Erklärung zum Zertifizierungsbetrieb der

Classic-UNITUE-CA der Zertifizierungsstelle UNITUE-CA in der DFN-PKI

Eberhard-Karls-Universität Tübingen

CPS V1.1, 6.07.2006

1 Einleitung

Die UNITUE-CA ist eine von der Eberhard-Karls-Universität Tübingen betriebene Zertifizierungsstelle innerhalb der DFN-PKI. Die UNITUE-CA selbst zertifiziert nicht, sie betreibt bzw. repräsentiert eine oder mehrere CA. Die Zertifizierungsstelle UNITUE-CA betreibt u. a. die RA der Classic-UNITUE-CA. Der Betrieb der Classic-UNITUE-CA erfolgt durch den DFN-Verein (Abschn. 1.5.1).

Sonderregelung: Das bisher, direkt an die UNITUE-CA vergebene Zertifikat im Rahmen der WWW-Policy der DFN-PCA behält bis zum Ablauf Ende 2007 Gültigkeit für alle damit ausgestellten Teilnehmerzertifikate. Mit Inbetriebnahme der Classic-UNITUE-CA werden keine Teilnehmerzertifikate von der UNITUE-CA ausgestellt.

Die Classic-UNITUE-CA ist eine Zertifizierungsstelle des DFN-Anwenders Eberhard-Karls-Universität Tübingen innerhalb der DFN-PKI. In der DFN-PKI wird eine Zertifizierungshierarchie verwendet, bei der das Zertifikat der Classic-UNITUE-CA von der Wurzelzertifizierungsstelle der DFN-PKI, der DFN-PCA, ausgestellt wird.

Für den Betrieb der Classic-UNITUE-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 Classic-UNITUE-CA sind in Abschnitt 3 dieses Dokuments beschrieben.

2 Identifikation des Dokuments

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

Abschnitt 1.3.1 Zertifizierungsstellen

Die Anschrift der UNITUE-CA lautet:

Eberhard-Karls-Universität Tübingen	Telefon: +49 7071 29-70201
Zentrum für Datenverarbeitung	Telefax: +49 7071 29-5912
UNITUE-CA	
Wächterstr. 76	E-Mail: unitue-ca@uni-tuebingen.de
D – 72074 Tübingen	WWW: http://www.ca.uni-tuebingen.de

Abschnitt 1.3.2 Registrierungsstellen

Die ausgezeichneten Registrierungsstellen für die zuvor genannten Zertifizierungsstellen befinden sich in den Räumen der UNITUE-CA.

Darüber hinaus sind keine weiteren Registrierungsstellen verfügbar.

Abschnitt 1.5.1 Organisation

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

Der Betrieb der Classic-UNITUE-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 Classic-UNITUE-CA ist:

Eberhard-Karls-Universität Tübingen	Jörg Heitzenröther
Zentrum für Datenverarbeitung	Telefon: +49 7071 29-70305
UNITUE-CA	
Wächterstr. 76	Telefax: +49 7071 29-5912
D – 72074 Tübingen	E-Mail: heitzenroether@zdv.uni-tuebingen.de

Abschnitt 2.1 Verzeichnisdienst

Der Verzeichnisdienst der Classic-UNITUE-CA ist online zu erreichen unter:

- http(s)://www.pca.dfn.de/classic-unitue-ca
- ldap://ldap.pca.dfn.de/c=DE, o=DFN-Verein, ou=DFN-PKI, o=Universitaet Tuebingen

Abschnitt 2.2 Veröffentlichung von Informationen

Die Classic-UNITUE-CA publiziert unter der Adresse http(s)://www.pca.dfn.de/classic-unitue-ca die folgenden Informationen:

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

Abschnitt 3.1.1 Namensform

Die DNs aller Zertifikatnehmer unterhalb der Classic-UNITUE-CA enthalten die Attribute "`C=DE`" und "`O=Universitaet Tuebingen`".

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=Universitaet Tuebingen,

[OU=<Organisationseinheit>,]

CN=<Eindeutiger Name>,

[EMAIL=<E-Mail Adresse>]

Abschnitt 3.1.3 Pseudonymität / Anonymität

Die Classic-UNITUE-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 Classic-UNITUE-CA bietet ihre Dienstleistungen allen Angehörigen und Mitarbeitern des DFN-Anwenders Eberhard-Karls-Universität Tübingen an.

Abschnitt 4.4.2 Veröffentlichung des Zertifikats

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

Zertifikate für natürliche und juristische Personen werden immer durch die Classic-UNITUE-CA veröffentlicht.

Abschnitt 4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und –wiederherstellung

Hier gilt dieselbe Regelung wie 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 Eberhard-Karls-Universität Tübingen 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 Classic-UNITUE-CA bietet keine Möglichkeit zur Schlüsselerzeugung durch die Zertifizierungsstelle.

Abschnitt 6.2.3 Hinterlegung privater Schlüssel

Die Classic-UNITUE-CA bietet keine Möglichkeit zur Schlüsselhinterlegung an.