Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb der

HU-CA in der DFN-PKI

Humboldt-Universität zu Berlin

CP & CPS V2.0, 23.03.2005

1. Einleitung

Die HU-CA ist eine von Humboldt-Universität zu Berlin betriebene Zertifizierungsstelle innerhalb der DFN-PKI.

Zur Diensterbringung wird eine Zertifizierungshierarchie verwendet, bei der die Zertifikate der HU-CA von der Wurzelzertifizierungsstelle der DFN-PKI, der DFN-PCA, ausgestellt werden.

Die Instanzen der HU-CA (HU-CA *X*) haben eine Laufzeit von jeweils 4 Jahren, es werden Zertifikate für Endnutzer (Teinehmer) und für Datenverarbeitungssysteme ausgestellt.

Eine gültige HU-CA stellt, bis zur Hälfte ihrer Laufzeit, Zertifikate für Endnutzer mit einer Gültigkeitsdauer von zwei Jahren aus und veröffentlicht dann nur noch Zertifikat Widerruflisten (CRL). Diese Verfahrensweise gewährleistet, dass Zertifikate, die ausgegeben werden, mindestens so lange gültig sind, wie die ausstellende CA.

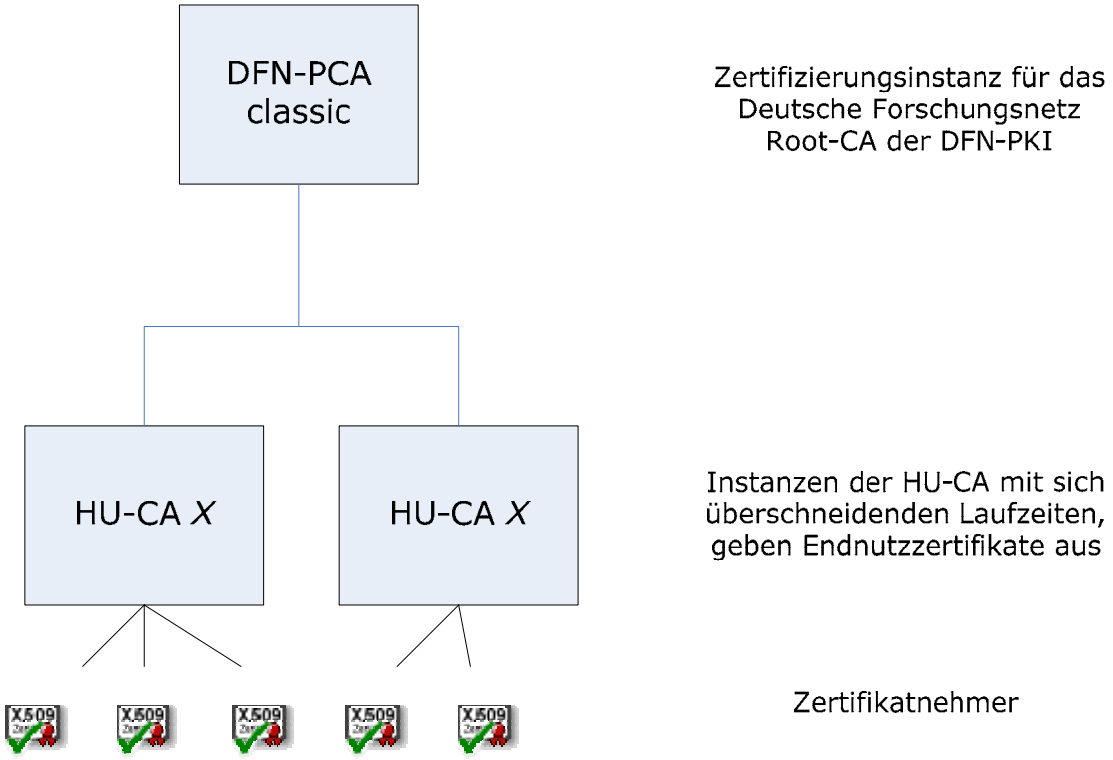

Abbildung 1 Zertifizierungshierarchie der HU-CA

2. Identifikation des Dokuments

- Titel: „Zertifizierungsrichtlinien und Erklärung zum Zertifizierungsbetrieb der HU-CA in der DFN-PKI“
- Version: 2.0
- Object Identifier (OID): 1.3.6.1.4.1.13687.300.1.1.2

Zusammensetzung der OID:		
	IANA	1.3.6.1.4.1
	Humboldt-Universitaet zu Berlin	13687
	PKI	300
	HU-CA	1
	HU-CA Richtlinie	1
	Version 2.0	2

