



**DEUTSCHE INITIATIVE  
FÜR NETZWERKINFORMATION E.V.**

**DINI-Zertifikat  
Dokumenten- und Publikationsservice  
2007**

Arbeitsgruppe „Elektronisches Publizieren“





**DEUTSCHE INITIATIVE  
FÜR NETZWERKINFORMATION E.V.**

**DINI-Zertifikat  
Dokumenten- und Publikationsservice  
2007**

Arbeitsgruppe „Elektronisches Publizieren“

DINI Schriften 3-de

[Version 2.0, September 2006]

## **Impressum**

DINI – Deutsche Initiative für Netzwerkinformation e.V.

– Geschäftsstelle –

c/o Niedersächsische Staats- und Universitätsbibliothek Göttingen

Papendiek 14

37073 Göttingen

Tel.: 0551-39-38 66

Fax: 0551-39-38 56

E-Mail: [gs@dini.de](mailto:gs@dini.de)

[www.dini.de](http://www.dini.de)

# Inhaltsverzeichnis

<b>Über DINI</b>	<b>5</b>
<b>Zusammenfassung</b>	<b>6</b>
<b>1 Zielstellung</b>	<b>7</b>
<b>2 Kriterien</b>	<b>9</b>
2.1 Sichtbarkeit des Gesamtangebotes	9
2.2 Leitlinien (Policy)	10
2.3 Autorenbetreuung	11
2.4 Rechtliche Aspekte	12
2.5 Sicherheit, Authentizität und Integrität	14
2.5.1 Server	14
2.5.2 Dokumente	15
2.6 Erschließung	15
2.6.1 Sacherschließung	15
2.6.2 Metadatenexport	16
2.6.3 Schnittstellen	17
2.7 Zugriffsstatistik	17
2.8 Langzeitverfügbarkeit	18
<b>3 Vergabemodus und Evaluierung</b>	<b>18</b>
<b>4 Erläuterungen und Beispiele</b>	<b>20</b>
4.1 Sichtbarkeit des Service	20
4.2 Leitlinien (Policy)	20
4.2.1 Beispiel: Leitlinien für den Dokumenten- und Publikationsserver der Humboldt-Universität zu Berlin	20
4.2.2 Beispiel: Open Access Politik der Georg-August-Universität Göttingen	24
4.3 Autorenbetreuung	26
4.4 Rechtliche Aspekte	27

4.5	Sicherheit, Authentizität und Integrität	29
4.5.1	Server	29
4.5.2	Dokumente	31
4.6	Erschließung	34
4.6.1	Sacherschließung	34
4.6.2	Metadatenexport und Schnittstellen	34
4.7	Zugriffsstatistik	35
4.8	Langzeitverfügbarkeit	35
	<b>Aufnahmeantrag für die Mitgliedschaft in DINI e. V.</b>	<b>39</b>

## Über DINI

Die Entwicklung der modernen Informations- und Kommunikationstechnologie verursacht einen Wandel innerhalb der Informations-Infrastrukturen der Hochschulen und anderer Forschungseinrichtungen. Dieser Wandel ist ein zentrales Thema in der deutschen Hochschullandschaft und setzt mehr als bisher Absprachen, Kooperationen, Empfehlungen und Standards voraus. Die Deutsche Initiative für Netzwerkinformation (DINI) unterstützt diese Entwicklung.

DINI wurde gegründet, um die Verbesserung der Informations- und Kommunikationsdienstleistungen und die dafür notwendige Entwicklung der Informations-Infrastrukturen an den Hochschulen sowie regional und überregional zu fördern. Durch Absprachen und Arbeitsteilung zwischen den Infrastruktureinrichtungen soll das Informationstechnik- und Dienstleistungsangebot weiter verbessert werden. Hierfür ist auch die gemeinsame Entwicklung von Standards und Empfehlungen erforderlich.

