

Zertifikate für WWW-Server müssen im Attribut "cn= " einen eindeutigen Hostnamen enthalten.

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

Es sollte eine gültige, vorzugsweise funktionsbezogene Emailadresse, beispielsweise die des Server-Administrators, aufgenommen werden.

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

```
C=DE,
[ST=Niedersachsen,
L=Hannover,]
O=Leibniz Universitaet Hannover,
OU=<Institut/Einrichtung>,
CN=<voller Rechnername>,
emailAddress=<E-Mail-Adresse des Server-Admin>
```

Beispiel (ohne optionale Attribute):

```
C=DE,
O=Leibniz Universitaet Hannover,
OU=Musterinstitut,
CN=www.mi.uni-hannover.de,
emailAddress=webmaster@mi.uni-hannover.de
```

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

Die UH-CA ist zuständig für die Leibniz Universität Hannover und alle ihr zugeordneten Einrichtungen. Berechtigt zur Antragstellung auf Zertifizierung sind alle Mitglieder und Angehörigen der Leibniz Universität Hannover. Bezüglich der Berechtigung von Mitgliedern und Angehörigen von zugeordneten Einrichtungen können besondere Regelungen zur Anwendung gelangen.

Über diesen Kreis der Berechtigten hinaus kann die UH-CA in Einzelfällen Zertifikate gemäß Kapitel 1.3.3 ausstellen. Hinsichtlich der Namensgebung werden solche Zertifikatnehmer, wie im Dokument „Erklärung zum Zertifizierungsbetrieb der DFN-PCA“, Kapitel 3.1.2, beschrieben, als externe Zertifikatnehmer behandelt.

Die UH-CA behält sich grundsätzlich vor, Zertifizierungsanträge nicht entgegenzunehmen.

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

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