3. Zertifizierungsrichtlinien und Erklärung zum Zertifizierungsbetrieb

Für den Betrieb der Zertifizierungsstelle HU-CA gilt das folgende Dokument uneingeschränkt:

"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

http://www.pca.dfn.de/dfn-pki/certification/cp/classic/x509/dfn-pki-cp-classic-1.3.6.1.4.1.22177.300.1.1.1.1.1.html

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

http://www.pca.dfn.de/dfn-pki/certification/cps/classic/x509/dfn-pki-cps-classic-1.3.6.1.4.1.22177.300.2.1.1.1.1.html

Die Abweichungen zu den oben genannten Dokumenten sind in den folgenden Abschnitten beschrieben.

4. Abweichungen zu den Zertifizierungsrichtlinien der DFN-PCA

Die Zertifizierungsrichtlinien der DFN-PCA werden durch die HU-CA in einigen Bereichen erweitert 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 1.3.1.2 Zertifizierungsstellen (CA)

Zertifikate mit dem Verwendungszweck „Object-Signing“ werden nicht ausgestellt.

Kapitel 1.5 Verwaltung dieses Dokumentes

Humboldt-Universität zu Berlin
Computer- und Medienservice
- Trustcenter -

Unter den Linden 6
10099 Berlin

Telefon: +49-(0)30-2093 7043
Telefax: +49-(0)30-2093 2959
E-Mail: ca@hu-berlin.de
WWW: http://ca.hu-berlin.de/

Kapitel 2.2 Veröffentlichung von Informationen

Der öffentliche Schlüssel der HU-CA wird im "CMS-Journal" und auf den offiziellen Webseiten der HU-CA veröffentlicht.

Die HU-CA stellt zum Zwecke der Bekanntmachung der Schlüssel, alle Zertifikate auf ihrem WWW-Server und in einem Directory-Server zur Verfügung.

WWW: https://ra.hu-berlin.de
LDAP: ldap://ra.hu-berlin.de:389/o=Humboldt-Universitaet zu Berlin,c=DE

Kapitel 3.1.1 Namensform

Die Namensgebung der HU-CA und der Teilnehmer folgt einem einheitlichen Standard und spiegelt die unmittelbare Zugehörigkeit zu einer Organisationseinheit oder assoziierten Stelle der Humboldt-Universität zu Berlin wider.

Der DN der HU-CA wird wie folgt festgelegt:

cn=HU-CA*[X]***, ou=HU-CA, o=Humboldt-Universitaet zu Berlin, c=DE**

Jeder DN muss innerhalb der HU-CA eineindeutig sein.

Der DN eines Teilnehmers innerhalb einer HU-CA muss folgender Konvention folgen:

cn=*[Vorname Nachname]***, ou=***[Subdomain oder Organisationseinheit]***, o=Humboldt-Universitaet zu Berlin, c=DE**

Der DN (Subject Distinguished Names) eines Gruppen- oder Organisationszertifikates innerhalb einer HU-CA muss folgenden Konventionen entsprechen:

cn=GRP:*[Name]***, ou=***[Subdomain oder Organisationseinheit]***, o=Humboldt-Universitaet zu Berlin, c=DE**

*Name = z.B. GRP:Poststelle, GRP:Fakultaetsbuero

Gruppen- und Organisationszertifikate müssen durch ihre Namensgebung als solche erkennbar sein.

[kursiv] = Variabel

Das optionale Attribut „ou=<Organisationseinheit>“ muss einmal angegeben werden.

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

Kapitel 3.1.3 Pseudonymität / Anonymität

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

Kapitel 3.2.2 Authentifizierung einer Organisation, Regelungen für Organisationszertifikate

Teilnehmer für ein Organisationszertifikat sind ein Schlüsselverantwortlicher und eine definierte Gruppe weiterer Schlüsselnutzer.

In folgenden Fällen können Organisationszertifikate ausgegeben werden:

- Das Zertifikat ist an eine bestimmte Funktion, nicht aber an eine einzelne Person gebunden.
- Mehrere Personen nehmen eine gemeinsame Rolle wahr (z.B. in Form einer Poststelle).
- Zertifikate werden in automatisierten Prozessen verwendet, in denen z.B. signierte und oder verschlüsselte E-Mail gesendet/empfangen werden sollen, aber mehrere Personen die Berechtigung für diese Prozesse haben.