DINI ist eine Initiative der drei Partnerorganisationen:

- AMH (Arbeitsgemeinschaft der Medienzentren an Hochschulen e.V.),
- dbv (Deutscher Bibliotheksverband Sektion 4: Wissenschaftliche Universalbibliotheken) und
- ZKI (Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V.).

DINI verfolgt das Ziel,

- beispielhafte Lösungen bekannt zu machen und für die Nachnutzung zu empfehlen,
- die Erarbeitung, Anwendung und Weiterentwicklung von Standards anzuregen, zu unterstützen sowie Empfehlungen für deren Einsatz zu verbreiten,
- Kompetenzzentren zu registrieren und mit Hilfe moderner netzbasierter Instrumente bekannt zu machen,
- den übergreifenden Erfahrungsaustausch durch Tagungen, Workshops, Expertengespräche u. ä. zu verbessern,
- Förderprogramme bekannt zu machen und neue Programme anzuregen.

## Zusammenfassung

Durch den Aufbau von Dokumenten- und Publikationsservices an Hochschulen wird die Möglichkeit geschaffen, die an der jeweiligen Hochschule entstehenden wissenschaftlichen Publikationen für eine weltweite Verfügbarkeit zu archivieren und anzubieten. Weiterhin trägt dieses Serviceangebot der Infrastruktureinrichtungen – Bibliothek und Rechenzentrum – zur Verbreitung des elektronischen Publizierens als eines neuen Instruments des wissenschaftlichen Arbeitens bei. DINI – die Deutsche Initiative für Netzwerkinformation – unterstützt diese Entwicklungen, um so deutschland- und weltweit ein höheres Niveau der wissenschaftlichen Kommunikation zu erreichen. Dafür ist es notwendig, die Dokumenten- und Publikationsservices zu vernetzen. Ein Netzwerk lokaler Publikationsserver ergänzt die vorherrschenden Verlagspublikationen. Es kann auch als Regulativ für die monopolistischen Tendenzen im wissenschaftlichen Publikationswesen dienen.

Der Aufbau von Dokumenten- und Publikationsservices wird sowohl vom Wissenschaftsrat und der Hochschulrektorenkonferenz gefordert als auch durch die Fördereinrichtungen wie das Bundesministerium für Bildung und Forschung und die Deutsche Forschungsgemeinschaft als aktuelle Aufgabe unterstützt. Es ist wichtig, dass diese Entwicklung nach internationalen Standards und auf der Basis einer gesicherten Technologie erfolgt. Denn nur so ist sichergestellt, dass die Sichtbarkeit und die Wirkung der wissenschaftlichen Arbeitsergebnisse der einzelnen Wissenschaftler, aber auch die Forschungsleistung der gesamten Universität weltweit besser wahrgenommen werden.

Diese zweite Auflage des „DINI-Zertifikats Dokumenten- und Publikationsservice“ trägt aktuellen internationalen Entwicklungen Rechnung und beschreibt, wie Dokumenten- und Publikationsservices das Open-Access-Publizieren wissenschaftlicher Dokumente unterstützen und wie sie sich als Institutional Repositories in ihrer jeweiligen Institution positionieren können. Dies bezieht sich insbesondere auch darauf, Wissenschaftlerinnen und Wissenschaftler dabei zu unterstützen, so genannte Pre- und Postprints bereits über Verlage veröffentlichter wissenschaftlicher Dokumente zeitlich und räumlich unbeschränkt verfügbar zu machen.

Die Vergabe des DINI-Zertifikats 2007 verfolgt diese Ziele:

- Lieferung einer detaillierten Beschreibung der Anforderungen an einen Dokumenten- und Publikationsservice
- Positionierung des Dokumenten- und Publikationsservice als Institutional Repository

- Aufzeigen von Entwicklungsrichtungen bei der Gestaltung von Services und beim Austausch von Informationen
- Darstellung einer für Nutzende und Betreiber sichtbaren Dokumentation der Einhaltung von Standards und Empfehlungen durch diesen Service

Mit der Vergabe eines Zertifikats ermöglicht DINI e.V. eine Qualitätskontrolle für Dokumenten- und Publikationsservices.

