Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb der

UH-CA in der DFN-PKI

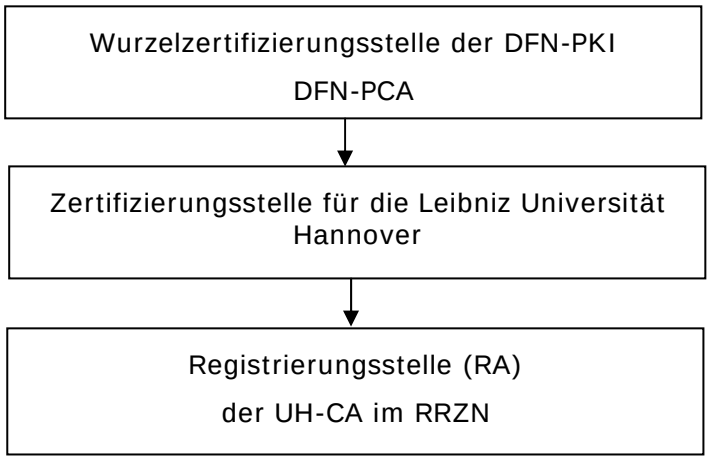
Leibniz Universität Hannover

CP & CPS V1.3, 24. Oktober 2006

1 Einleitung

Die UH-CA ist eine an der Leibniz Universität Hannover angesiedelte, vom DFN betriebene Zertifizierungsstelle innerhalb der DFN-PKI. Das Regionale Rechenzentrum für Niedersachsen (RRZN) übernimmt die Aufgaben einer ausgezeichneten Registrierungsstelle (RA) (CP 1.3.2.1) für die UH-CA.

Zur Diensteerbringung wird eine Zertifizierungshierarchie verwendet, bei der das Zertifikat der UH-CA von der Wurzelzertifizierungsstelle der DFN-PKI, der DFN-PCA, ausgestellt wird.



2 Identifikation des Dokuments

- Titel: „Zertifizierungsrichtlinien und Erklärung zum Zertifizierungsbetrieb der UH-CA in der DFN-PKI“
- Version: 1.3
- Object Identifier (OID): 1.3.6.1.4.1.18141.20.1.1.3
- Zusammensetzung der OID:

IANA	1.3.6.1.4.1
Regionales Rechenzentrum für Niedersachsen (RRZN)	18141
UH-CA	20
Zertifizierungsrichtlinien	1
Hauptversion	1
Nebenversion	3

3 Zertifizierungsrichtlinien und Erklärung zum Zertifizierungsbetrieb

Für den Betrieb der Zertifizierungsstelle UH-CA gilt das folgenden Dokument verbindlich:

"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

Zusätzliche Spezifikationen zu dem oben genannten Dokument sind in Kapitel 4 beschrieben.

Das folgende Dokument ist nicht als verbindlich anzusehen, setzt aber den grundlegenden Rahmen für den Betrieb der Zertifizierungsstelle:

"Erklärung zum Zertifizierungsbetrieb 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

Zusätzliche Spezifikationen zu dem oben genannten Dokument sind in Kapitel 5 beschrieben.

4 Zusätzliche Spezifikationen zu den Zertifizierungsrichtlinien der DFN-PCA

Die Zertifizierungsrichtlinien der DFN-PCA werden durch die UH-CA in einigen Bereichen ergänzt bzw. dort, wo für die untergeordneten Zertifizierungsstellen Freiräume existieren, konkretisiert. Dies resultiert in abweichenden und ergänzenden Texten, die hier mit Verweis auf das Kapitel der Zertifizierungsrichtlinien aufgeführt sind.

Kapitel 3.1.3 Pseudonymität / Anonymität

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

Kapitel 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.

Kapitel 4.1.2 Registrierungsprozess

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

Kapitel 4.2.2 Annahme oder Abweisung von Zertifikatanträgen

Die UH-CA behält sich gemäß Kapitel 4.1.1 grundsätzlich vor, Zertifizierungsanträge nicht entgegenzunehmen.

Kapitel 4.4.2 Veröffentlichung des Zertifikats

Die UH-CA veröffentlicht die gemäß der Zertifizierungsrichtlinien der DFN-PKI geforderten Zertifikate über die unten angegebenen Informationssysteme.

Zertifikate für natürliche Personen werden immer durch die UH-CA veröffentlicht.

Kapitel 4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung.

Die UH-CA bietet keine Möglichkeit zur Schlüsselhinterlegung für Schlüssel.

Kapitel 9.1 Gebühren

Die UH-CA behält sich vor, für bestimmte Leistungen Entgelte zu erheben. Eine Preisliste wird auf den Webseiten der UH-CA veröffentlich.

5 Zusätzliche Spezifikationen zu der „Erklärung zum Zertifizierungsbetrieb der DFN-PCA“

Die Erklärung zum Zertifizierungsbetrieb der DFN-PCA ist für die untergeordneten Zertifizierungsstellen nicht verbindlich, dient aber als „Best Practice“. Außerdem kann eine untergeordnete Zertifizierungsstelle sich entscheiden, die Erklärung sinngemäß zu übernehmen. In diesem Fall – der für die durch den DFN-Verein im Auftrag eines DFN-Anwenders betriebenen Zertifizierungsstellen der Normalfall ist – sind nur geringfügige Abweichungen bzw. Ergänzungen notwendig.

