

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

- Sicherheitsniveau: Global -



## 1 Einleitung

Die RHRK-CA ist eine Zertifizierungsstelle des DFN-Anwenders Regionales Hochschulrechenzentrum TU Kaiserslautern innerhalb der DFN-PKI. In der DFN-PKI wird eine Zertifizierungshierarchie verwendet, bei der das Zertifikat der RHRK-CA von der DFN-PCA ausgestellt wird.

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

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

## 2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der RHRK-CA in der DFN-PKI"
- Version: 2.2

## 3 Abweichungen vom CPS der DFN-PCA

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

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

Die Anschrift der RHRK-CA lautet:

Regionales Hochschulrechenzentrum TU Kaiserslautern	Telefon: +49 631 205-2265 Telefax: +49 631 205-3056
RHRK-CA	
Paul-Ehrlich-Straße, Gebäude 34 D – 67663 Kaiserslautern	E-Mail: pki@rhrk.uni-kl.de <a href="http://www.rhrk.uni-kl.de/pki">http://www.rhrk.uni-kl.de/pki</a>

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

Die ausgezeichnete Registrierungsstelle für die zuvor genannte Zertifizierungsstelle befindet sich in den Räumen der RHRK-CA. Die Liste weiterer Registrierungsstellen wird unter der im Abschnitt zur Veröffentlichung von Informationen genannten Adresse bekannt gegeben.

Die Identitätsprüfung von Zertifikatnehmern kann von Mitarbeitern der Registrierungsstellen auch außerhalb der Räume der RHRK-CA vorgenommen werden.

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

Die Verwaltung dieses CPS erfolgt durch die oben unter "1.3.1 Zertifizierungsstellen" genannte Einrichtung.

Der Betrieb der RHRK-CA erfolgt durch:

DFN-Verein	Telefon: +49 30 884299-24 Telefax: +49 30 884299-70
Stresemannstr. 78 D - 10963 Berlin	E-Mail: pki@dfn.de WWW: <a href="http://www.pki.dfn.de">http://www.pki.dfn.de</a>

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

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

Regionales Hochschulrechenzentrum TU Kaiserslautern	Joachim Stemler
RHRK-CA	Telefon: +49 631 205-4434
Paul-Ehrlich-Straße, Gebäude 34	Telefax: +49 631 205-3056
D – 67663 Kaiserslautern	E-Mail: jstemler@rhrk.uni-kl.de

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

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

<http://www.rhrk.uni-kl.de/pki>

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

Die DNs aller Zertifikatnehmer der **Technischen Universität Kaiserslautern** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Technische Universitaet Kaiserslautern".

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 der Technischen Universität Kaiserslautern dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Kaiserslautern ]
O=Technische Universitaet Kaiserslautern
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Zertifikate für den Betrieb der Zertifizierungsstelle RHRK-CA selbst beginnen mit dem DN-Präfix "C=DE" und "O=Regionales Hochschulrechenzentrum Kaiserslautern"

und entsprechen damit dem folgenden Schema:

```
C=DE
O=Regionales Hochschulrechenzentrum Kaiserslautern
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNs aller Zertifikatnehmer der **Deutschen Hochschule für Verwaltungswissenschaften Speyer** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Deutsche Hochschule fuer Verwaltungswissenschaften Speyer".

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 der Deutschen Hochschule für Verwaltungswissenschaften Speyer dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Speyer ]
O=Deutsche Hochschule fuer Verwaltungswissenschaften Speyer
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNs aller Zertifikatnehmer der **Fachhochschule Bingen** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Fachhochschule Bingen".

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 der Fachhochschule Bingen dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Bingen ]
O=Fachhochschule Bingen
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNs aller Zertifikatnehmer der **Fachhochschule Kaiserslautern** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Fachhochschule Kaiserslautern".

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 der Fachhochschule Kaiserslautern dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Kaiserslautern oder L=Pirmasens oder L=Zweibruecken ]
O=Fachhochschule Kaiserslautern
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNs aller Zertifikatnehmer der **Fachhochschule Koblenz** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Fachhochschule Koblenz".

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 der Fachhochschule Koblenz dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Koblenz oder L=Remagen oder L=Hoehr-Grenzhausen ]
O=Fachhochschule Koblenz
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNS aller Zertifikatnehmer der **Fachhochschule Ludwigshafen** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Fachhochschule Ludwigshafen".

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 der Fachhochschule Ludwigshafen dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Ludwigshafen ]
O=Fachhochschule Ludwigshafen
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNS aller Zertifikatnehmer der **Fachhochschule Mainz** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Fachhochschule Mainz".

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 der Fachhochschule Mainz dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Mainz ]
O=Fachhochschule Mainz
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNS aller Zertifikatnehmer der **Fachhochschule Trier** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Fachhochschule Trier".

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 der Fachhochschule Trier dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Trier oder L=Birkenfeld oder L=Idar-Oberstein ]
O=Fachhochschule Trier
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNSs aller Zertifikatnehmer der **Fachhochschule Worms** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Fachhochschule Worms".

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 der Fachhochschule Worms dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Worms ]
O=Fachhochschule Worms
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNSs aller Zertifikatnehmer der **Universität Koblenz-Landau** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Universitaet Koblenz-Landau".

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 der Universität Koblenz-Landau dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Koblenz oder L=Landau oder L=Mainz ]
O=Universitaet Koblenz-Landau
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

Die DNS aller Zertifikatnehmer der **Universität Trier** unterhalb der RHRK-CA enthalten die Attribute "C=DE" und "O=Universitaet Trier".

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 der Universität Trier dem folgenden Schema:

```
C=DE
[ ST=Rheinland-Pfalz
L=Trier ]
O=Universitaet Trier
[ OU=<Organisationseinheit> ]
CN=<Eindeutiger Name>
[ emailAddress=<E-Mail Adresse> ]
```

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

Die RHRK-CA bietet ihre Dienstleistungen allen Angehörigen und Mitarbeitern der folgenden Einrichtungen an:

- TU Kaiserslautern (DFN-Anwender)
- Regionales Hochschulrechenzentrum Kaiserslautern (DFN-Anwender)
- Deutsche Hochschule für Verwaltungswissenschaften Speyer
- Fachhochschule Bingen
- Fachhochschule Kaiserslautern
- Fachhochschule Koblenz
- Fachhochschule Ludwigshafen
- Fachhochschule Mainz
- Fachhochschule Trier
- Fachhochschule Worms
- Universität Koblenz-Landau
- Universität Trier

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

Die RHRK-CA wird durch den DFN-Verein im Auftrag des DFN-Anwenders Regionales Hochschulrechenzentrum TU Kaiserslautern bei der DFN-PCA betrieben. Daher sind für die RHRK-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 RHRK-CA ausgestellten Serverzertifikate haben standardmäßig eine Laufzeit von fünf Jahren, die Nutzerzertifikate von drei Jahren.