Um ein Zertifikat zu erhalten, sind Mindestanforderungen an einen Service und seine Betreiber gestellt, deren Erfüllung zur Wahrung einer modernen wissenschaftlichen Kommunikation unabdingbar ist. Gleichzeitig werden Empfehlungen gegeben, welche die heute vorhersehbare Entwicklung aufgreifen und damit mögliche künftige Anforderungen an Services aufzeigen.

Die Kriterien für das DINI-Zertifikat werden durch eine Arbeitsgruppe anhand internationaler Standards und Entwicklungen überprüft und fortgeschrieben. Das Zertifikat wird deshalb mit dem Jahr der Zertifikatsversion gekennzeichnet.

Mit dieser zweiten Version des Zertifikats wurde der Titel geändert, von „Dokumenten- und Publikationsserver“ hin zu „Dokumenten- und Publikationsservice“. Dies soll verdeutlichen, dass es nicht nur um den Server geht, sondern um Dienste, die serverbasierend angeboten werden.

## 1 Zielstellung

Mit dem World Wide Web hat die Wissenschaft ein neues Kommunikationsmittel geschaffen, das inzwischen auch in großem Umfang kommerziell eingesetzt wird. Die Chancen, die wissenschaftliche Kommunikation durch den gezielten WWW-Einsatz zu verbessern, sind trotz der intensiven Nutzung im Alltag jedes wissenschaftlich Arbeitenden noch lange nicht ausgenutzt.

Insbesondere gibt es noch Defizite bei der gezielten Verbreitung qualitativ hochwertiger Forschungspublikationen. Die Akzeptanz elektronischer Medien nimmt zwar in hohem Maße zu, die Bereitschaft zur aktiven Nutzung als Publikationsmittel bleibt jedoch weitgehend auf die Veröffentlichung in Verlagspublikationen beschränkt, die – insbesondere in den STM-Fächern (Science, Technology, Medicine) – in vielen Fällen auch elektronisch erfolgt. Allerdings hat gerade in diesen Fachgebieten das Quasi-Veröffentlichungsmonopol der Verlage zu exorbitanten Preisentwicklungen geführt, die in zunehmendem Maße die Investitionsmöglichkeiten der Wissenschaftsfinanzierung überschreiten. Der Aufbau lokaler Publikationsservices kann hier als ein Regulativ eingesetzt werden. Gelingt es, die Bereitstellung für die Mehrzahl wissenschaftlicher Publikationen auf nichtkommer-

ziellen Internetservern breit einzuführen, ist ein Kommunikationsnetz geschaffen, das eine unverhältnismäßige Gewinnmaximierung mindestens erheblich erschweren wird.

Mit dem Bereitstellen von Publikationen auf lokalen Servern lassen sich aber auch wesentliche Verbesserungen beim Publizieren von kommerziell weniger interessanten wissenschaftlichen Produktionen erreichen. Die Publikation von Dissertationen im Internet ist ein erfolgreiches Beispiel für diesen Prozess. Wesentliche Voraussetzungen für den Erfolg waren dabei

- die deutschlandweit einheitliche Entwicklung von Standards für die Erfassung von Metadaten,
- die Bereitstellung auf lokalen Servern in Zusammenarbeit von Rechenzentren und Bibliotheken sowie
- ein Workflow für die geregelte Abgabe an die Deutsche Nationalbibliothek, die auch für die langfristige Archivierung zu sorgen bereit ist.