Über die gerechtfertigte Ausstellung von Organisationszertifikaten über die hier dargestellten Möglichkeiten hinaus entscheidet der Direktor/die Direktorin der Zentraleinrichtung Computer- und Medienservice der Humboldt-Universität zu Berlin.

Sollen Organisationszertifikate ausgestellt werden, so ist hierfür von der beantragenden Stelle ein gesonderter Antrag (Antrag Organisationszertifikat [Antrag_OrgZert]) zu stellen. Insbesondere sind ein Schlüsselverantwortlicher und alle weiteren Schlüsselnutzer zu benennen. Anträge auf Organisationszertifikate können nur von den Leitern dieser Stellen gestellt werden.

Der Schlüsselverantwortliche hat zuvor selbst ein eigenes Zertifikat zu beantragen und ist für die Umsetzung folgender Maßnahmen verantwortlich:

- Alle Schlüsselnutzer werden durch den Schlüsselverantwortlichen identifiziert; für die entsprechenden Daten und die Unterschriften ist ein gesonderter Antrag (Antrag_OrgZert) zu verwenden.
- Der Schlüsselverantwortliche regelt die Zugriffsrechte auf das Schlüsselpaar und die dazugehörige PIN sowie deren sichere Verteilung.
- Der Schlüsselverantwortliche regelt die Anwendungsbereiche und die Verfahren für den Einsatz des Schlüsselpaares.
- Die Befugnis und die Details für mögliche Gründe zur Sperrung des Zertifikates werden durch den Schlüsselverantwortlichen bestimmt.

Gruppen- und Organisationszertifikate müssen durch ihre Namensgebung als solche erkennbar sein.

Die ausstellende HU-CA hat in das Zertifikat einen entsprechenden Kommentar aufzunehmen ("Organization Certificate of Humboldt-Universitaet zu Berlin").

Kapitel 3.4 Identifizierung und Authentifizierung bei einem Widerruf

Zusätzlich steht dem Zertifikatnehmer ein Onlineinterface für den Widerruf seines Zertifikates, mit Hilfe seiner CRIN (Certificate Revocation Number) zur Verfügung.

Organisationszertifikate können von dem Schlüsselverantwortlichen auch elektronisch signiert widerrufen werden.

Kapitel 4.1.1 Wer kann ein Zertifikat beantragen

Berechtigt zur Antragstellung sind alle Mitglieder und Angehörige der Humboldt-Universität zu Berlin und sonstige assoziierte Stellen. Über den Status einer assoziierten Stelle entscheidet der Direktor/die Direktorin der Zentraleinrichtung Computer- und Medienservice der Humboldt-Universität zu Berlin.

Der Antragsteller muss eine gültige Email-Adresse der Humboldt-Universität zu Berlin besitzen.

Kapitel 4.1.2 Registrierungsprozess

Die HU-CA bietet eine optionale Schlüsselerzeugung durch die Zertifizierungsstelle.

Die zuständige Registrierungs- oder Zertifizierungsstelle kann die Identifikation eines Zertifikatnehmers auch bei Übergabe des Zertifikates vornehmen.

Kapitel 4.4.1 Annahme des Zertifikates

Ein Zertifikat wird durch den Zertifikatnehmer akzeptiert, wenn

- das Zertifikat verwendet wird oder

- wenn dem Zertifikat nicht innerhalb von 4 Wochen nach Ausstellung widersprochen wird.

Fehlerhaft ausgestellte Zertifikate hat die ausstellende Zertifizierungsstelle unverzüglich zu widerrufen.

Kapitel 4.4.2 Veröffentlichung des Zertifikats

Die HU-CA veröffentlicht die gemäß der Zertifizierungsrichtlinien der DFN-PKI geforderten Zertifikate über die in (Abschnitt 2.2) angegebenen Informationssystemen.

Zertifikate werden immer durch die HU-CA veröffentlicht.

Kapitel 4.6 Zertifikaterneuerung / Re-Zertifizierung

Bei einer Re-Zertifizierung wird dem Zertifikatnehmer durch die zuständige Zertifizierungsstelle ein neues Zertifikat ausgestellt, wobei auch ein neues Schlüsselpaar verwendet werden kann. Entsteht hierbei ein neuer Zertifizierungspfad (z.B. durch eine neue HU-CA), muss das alte Zertifikat nicht zwangsläufig widerrufen werden.

Kapitel 4.9.7 Veröffentlichungsfrequenz für CRLs

Die CRL wird mindestens einmal pro Monat veröffentlicht.

Wird ein Zertifikat widerrufen, erfolgt unmittelbar danach die Ausstellung einer neuen CRL und deren Veröffentlichung.

