Erklärung zum Zertifizierungsbetrieb der

RHRK-CA

in der DFN-PKI

Regionales Hochschulrechenzentrum TU Kaiserslautern

CPS V1.1, 16. März 2006

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 Wurzelzertifizierungsstelle der DFN-PKI, der DFN-PCA, ausgestellt wird.

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

- CP der DFN-PKI: "Zertifizierungsrichtlinie der Public Key Infrastruktur im Deutschen Forschungsnetz – Classic -", Version 1.1, Februar 2005, OID 1.3.6.1.4.1.22177.300.1.1.1.1.1
- CPS der DFN-PCA: "Erklärung zum Zertifizierungsbetrieb der obersten Zertifizierungsstelle der Public Key Infrastruktur im Deutschen Forschungsnetz – Classic -", Version 1.1, Februar 2005, OID 1.3.6.1.4.1.22177.300.2.1.1.1.1

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

2 Identifikation des Dokuments

- Titel: "Erklärung zum Zertifizierungsbetrieb der RHRK-CA in der DFN-PKI"
- Version: 1.1

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.

Abschnitt 1.3.1 Zertifizierungsstellen

Die Anschrift der RHRK-CA lautet:

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

Abschnitt 1.3.2 Registrierungsstellen

Die ausgezeichnete Registrierungsstelle für die zuvor genannte Zertifizierungsstelle befindet sich in den Räumen der RHRK-CA. Die Liste der Registrierungsstellen wird unter der im Abschnitt 2.2 zur Veröffentlichung von Informationen genannten Adresse bekannt gegeben.

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

Abschnitt 1.5.1 Organisation

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

Der Betrieb der RHRK-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: http://www.dfn.de/pki

Abschnitt 1.5.2 Kontaktperson

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

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

Abschnitt 2.1 Verzeichnisdienst

Der Verzeichnisdienst der RHRK-CA ist online zu erreichen unter:

- http(s)://www.pca.dfn.de/rhrk-ca
- ldap://ldap.pca.dfn.de/c=DE, o=DFN-Verein, ou=DFN-PKI, o=Regionales Hochschulrechenzentrum Kaiserslautern

Abschnitt 2.2 Veröffentlichung von Informationen

Die RHRK-CA publiziert unter der Adresse http://www.rhrk.uni-kl.de/pki die folgenden Informationen:

- Zertifikat und Fingerabdruck
- Erklärung zum Zertifizierungsbetrieb
- Liste der Registrierungsstellen

Abschnitt 3.1.1 Namensform

Die DNs der Zertifikatnehmer der TU 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 wird diese über das Attribut "EMAIL=" in den Namen aufgenommen.

Damit entspricht der Name jedes Zertifikatnehmers dem folgenden Schema:

C=DE,

O=Technische Universitaet Kaiserslautern,

[OU=<Organisationseinheit>,]

CN=<Eindeutiger Name>,

[EMAIL=<E-Mail Adresse>]

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

Abschnitt 3.1.3 Pseudonymität / Anonymität

Die RHRK-CA bietet keine Möglichkeit an, auf Verlangen einer natürlichen Person anstelle des Namens im Zertifikat ein Pseudonym aufzuführen.

Abschnitt 4.1.1 Wer kann ein Zertifikat beantragen

Die RHRK-CA bietet ihre Dienstleistungen allen Angehörigen und Mitarbeitern des DFN-Anwenders TU Kaiserslautern an. Entsprechend den DFN-PCA Zerrtifizierungs-Richtlinien besteht kein Rechtsanspruch auf die Erteilung eines Zertifikates durch die RHRK-CA.

Abschnitt 4.4.2 Veröffentlichung des Zertifikats

Die RHRK-CA veröffentlicht die gemäß den Zertifizierungsrichtlinien der DFN-PKI geforderten Zertifikate über die oben angegebenen Informationssysteme.

Zertifikate für natürliche und juristische Personen werden in der Regel durch die RHRK-CA veröffentlicht.

Abschnitt 4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und –wiederherstellung

Hier gilt dieselbe Regelung wird unter Abschnitt 6.2.3

Abschnitt 5.8 Einstellung des Betriebs

Falls es zur Einstellung des Zertifizierungsbetriebs kommen sollte, werden folgende Maßnahmen ergriffen:

- Information der DFN-PCA mindestens drei Monate vor Einstellung der Tätigkeit.
- Information aller Zertifikatnehmer, Registrierungsstellen und betroffenen Organisationen mindestens drei Monate vor Einstellung der Tätigkeit.
- Rechtzeitiger Widerruf aller Zertifikate.
- Sichere Zerstörung der privaten Schlüssel der Zertifizierungsstelle nach Widerruf aller Zertifikate.

Der DFN-Anwender Regionales Hochschulrechenzentrum TU Kaiserslautern stellt den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen Widerrufsliste für den zugesicherten Aufbewahrungszeitraum sicher.

Abschnitt 6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatnehmer

Die RHRK-CA bietet keine Möglichkeit zur Schlüsselerzeugung durch die Zertifizierungsstelle.

Abschnitt 6.2.3 Hinterlegung privater Schlüssel

Die RHRK-CA bietet keine Möglichkeit zur Schlüsselhinterlegung an.