Der Aufbau lokaler Server an den Hochschulen wird deshalb vom Wissenschaftsrat ebenso empfohlen wie von der Deutschen Hochschulrektorenkonferenz. Die Deutsche Forschungsgemeinschaft fördert ihre Entwicklung ebenso wie das Bundesministerium für Forschung und Technologie sie unterstützt. Nationale Wissenschaftseinrichtungen wie die Max-Planck-Gesellschaft bereiten ihren breiten Einsatz vor. Auch international setzt sich z.B. SPARC auf breiter Front für die Entwicklung ein. Das MIT und Universitäten in den Vereinigten Staaten, Großbritannien und Deutschland bieten Open-Source-Software für die Einrichtung an.<sup>1</sup> In den Niederlanden erfolgt eine breite Nutzung im Rahmen des Projekts DARE. Der Einsatz lokaler Publikationssysteme ist auch in Deutschland weit verbreitet. Soll er zu einem durchschlagenden Erfolg werden, ist seine standardisierte Weiterentwicklung notwendig. DINI, die Deutsche Initiative für Netzwerkinformation, hat in den Empfehlungen zum Aufbau von Hochschulservern eine erste Grundlage zur Einführung allgemeiner Regelungen geschaffen. Das hier vorgelegte Papier ist deren konsequente Weiterentwicklung durch die klare Beschreibung von Merkmalen, die gewährleisten, dass Services nationalen Standards und internationalen Entwicklungen entsprechen. Services, die diese Bedingungen erfüllen, können das DINI-Zertifikat erhalten, das ihre Qualität weltweit erkennbar macht. Die zertifizierten Services werden Bindeglieder einer Kette von Content-Providern sein, die entsprechend dem Modell der Open-Archive-Initiative durch standardi-

---

<sup>1</sup> Vgl. OSI Guide to Institutional Repository Software v 3.0 <http://www.soros.org/openaccess/software/>

sierte Metadatenbereitstellung spezialisierten Service-Providern die Aggregation fachlich relevanter Publikationen ermöglichen. An dieser Stelle können sie durchaus auch ein Bindeglied zu kommerziellen Dienstleistern werden.

Wenn es gelingt, die weltweite Bewegung zum Aufbau lokaler Services in standardisierter Form auf die solide Grundlage der Informationsinfrastruktureinrichtungen Rechenzentren und Bibliotheken in ihrer internationalen Vernetzung zu stellen, bestehen reelle Chancen, dass ein neues Fundament für die Kommunikationsgrundstruktur der Wissenschaft gelegt werden kann. Dabei können die sowieso unerlässlichen Investitionen in die Informationsinfrastruktur ohne großen Zusatzaufwand, aber mit hohem Zusatznutzen für die Wissenschaft und die Kostensituation der Hochschulen im Informationswesen besonders effizient eingesetzt werden.

Die Zertifizierung von Services als Garantie ihrer weltweiten Kompatibilität im entstehenden Kommunikationsnetz der Wissenschaft für qualitativ hochwertige Publikationen muss nicht auf Hochschulen beschränkt bleiben. Z. B. wäre es auch für Verlage wünschenswert, wenn sie sich auf dieser Basis in die standardisierte Wissenschaftskommunikation der Zukunft integrierten.

## **2 Kriterien**

Die nachfolgenden Kriterien sind jeweils in zwei Bereiche unterteilt. Zum einen werden Mindeststandards bzw. -anforderungen beschrieben, die von den Dokumenten- und Publikationsservices bzw. deren Anbietern erfüllt werden müssen, um das Zertifikat zu erlangen. Es ist vorgesehen, das DINI-Zertifikat kontinuierlich fortzuschreiben. Deshalb werden aus gegenwärtiger Sicht zusätzlich Empfehlungen für wünschenswerte Anforderungen gegeben, die in zukünftigen Versionen des Zertifikats als Mindeststandards eingestuft werden könnten.

### **2.1 Sichtbarkeit des Gesamtangebotes**

#### **Mindeststandard:**

- Das gesamte Angebot muss über eine Web-Seite erreichbar sein.
- Die Hauptseite des Dokumenten- und Publikationsservice muss von den Hauptseiten der Institution referenziert werden.