Kapitel 4.9.8 Maximale Latenzzeit für CRLs

Die maximale Latenzzeit für CRLs beträgt 30 Tage.

Kapitel 4.9.9 Verfügbarkeit von Online-Widerrufs/Status-Überprüfungsverfahren

Alle ausgestellten Zertifikate können über ein Onlineinterface der ausstellenden HU-CA auf Gültigkeit hin überprüft werden.

Kapitel 4.12 Schlüsselhinterlegung und -wiederherstellung

Die HU-CA bietet keine Möglichkeit zur Schlüsselhinterlegung und Schlüsselwiederherstellung.

Wird der private Schlüssel durch die HU-CA erzeugt, wird dieser nach Übergabe an den Zertifikatnehmer auf Seiten der Zertifizierungsstelle unwiederbringlich gelöscht. Der Zertifikatnehmer ist für die Verwendung und sichere Aufbewahrung des privaten Schlüssels selbst verantwortlich.

5. Abweichungen 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:

Zertifizierungsinstanz der Humboldt-Universität zu Berlin	Telefon: +49 (0)30 2093 7043
Computer- und Medienservice	Telefax: +49 (0)30 2093 2959
Unter den Linden 6	E-Mail: pki@hu-berlin.de
D - 10099 Berlin	WWW: http://ca.hu-berlin.de/

Kapitel 1.3.2 Registrierungsstellen

Die ausgezeichneten Registrierungsstellen für die zuvor genannten Zertifizierungsstellen befinden sich:

- am Standort **Mitte** (Unter den Linden 6, Raum 1063e, Tel:2093 2482),
- am Standort **Adlershof** (Rudower Chaussee 26, Raum 2'303,Tel:2093 7043)

Darüber hinaus besteht die Möglichkeit Registrierungsaufgaben an andere MA der HU (z.B. Personalabteilung, Studierendenverwaltung) zu übertragen.

Kapitel 1.5.1 Organisation

Die Verwaltung der Richtlinien erfolgt durch:

Zertifizierungsinstanz der Humboldt-Universität zu Berlin	Telefon: +49 (0)30 2093 7043
Computer- und Medienservice	Telefax: +49 (0)30 2093 2959
Unter den Linden 6	E-Mail: pki@hu-berlin.de
D - 10099 Berlin	WWW: http://ca.hu-berlin.de/

Kapitel 1.5.2 Kontaktperson

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

Steffen Platzer	Telefon: +49 (0)30 2093 7043
Humboldt-Universität zu Berlin Computer- und Medienservice	Telefax: +49 (0)30 2093 2959
Rudower Chaussee 26, Raum 2'303	E-Mail: pki@hu-berlin.de
D - 12489 Berlin	WWW: http://ca.hu-berlin.de/

Kapitel 2.1 Verzeichnisdienst

Der Verzeichnisdienst der HU-CA ist unter der folgenden Bezugsadresse online zu erreichen:

- https://ca.hu-berlin.de/
- http://ca.hu-berlin.de/
- ldap://ra.hu-berlin.de:389/o=Humboldt-Universitaet zu Berlin,c=DE

Kapitel 2.2 Veröffentlichung von Informationen

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

http://www.ca.hu-berlin.de:

- Zertifikat und Fingerabdruck aller relevanten Zertifizierungsinstanzen
- Zertifizierungsrichtlinien
- Informationen zu den HU-Zertifizierungsinstanzen
- Schnittstellen zur Zertifikatbeantragung, -suche und für CRLs
- Liste und Örtlichkeiten der Registrierungsstellen
- Antragsformulare

Kapitel 4.4.2 Veröffentlichung des Zertifikats

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

Zertifikate für natürliche Personen werden nur nach Freigabe durch die Person selbst durch die HU-CA veröffentlicht. Diese Freigabe ist Bedingung für eine Zertifizierung durch die HU-CA.

Kapitel 4.6 Zertifikaterneuerung / Re-Zertifizierung

Soweit ein Antrag auf Zertifikaterneuerung mit einem gültigen und von der HU-CA zertifizierten Schlüssel signiert wurde, kann von einer erneuten Identifikation und eigenhändigen Unterschrift abgesehen werden, sofern der Antragsteller versichert, dass sich die Daten des Namen im Zertifikat nicht geändert haben.

Kapitel 5.1.1 Lage und Konstruktion

Die technischen Systeme der HU-CA sind in den Räumen des Computer- und Medienservice der Humboldt-Universität zu Berlin untergebracht.

