

**Erklärung zum Zertifizierungsbetrieb
der
HE CA
in der DFN-PKI**

**Hochschule Esslingen
CPS V1.1, 01.09.2006**

1 Einleitung

Die HE CA ist eine Zertifizierungsstelle des DFN-Anwenders Hochschule Esslingen innerhalb der DFN-PKI. In der DFN-PKI wird eine Zertifizierungshierarchie verwendet, bei der das Zertifikat der HE CA von der Wurzelzertifizierungsstelle der DFN-PKI, der DFN-PCA, ausgestellt wird.

Für den Betrieb der HE 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 HE CA sind in Abschnitt 3 dieses Dokuments beschrieben.

2 Identifikation des Dokuments

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

Abschnitt 1.3.1 Zertifizierungsstellen

Die Anschrift der HE CA lautet:

Hochschule Esslingen	Telefon: +49 711-397-4111
Rechenzentrum HE Raum F01.203	HZETelefax: +49 711-397-4115 CA
Flandernstr. 101	E-Mail: pki@hs-esslingen.de
D – 73732 Esslingen	WWW: http://www.hs-esslingen.de/pki

Abschnitt 1.3.2 Registrierungsstellen

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

Hochschule Esslingen	Prof. Herbert Wiese
Rechenzentrum HZE HE CA	Telefon: +49 711-397-4110
Flandernstr. 101	Telefax: +49 711-397-4214
D - 73732 Esslingen	E-Mail: Herbert.Wiese@hs-esslingen.de

Abschnitt 2.1 Verzeichnisdienst

Der Verzeichnisdienst der HE CA ist online zu erreichen unter:

- [http\(s\)://www.pca.dfn.de/hs-esslingen-ca](http(s)://www.pca.dfn.de/hs-esslingen-ca)
- `ldap://ldap.pca.dfn.de/c=DE, o=DFN-Verein, ou=DFN-PKI, o=Hochschule Esslingen`

Abschnitt 2.2 Veröffentlichung von Informationen

Die HE CA publiziert unter der Adresse [http\(s\)://www.pca.dfn.de/hs-esslingen-ca](http(s)://www.pca.dfn.de/hs-esslingen-ca) die folgenden Informationen:

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

Abschnitt 3.1.1 Namensform

Die DNSs aller Zertifikatnehmer unterhalb der HE CA enthalten die Attribute "C=DE" und "O=Hochschule Esslingen".

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=Hochschule Esslingen,  
[ OU=<Organisationseinheit>, ]  
CN=<Eindeutiger Name>,  
[ EMAIL=<E-Mail Adresse> ]
```

Abschnitt 3.1.3 Pseudonymität / Anonymität

Die HE 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 HE CA bietet ihre Dienstleistungen allen Angehörigen des DFN-Anwenders Hochschule Esslingen an.

Abschnitt 4.4.2 Veröffentlichung des Zertifikats

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

Zertifikate für natürliche und juristische Personen werden nur nach Freigabe durch die Person selbst durch die HE CA veröffentlicht.

Abschnitt 4.12.1 Richtlinien und Praktiken zur Schlüssel hinterlegung 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 Hochschule Esslingen 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 HE CA bietet keine Möglichkeit zur Schlüsselerzeugung durch die Zertifizierungsstelle.

Abschnitt 6.2.3 Hinterlegung privater Schlüssel

Die HE CA bietet keine Möglichkeit zur Schlüssel hinterlegung an.