### **Empfehlungen:**

- Registrierung des Service beim Directory of Open Access Repositories – OpenDOAR<sup>2</sup> oder beim Registry of Open Access Repositories (ROAR)<sup>3</sup>
- Registrierung des Service als Data-Provider bei der Open Archives Initiative.<sup>4</sup>

## **2.2 Leitlinien (Policy)**

### **Mindeststandard:**

Der Anbieter des Dokumenten- und Publikationsservice veröffentlicht Leitlinien für inhaltliche Kriterien sowie den Betrieb. Darin müssen die Rechte und Pflichten des Anbieters sowie der Autoren/Herausgeber der Dokumente festgeschrieben sein. Die Policy muss enthalten:

- Festlegungen der inhaltlichen, funktionalen und technischen Qualität der Dokumente, die auf einem Dokumentenserver veröffentlicht werden.
- Eine Garantie für bestimmte Archivierungszeiträume in Abhängigkeit von der inhaltlichen, funktionalen und technischen Qualität der Dokumente.
- Verfahren zum Betrieb eines Dokumentenservers und Festlegung bestimmter Leistungen, die der Anbieter des Dokumenten- und Publikationsservice den Autoren und Herausgebern anbietet.
- Festlegung von Rechten und Pflichten der Autoren und Herausgeber.
- Formulierung einer Erklärung zu Open Access.

### **Empfehlungen:**

Wenn der Service in eine Open Access Politik der Institution eingebunden sein soll, ist diese Policy um eine Reihe von Elementen zu erweitern. Neben einer Definition des jeweiligen Verständnisses von ‚Open Access‘ muss die Policy dann Aussagen zu drei Bereichen enthalten:

- Handlungsrichtlinien für Autoren: Angestrebt sein kann das Selbst-Archivieren anderweitig publizierter Dokumente (Open Access „green“) und/oder das elektronische Publizieren im Open Access (Open Access „gold“); die jeweils intendierte Praxis kann von der Institution empfohlen sein oder verpflichtend formuliert werden; die Beachtung resp. Missachtung der intendierten Praxis mit Belohnungen und/oder Sanktionen verbunden sein.

---

<sup>2</sup> <http://www.opendoar.org/>

<sup>3</sup> <http://archives.eprints.org/>

<sup>4</sup> Direkt oder über einen aggregierenden oder kumulierenden Datenprovider bei <http://www.openarchives.org/>

- Diese Handlungsrichtlinien können ferner auf alle Publikationsformen oder jeweils auf einzelne Publikationsformen (z. B. Zeitschriftenartikel) bezogen sein.
- Je nach beabsichtigter Publikationsform und Handlungsrichtlinie werden unterschiedliche Umsetzungsinstrumente als Teil des Dokumentenservice bzw. in dessen Umfeld benötigt; die Spanne reicht dabei von einem einfachen Repository und entsprechenden ‚Upload-Tools‘ bis hin zu Verfahren für die Versionierung und Dokument-Authentifizierung sowie für die automatisierte Lizenzdefinition im Falle der genuinen elektronischen Publikation.

## 2.3 Autorenbetreuung

### Mindeststandard:

- Ein nach außen sichtbares Kontakt- und Beratungsangebot (WWW-Seiten, E-Mail- und telefonische Kontaktadresse, telefonische und persönliche Autorenbetreuung) ist vorhanden.
- Unterstützung des gesamten Publikationsprozesses (einschließlich rechtlicher und technischer Aspekte<sup>5</sup>) ist gegeben.
- Ein Link auf die SHERPA/RoMEO-Liste<sup>6</sup> ist vorhanden.

Wenn der Server in eine Open-Access-Politik der Institution eingebunden ist:

- Bereitstellung von Online-Formularen für Autoren, die ihre Pre- und Postprints einbringen wollen (Document upload tools).