Die Räume bieten hinsichtlich der infrastrukturellen Sicherheitsmaßnahmen einen ausreichenden Schutz, der dem erforderlichen Sicherheitsniveau angemessen ist.

Kapitel 5.1.2 Zutrittskontrolle

Die Betriebsräume der Zertifizierungsstellen sind durch geeignete technische und infrastrukturelle Maßnahmen gesichert. Ein Zutritt zu den Betriebsräumen der Zertifizierungsstelle wird nur Mitarbeitern gestattet, die vom HU-CA Administrator autorisiert worden sind. Der Zutritt durch betriebsfremde Personen, wird nach Anmeldung durch eine Besucherregelung unter Aufsicht durchgeführt.

Kapitel 5.2.1 Sicherheitsrelevante Rollen

Um einen ordnungsgemäßen und revisionssicheren Betrieb einer Zertifizierungsstelle zu gewährleisten, ist u.a. eine entsprechende Aufgabenverteilung und Funktionstrennung vorzunehmen.

Ein Mitarbeiter kann auch in mehr als einer Rolle auftreten. Ebenso ist es möglich, dass Funktionen einer Rolle auf mehrere Mitarbeiter mit dieser Rolle verteilt werden.

Rolle	Funktion	Kürzel
Registrierungsauthority	Schnittstelle für Zertifikat Abholung, Prüfung der notwendigen Unterlagen und Annahme von Zertifikat- und Sperranträgen, Identifizierung, Authentifizierung und Prüfung der Autorisierung der Zertifikatnehmer, Verifikation der Dokumente, Belehrung/Information der Zertifikatnehmer	RA
Registrator	Prüfung des Zertifikatantrags hinsichtlich Vollständigkeit und Korrektheit Archivierung von Dokumenten, falls erforderlich. Freigabe, Übermittlung von Zertifikatanträgen und Sperr/Widerrufsanträgen an die zuständige Zertifizierungsstelle. Die erforderlichen Daten werden aus den entsprechenden Universitätsdatenbanken übernommen und durch automatisierte Verfahren überprüft.	RG
Zertifizierungsinstanz	Ausstellen von Zertifikaten und Widerrufslisten, Erzeugung und Verwahrung der CA-Schlüssel.	CA
CA-Mitarbeiter 1	Verantwortlich für die Anwendung und Lagerung von elektronischen Datenträgern, auf denen die privaten Schlüssel der Zertifizierungsstelle gespeichert sind.	CAO1

CA-Mitarbeiter 2	Verantwortlich für die Anwendung des Vier-Augen-Prinzips, hat Kenntnis der PINs (Passwörter) zu den privaten Schlüsseln der Zertifizierungsstelle	CAO2
Systembetreuung	Administration der IT-Systeme und dem täglichem Betrieb (Backups usw.).	
Systemadministrator	Installation, Konfiguration, Administration und Wartung der IT- und Kommunikationssysteme. Vollständige Kontrolle über die eingesetzte Hard- und Software, jedoch keinen Zugriff auf und keine Kenntnis von kryptographischen Schlüsseln und deren Passwörtern für Zertifizierungsprozess, Zertifikat- und Sperrmanagement. Ausschließliche Kenntnis der Boot- und Administrator- Passwörter der Systeme.	SA
Systemoperator	Installation, Konfiguration, Administration und Wartung der Anwendungen zur Datensicherung und -Wiederherstellung, des Web-Server sowie Zertifikat- und Sperrmanagement.	SO
Überwachung des Betriebs	Keine Funktion im operativen Betrieb, zuständig für die Durchsetzung der in der CP, dem CPS und des Sicherheitskonzeptes festgelegten Grundsätze	
Revision	Durchführung der betriebsinternen und externen Audits, Überwachung und Einhaltung der Datenschutzbestimmungen	R
Sicherheitsbeauftragter	Definition und Einhaltung der Sicherheitsbestimmungen Überprüfung der Mitarbeiter Vergabe von Berechtigungen Ansprechpartner für sicherheitsrelevante Fragen	ISO

Kapitel 5.2.2 Involvierte Mitarbeiter pro Arbeitsschritt

In der folgenden Tabelle werden die sicherheitsrelevanten Tätigkeiten beschrieben und den entsprechenden Rollen zugeordnet. Aus der Tabelle ist ebenso zu entnehmen, für welche Tätigkeiten das Vier-Augen-Prinzip eingehalten werden sollte.