Kapitel 1.3.1 Zertifizierungsstellen

Die Anschrift der Zertifizierungsstelle ist:

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

Kapitel 1.3.2 Registrierungsstellen

Die ausgezeichnete Registrierungsstelle für die zuvor genannte Zertifizierungsstelle befindet sich in den Räumen des Regionalen Rechenzentrums für Niedersachsen (RRZN) an der Leibniz Universität Hannover.

Darüber hinaus sind keine weiteren Registrierungsstellen verfügbar.

Kapitel 1.5.1 Organisation

Die Verwaltung der Richtlinien erfolgt durch:

RRZN/Leibniz Universität Hannover	Telefon: +49 511/762-2883
Schloßwender Str. 5	Telefax: +49 511/762-3003
D – 30159 Hannover	

Der Betrieb der unter Abschnitt 1.3. aufgeführten Zertifizierungsstellen erfolgt durch:

DFN-Verein	Telefon: +49 30 884299-23/24
Stresemannstr. 78	Telefax: +49 30 884299-70
	E-Mail: pki@dfn.de
D - 10963 Berlin	WWW: http://www.dfn.de/pki

Kapitel 1.5.2 Kontaktperson

Die verantwortliche Person für die Zertifizierungsrichtlinien und die Erklärung zum Zertifizierungsbetrieb ist:

RRZN/Leibniz Universität Hannover	Telefon: +49 511/762-19789
Birgit Gersbeck-Schierholz	Telefax: +49 511/762-3003
Schloßwender Str. 5	E-Mail: gersbeck@rrzn.uni-hannover.de
D – 30159 Hannover	

Kapitel 2.1 Verzeichnisdienst

- Die Bezugsadresse für den Verzeichnisdienst der UH-CA wird auf den Webseiten der UH-CA veröffentlicht (s. Kapitel 1.3.1).

Kapitel 2.2 Veröffentlichung von Informationen

Die UH-CA publiziert die folgenden Informationen über den Web-Server

http://www.pca.dfn.de/

- Zertifikat und Fingerabdruck:
  http://www.pca.dfn.de/uh-ca/policy.html
  sowie
  https://www.pca.dfn.de/uh-ca/policy.html
- Zertifizierungsrichtlinien:
  http://www.pca.dfn.de/uh-ca/policy.html
  und
  https://www.pca.dfn.de/uh-ca/policy.html
- Erklärung zum Zertifizierungsbetrieb:
  http://www.pca.dfn.de/uh-ca/policy.html
  und
  https://www.pca.dfn.de/uh-ca/policy.html
- Liste der Registrierungsstellen:
  http://www.rrzn.uni-hannover.de/ra_uhca.html

Kapitel 3.1.1 Namensform

Die DNs aller Zertifikatnehmer unterhalb der Zertifizierungsstelle enthalten die Attribute "`C=DE`" und "`O=Leibniz Universitaet Hannover`".

Optional können die Attribute "`st=Niedersachsen`" und "`l=Hannover`" in den Namen aufgenommen werden (diese Einträge können nur gemeinsam verwendet werden).

Daraus ergibt sich, dass Zertifikate mit folgende Prefixen von der UH-CA ausgestellt werden können:

C=DE, O=Leibniz Universitaet Hannover
oder

C=DE, ST=Niedersachsen, L=Hannover, O=Leibniz Universitaet Hannover

Der Name jedes Zertifikatnehmers entspricht grundsätzlich dem folgenden Schema:

C=DE,

O=Leibniz Universitaet Hannover,

[OU=<Organisationseinheit>,]

CN=<Eindeutiger Name>,

[EMAIL=<Email-Adresse>]

Das optionale Attribut "OU=<Organisationseinheit>" kann mehrfach angegeben werden.

Das Attribut "CN=" ist zwar bei juristischen Personen nicht zwingend erforderlich, wird jedoch aus Interoperabilitätsgründen verwendet.

Das Attribut "CN=" ist daher für alle Endteilnehmer obligatorisch und kommt genau einmal vor. Es enthält den vollständigen Namen des Benutzers.

Es wird empfohlen, über das Attribut "email=" eine gültige Emailadresse in den Namen aufzunehmen.

Für Endteilnehmer der UH-CA lautet der Name:

c=DE,
o=Leibniz Universitaet Hannover,
ou=<Institut/Einrichtung der Leibniz Universitaet Hannover>,
cn=<eindeutiger Name>,
email=<E-Mail-Adresse>

Beispiel:

c=DE,
o=Leibniz Universitaet Hannover,
ou=Musterinstitut,
cn=Erich Mustermann,
email=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.

Das optionale Attribut "email=" sollte eine gültige, vorzugsweise funktionsbezogene Emailadresse, beispielsweise die des Server-Administrators, enthalten.

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>,

email=<E-Mail-Adresse des Server-Admin>

Beispiel (ohne optionale Attribute):

c=DE,

o=Leibniz Universitaet Hannover,

ou=Musterinstitut,

cn=www.mi.uni-hannover.de,

email=webmaster@mi.uni-hannover.de

Kapitel 4.4.2 Veröffentlichung des Zertifikats

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

Zertifikate für natürliche Personen werden immer durch die UH-CA veröffentlicht.

Kapitel 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.

Die Leibniz Universität Hannover stellt den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen Widerrufsliste für den zugesicherten Aufbewahrungszeitraum sicher.

Kapitel 6.1.2 Übermittlung des privaten Schlüssels an den Zertifikatnehmer

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

Kapitel 6.2.3 Hinterlegung privater Schlüssel

Die UH-CA bietet keine Möglichkeit zur Schlüsselhinterlegung für Schlüssel.