### Empfehlungen:

- Kursangebot zum elektronischen Publizieren mindestens einmal im Semester
- Angebote zum strukturierten Schreiben für Autoren
- Verwendung von Helpdesk-Systemen
- Bereitstellung von Style-Sheets oder Mustervorlagen
- Angebot von Hilfetexten (z. B. zur PDF-Erstellung) zum Herunterladen
- Bereitstellung von Hinweisen zur Nutzung und Zitierung von Dokumenten
- Bereitstellung von Hinweisen zu Urheber- und Verwertungsrechten
- Bereitstellung englischsprachiger Schnittstellen und Beschreibungen

---

<sup>5</sup> Vor allem tiefer gehende Hilfestellungen technischer Art (PDF-Erstellung, Umformatierung etc.) müssen nicht kostenfrei sein. Die Höhe der Kosten sollte für den Hilfesuchenden transparent gestaltet sein.

<sup>6</sup> <http://www.sherpa.ac.uk/romeo.php>

## 2.4 Rechtliche Aspekte

Bei der Bereitstellung von Dokumenten über einen Server ist hinsichtlich rechtlicher Fragen grundsätzlich zu unterscheiden zwischen einer Primärpublikation und der Bereitstellung von Autorenkopien anderweitig bereits veröffentlichter Werke. Im Fall der Primärpublikation sind in der Regel noch alle Rechte bei den Autoren, im Fall der Autorenkopie sind in der Regel durch Autorenverträge schon Rechte an Dritte übertragen worden. Viele Verlage erlauben jedoch durch Verlagskonventionen (Publisher's Policies) übergreifend die Ablage von Autorenkopien auf der Homepage der Autoren oder institutionellen Servern (SHERPA/RoMEO), auch wenn Rechte an sie übertragen wurden.

Grundsätzlich ist die rechtliche Situation am einfachsten, wenn zum Zeitpunkt des Dokumenten-Uploads alle Rechte noch beim Autor liegen.

### Mindeststandard:

#### Bei Primärpublikation:

Es werden bzw. wurden keine ausschließlichen Rechte an Dritte übertragen. (Echte Primärpublikation auf dem Dokumenten- oder Publikationsserver).

- Es ist mit den Autoren eine Vereinbarung (Autorenvertrag) zu schließen, in der den Endnutzern die freie elektronische Verbreitung des Dokuments erlaubt wird und deren Bedingungen festgeschrieben sind. (Recht zur elektronischen Speicherung, insbesondere in Datenbanken, und zum Verfügbarmachen für die Öffentlichkeit zum individuellen Abruf, zur Wiedergabe auf dem Bildschirm und zum Ausdruck beim Nutzer [Online-Nutzung], auch auszugsweise)

Wenn eine anderweitige Veröffentlichung des Werkes geplant ist (z. B. Fachzeitschrift), ist dieser Weg nur dann sinnvoll, wenn sich der Autor sicher ist, dass der Verlag dies unterstützt. Alternativ kann der Weg über Autorenkopien (s. u.) gewählt werden.

#### Bei Autorenkopien:

Das Werk ist oder wird auch anderweitig veröffentlicht, und die Rechte wurden oder werden an Dritte übertragen.<sup>7</sup>

---

<sup>7</sup> Wenn es keine anderweitige Vereinbarung mit dem Verlag gibt, fallen nach einem Jahr die Verwertungsrechte an Beiträgen in Sammelbänden und Periodika zurück an den Autor und erlauben damit die Archivierung einer Autorenkopie.

Folgende Fälle sind zu unterscheiden:

- Eine Lizenzierung des Werkes durch den Autor über entsprechende Vereinbarungen (CC, DPPL)<sup>8</sup> wurde oder wird vorgenommen. Diese erlaubt die Bereitstellung auf dem Server und widerspricht nicht der Rechteübertragung (z. B. Autorenvertrag).
- Der Autorenvertrag enthält Rechte für die Bereitstellung von digitalen Autorkopien.
- Die Bereitstellung von digitalen Autorkopien ist durch Vertragsergänzungen geregelt (Addendum).
- Die Bereitstellung von digitalen Autorkopien ist durch Verlagskonventionen geregelt.

Auf den jeweiligen Fall ist unter Berücksichtigung der Regeln für jedes einzelne Werk hinzuweisen.