Tätigkeit	Rollen	Vier Augen-Prinzip	Erläuterung
Annahme von Zertifikatsanträgen	RA		Web Interface, persönlich
Identifizierung und Authentifizierung von Zertifikatnehmern	RA		durch geeignete Dokumente (PA, Reisepass)
Prüfung der Autorisierung von Zertifikatnehmern	RA		
Verifikation von Dokumenten	RA		
Belehrung/Information der Zertifikatnehmer	RA		Informationsmaterial

Prüfung des DN	RA		entsprechend 3.1.1
Annahme und Prüfung von Sperranträgen	RA/RG		Entweder nimmt die RA den Sperrauftrag entgegen und prüft Autorisierungsinformation oder initialisiert einen Rückruf
Prüfung der Anträge hinsichtlich Vollständigkeit und Korrektheit	RA/RG		Die Verwaltung und der Antragsteller
Archivierung von Dokumenten sofern erforderlich	RA/RG		Antragsformulare
Freigabe und Übermittlung von Zertifikat- und Sperranträgen an die zuständige Zertifizierungsstelle	RA/RG		
Erzeugung von Schlüsselpaaren für selbst betriebene CAs, RAs und Datenverarbeitungssysteme	CAO1, CAO2	**x**	
Starten von Prozessen zur Erzeugung von Schlüsselpaaren für Zertifikatsnehmer und PIN-Briefen	CAO1, CAO2	**x**	
Zertifizierung, Starten von Prozessen zum Ausstellen von Zertifikaten und Widerrufslisten	CAO1, CAO2	**x**	
Übertragen von Zertifikat-Requests zum Zertifizierungsrechner	CAO1		
Veröffentlichen von Zertifikaten und Widerrufslisten	CAO1		
Schlüsselhinterlegung von privaten CA Schlüsseln für selbst betriebene CAs	CAO1, CAO2	**x**	
Kenntnis von Boot- und Administrator Passwörtern	SA		
Starten und Stoppen von Prozessen (z.B. Web-Server, Datensicherung)	SO		
Datensicherung	SO, CAO1		CAO1 ermöglicht physikalischen Zugang
Austausch von Soft- und Hardware Komponenten für			
Zertifizierung	SA, CAO1	**x**	
andere Systeme	SA, CAO1		CAO1 ermöglicht physikalischen Zugang
Wiedereinspielung von Datensicherungen			
Zertifizierung	SA, CAO1	**x**	
andere Systeme	SA, CAO1		CAO1 ermöglicht physikalischen Zugang

Überprüfung von Protokolldateien	SA, R		Wird regelmäßig durch SA wahrgenommen, im Rahmen eines Audits durch R
Audit	R		
Vergabe von physikalischen Berechtigungen	ISO		
Technische Vergabe von Berechtigungen	SA, ISO	**x**	ISO überwacht
Fortschreibung des Betriebs- bzw. Sicherheits-konzepts	ISO		

Kapitel 5.2.4 Trennung von Aufgaben

Die Rollentrennung wird der personellen Situation entsprechend angepaßt. So können einige Rollen z.B. durch der HU-CA nicht permanent angehörende Personen wahrgenommen werden.

Zur Wahrung des vier Augen-Prinzips erfolgt eine personelle Trennung zwischen CAO1 und CAO2. Ebenso werden die Rollen ISO und R von unterschiedlichen Personen besetzt.

SA und SO können zwar bei einer Person zusammenfallen, aber weder RA/RG, CAOx, ISO noch R sein.

Kapitel 5.4.4 Datensicherungskonzept

Die in den Abschnitten 5.4.1 und 5.5.1 aufgeführten Daten werden auf Grundlage eines Datensicherungskonzepts regelmäßig mit einer Offline-Sicherung auf externe Medien (CD-ROM) unterzogen. Eckwerte des Datensicherungskonzepts:

- Nach jedem Signaturprozess der HU-CA erfolgt eine komplette Sicherung der CA.
- Es existieren von jeder Sicherung 3 Medien.
- Die Medien werden nach einem Rotationsprinzip in 2 örtlich getrennten Tresoren verwahrt.

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 deren Gültigkeit bis nach dem Einstellungsdatum liegt.
- Sichere Zerstörung der privaten Schlüssel der Zertifizierungsstelle nach Widerruf aller Zertifikate.

Die Humboldt-Universität zu Berlin stellt den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen Widerrufsliste für den zugesicherten Aufbewahrungszeitraum sicher.