## Empfehlungen

- Bei Primärpublikationen: Zu empfehlen ist grundsätzlich die Lizenzierung durch den Autor über entsprechende Vereinbarungen (CC, DPPL), bei der der Autor Endnutzern die freie elektronische Verbreitung erlaubt.
- Bei Primärpublikationen: Angebot an die Autoren, die Nutzung der eingestellten Inhalte durch Lizenzen zu regeln, möglichst schon implementiert in den Upload-Prozess. (Wie z. B. durch das Lizenzmodul in OPUS 3.0<sup>9</sup> realisiert.)
- Zusätzlich zu der Lizenz für Endnutzer kann der Autor Dritten (z. B. Verlagen) weitere Rechte (z. B. Vervielfältigungs- und Verbreitungsrechte) in einem Autorenvertrag einräumen. Es ist dann darauf zu achten, dass die bereits eingeräumten Rechte der gewählten Lizenz dabei nicht widersprechen.
- Verankerung der Rechte in den Metadaten.
- Die Haftungsfrage bei Schadenersatz und/oder Rechtsverfolgung ist zwischen Autoren/Herausgebern und Betreiber vertraglich zu regeln.

---

<sup>8</sup> Unterschiedliche Inhaltsformen, seien es textorientierte Dokumente, Software, Simulationen, Primärdaten oder multimediale Inhalte, erfordern unterschiedliche Lizenzierungsmodelle. Es wird deshalb an dieser Stelle keine Empfehlung für ein bestimmtes Lizenzmodell gegeben. Verbreitet sind etwa die Creative Commons Licence (CCL) <http://creativecommons.org/>, die Lizenz des Digital Peer Publishing Projekts aus NRW (DPPL) <http://www.dipp.nrw.de/lizenzen> oder im Softwarebereich die gängigen Open-Source-Lizenzen, <http://www.opensource.org/licenses/>. Speziell für wissenschaftliche Anwendungen wird Science Commons rechtliche Rahmenbedingungen analysieren.

<sup>9</sup> [http://elib.uni-stuttgart.de/opus/doku/opus\\_sw.php](http://elib.uni-stuttgart.de/opus/doku/opus_sw.php)

Gerade die Propagierung der sog. „green road“, d.h. das Archivieren anderweitig veröffentlichter Dokumente, hat durch den urheberrechtlichen Schutz der Originalveröffentlichung Konsequenzen für den Autor, aber auch den Service-Anbieter. Im Rahmen der Autorenbetreuung sollte daher mindestens auf die SHERPA/RoMEO-Liste hingewiesen werden und die einschlägigen Rechtsprobleme vermittelt werden können. Service-Anbieter sollten sich gegenüber Autoren absichern, dass diese Autorenbetreuung keine verbindliche Rechtsauskunft darstellt. Die Zusammenarbeit mit der jeweiligen juristischen Fakultät, dem Justitiariat einer Institution, der DINI AG Urheberrecht<sup>10</sup> oder dem Aktionsbündnis „Urheberrecht für Bildung und Wissenschaft“<sup>11</sup> kann in diesem Zusammenhang nützlich sein.

## 2.5 Sicherheit, Authentizität und Integrität

### 2.5.1 Server

#### **Mindeststandard:**

- Das Betriebskonzept gewährleistet eine angemessene Verfügbarkeit des Systems.
- Es existiert eine Dokumentation des technischen Systems mit
  1. relevanten Versionsangaben und technischen Parametern zu allen Komponenten
  2. Zugangsregelung zum Server
    - räumlich
    - auf das System bezogen
    - personell (Verantwortlichkeit und Vertretung)
  3. Regelung der Wartung des Systems
- Einsatz einer Technologie zur Sicherung und Wiederherstellung der Server-Software, der Metadaten und der Dokumente mit täglicher Sicherung.
- Sichere Installation des Systems und der Software-Komponenten.
- Regelmäßige Wartung des Systems.
- Kontrollierte und nachweisbare Aufnahme von Dokumenten aus technischer Sicht.