Kapitel 6 Organisatorische und technische Sicherheitsmaßnahmen

Kapitel 6.1 für die HU-CA

Das asymmetrische Schlüsselpaar der HU-CA, das zur Erzeugung von Signaturen dient, muss eine Schlüssellänge von mindestens 2048 Bit RSA haben. Die Schlüssellänge richtet sich nach der technischen Verfügbarkeit und Notwendigkeit. Sie wird bei Verfügbarkeit geeigneter Methoden erhöht.

Das Erzeugen einer digitalen Signatur sowie andere Tätigkeiten, die die HU-CA betreffen, müssen auf einer dafür dedizierten Datenverarbeitungsanlage durchgeführt werden. Diese Anlage darf

über keinerlei Verbindung zu einem privaten oder öffentlichen Netzwerk verfügen. Sämtliche eventuell vorhandene Netzwerktreiber oder Netzwerk-Kernelmodule müssen von dieser Datenverarbeitungsanlage dauerhaft entfernt sein. Der private Schlüssel der HU-CA darf zu keinem Zeitpunkt auf einer anderen Datenverarbeitungsanlage temporär oder permanent gespeichert werden, die eine feste oder temporäre Verbindung zu einem privaten oder öffentlichen Netzwerk hat.

Die unberechtigte Nutzung dieser Datenverarbeitungsanlage muss durch einen erweiterten Schutz durch Passwörter oder PIN's verhindert werden. Dies bezieht einen Passwort- oder PIN-Schutz für einen Systemstart (BIOS-, Bootmanager- oder BootROM-Passwortschutz) zusätzlich zum System-Login mit ein.

Die Passphrase der geheimen (privaten) CA Schlüssel dürfen nur den unmittelbaren HU-CA-Administratoren bekannt sein. Diese müssen an einem für Unbefugte unzugänglichen Ort (Datensafe) in einzelnen Umschlägen o.ä. aufbewahrt werden.

Die benutzte Datenverarbeitungsanlage muss in einem Raum stehen, der keinen Publikumsverkehr hat und über eine organisatorische und technische Zutrittskontrolle verfügt.

Während der Nichtbenutzung der Datenverarbeitungsanlage wird diese in einem Datensafe aufbewahrt. Über die Verwendung und Lagerung der Schlüssel wird Protokoll geführt.

Die privaten Schlüssel der HU-CA müssen auf externen Datenträgern, wie Magnet- oder DAT-Bändern, Wechselplatten oder CD-ROM's gespeichert werden. Diese Datenträger dürfen nur für Signaturzwecke durch die HU-CA-Administratoren benutzt werden. Außerhalb dieser Zeiten müssen diese Datenträger an einem für Unbefugte unzugänglichen verschlossenen Ort (Datensafe) aufbewahrt werden.

Die privaten Schlüssel der HU-CA dienen ausschließlich der Signatur von Teilnehmer-Schlüsseln und Zertifikatswiderrufslisten (CRL) sowie dem Erstellen eventueller Crosszertifikate. Diese Schlüssel dürfen nicht als Kommunikationsschlüssel benutzt werden. E-Mail oder andere Daten dürfen mit diesem Schlüsseln nicht signiert oder ent- bzw. verschlüsselt werden.

Zu zertifizierende Schlüssel dürfen nicht automatisch ohne manuelle Prüfung signiert werden.

Die Integrität und die Unversehrtheit der Daten auf der verwendeten Datenverarbeitungsanlage ist durch die HU-CA-Administratoren unter Einsatz geeigneter kryptografischer Verfahren ständig zu kontrollieren.

Zertifikate für Teilnehmer haben eine Gültigkeitsdauer von höchstens 2 Jahren. Die begrenzte Gültigkeitsdauer von Signaturschlüssel-Zertifikaten ergibt sich dadurch, dass die kryptografischen Verfahren für digitale Signaturen nur für einen begrenzten Zeitraum sicher bewertet werden können.

Zertifikate werden ausschließlich dann ausgestellt, wenn der zu zertifizierende Public Key über eine sichere Mindestlänge (mind. 1024 Bit RSA) verfügt.

Die HU-CA hat jeden ihr zur Signatur vorgelegten Schlüssel daraufhin zu überprüfen, ob dieser nicht bereits einem anderen Teilnehmer innerhalb der HU-CA zugewiesen wurde. Dabei sind auch widerrufene Schlüssel zu betrachten. Doppelte Schlüssel sind zurückzuweisen. Wird ein doppelter, noch gültiger Schlüssel gefunden, ist der entsprechende Teilnehmer zu informieren.

Die HU-CA hat für die Rekonstruktion elektronischer Dokumentationen und Signaturen einmal erstellte öffentliche Schlüssel und Zertifikate zu archivieren und deren Überprüfung technisch sicherzustellen.

Kapitel 6.1.1 für Registrierungsinstanzen der HU-CA

Bei einer RA handelt es sich um einen durch eine HU-CA zertifizierten Teilnehmer, der im Auftrag der HU-CA die Identifizierung von Teilnehmern vor der Zertifizierung durch die HU-CA übernimmt.

Eine RA darf weder asymmetrische Schlüsselpaare für andere Teilnehmer erzeugen, noch kann sie selbst Zertifikate erteilen oder widerrufen.

Die RA leitet den Zertifizierungswunsch (schriftlicher Antrag, vorgelegten CSR) an die HU-CA weiter.

Die Übermittlung der überprüften Daten kann dabei durch persönliche Übergabe an die HU-CA oder durch gesicherte elektronische Übermittlung geschehen.
Um Fälschungen oder nachträgliche Änderungen zu verhindern, muss jede elektronische Übermittlung an die HU-CA durch die RA mit einem gültigen Signaturzertifikat signiert werden.

Elektronisch übermittelte Zertifizierungsanträge sind durch die HU-CA zu verifizieren.

Kapitel 6.1.2 für den Zertifikatnehmer

Der Zertifikatnehmer verpflichtet sich, den privaten Schlüssel vor Missbrauch und unberechtigter Nutzung durch Dritte zu schützen, insbesondere durch das Verwenden von nicht trivialen Passwörtern und PINs.

Er versichert:

- dass sämtliche Angaben und Erklärungen in Bezug auf die im Zertifikat enthaltenen Informationen der Wahrheit entsprechen;
- das Zertifikat ausschließlich in Übereinstimmung mit diesem CPS einzusetzen;
- und das Zertifikat unverzüglich zu widerrufen, wenn die enthaltenen Angaben nicht mehr stimmen oder der private Schlüssel kompromittiert wurde oder nicht mehr sicher ist;

Für die Speicherung seiner Schlüssel und deren sichere Aufbewahrung ist der Teilnehmer selbst verantwortlich. Eventuelle Sicherungskopien sind von ihm selbst zu erstellen.

Kapitel 6.1.3 Auslieferung des öffentlichen Schlüssels an den Zertifikatausssteller

Über ein Onlineinterface der ausstellenden HU-CA wird der CSR durch den Zertifikatnehmer oder die HU-CA selbst im PKCS#10 Format erzeugt. Es kann auch ein bereits erzeugter CSR im PKCS#10 Format über einen Upload der HU-CA übermittelt werden. Sollte dies nicht möglich sein, kann der öffentliche Schlüssel der zuständigen Registrierungs- bzw. Zertifizierungsstelle durch eine handlungsberechtigte Person auf einem Datenträger übergeben werden.

Kapitel 6.2 Übermittlung des privaten Schlüssels an den Zertifikatnehmer

Die HU-CA bietet eine optionale Schlüsselerzeugung durch die Zertifizierungsstelle. Dies erfolgt auf Antrag des Zertifikatnehmers.

Die Übermittlung an den Zertifikatnehmer kann erfolgen:

- als PKCS#12 Datei geschützt durch eine PIN, dabei wird der PIN-Brief gesondert und persönlich zugestellt oder übergeben
- auf einem Hardwaretoken (z.B. Smartcard), auf der der private Schlüssel durch eine PIN vor unberechtigtem Zugriff geschützt ist. Dabei kann der Hardwaretoken und die dazugehörige PIN persönlich übergeben werden, oder es erfolgt eine persönliche postalische Zustellung mit gesondertem PIN-Briefversand.

Der geheime Schlüssel wird auf Seiten der CA/RA unwiederbringlich gelöscht und der Schlüssel wird auf einem entsprechend gut gesicherten Computer/Token generiert.

Kapitel 6.2.3 Hinterlegung privater Schlüssel

Die HU-CA bietet keine Möglichkeit zur Schlüsselhinterlegung. Für Sicherungskopien und die sichere Aufbewahrung der übergebenen Schlüssel trägt der Zertifikatnehmer selbst Verantwortung.

Kapitel 6.2.4 Backup privater Schlüssel

Ein Backup von privaten Schlüsseln findet nicht statt.

Ein Backup von privaten Schlüsseln der HU-CA ist in 6.1 und 6.1.1 geregelt.

Kapitel 7.3 OCSP Profil

Ein OCSP Dienst wird von der HU-CA derzeit nicht angeboten.