#### **Empfehlungen:**

- SSL-Zertifizierung mit vertrauenswürdigen Zertifikat für verschlüsselte Kommunikation wird eingesetzt.

---

<sup>10</sup> [http://www.dini.de/dini/arbeitsgruppe/arbeitsgruppe\\_details.php?ID=31](http://www.dini.de/dini/arbeitsgruppe/arbeitsgruppe_details.php?ID=31)

<sup>11</sup> <http://www.urheberrechtsbuenndnis.de/>

- Aufteilung der Dokumentation des technischen Systems in einen veröffentlichten und einen internen Teil.
- Autonome Überwachungs- und Alarmfunktion bei Ausfall des Servers oder einzelner Komponenten.
- Havarieszenarien sind vorhanden.

## 2.5.2 Dokumente

### **Mindeststandard:**

- Verwendung von Persistent Identifiers, dazu zählen Systeme, die einen Resolver-Dienst besitzen, z. B. urn:nbn oder DOI.
- Ein inhaltlich verändertes Dokument ist wie ein neues Dokument zu behandeln (neuer Persistent Identifier).
- Archivierung der eingereichten Originaldateien des Autors auch im Ablieferungsformat (zu anderen Formaten vgl. Abschnitt 2.8).
- Diese Mindeststandards sind in der Policy bzw. den Leitlinien zu dokumentieren.

### **Empfehlungen:**

- Einsatz eines Verfahrens zum Nachweis der Unversehrtheit der Dokumente (Hash-Wert) sowie Veröffentlichung von Verfahren und Hash-Werten.
- Fortgeschrittene digitale Signatur nach § 2 Abs. 2 SigG 2001 wird verwendet.
- Erstellung von Archivierungsformaten im Hinblick auf den Export in Langzeitarchivierungssysteme<sup>12</sup> (vgl. Abschnitt 2.8 und 4.7).
- Darstellung der Dokumente in einem gängigen Präsentationsformat. Wenn dies nicht möglich ist, sollte entweder eine Visualisierungs-Software zum Herunterladen oder eine Internet-Referenz angeboten werden.

## 2.6 Erschließung

### 2.6.1 Sacherschließung

#### **Mindeststandard:**

- Eine Policy zur Sacherschließung muss vorhanden und dem Autor bekannt sein.
- Verbale Sacherschließung durch freie Schlagwörter oder klassifikatorische Erschließung wird durchgeführt.

---

<sup>12</sup> <http://www.langzeitarchivierung.de>

- Dewey-Dezimalklassifikation (DDC) gemäß der Verwendung in der Deutschen Nationalbibliografie als allgemeine klassifikatorische Erschließung aller Dokumente (entsprechend den DINI-OAI-Empfehlungen)<sup>13</sup> wird angewandt.

### **Empfehlungen:**

- Mindestens ein weiteres normiertes System verbaler oder klassifikatorischer Erschließung (allgemein oder fachspezifisch, z. B. Schlagwortnormdatei, LoC Subject Headings, CCS, MSC, PACS etc.) wird verwendet.
- Englischsprachige Schlagwörter werden vergeben.
- Kurzzusammenfassungen/Abstracts in Deutsch und Englisch werden angeboten.

## **2.6.2 Metadatenexport**

### **Mindeststandard:**

- Metadaten werden frei zugänglich angeboten.
- Metadaten sind nach Dublin Core Simple (ISO 15836:2003) strukturiert.

### **Empfehlungen:**

- Metadaten sind nach Dublin Core Qualified strukturiert<sup>14</sup>.
- Metadaten sind nach ONIX<sup>15</sup> strukturiert.
- Technische und/oder Archivierungsmetadaten – einschließlich ggf. Print-on-Demand-Daten – werden angeboten (z. B. PREMIS<sup>16</sup>, LMER<sup>17</sup>).
- Import und Export der Metadaten in und aus bibliografischen Datenbanken (z. B. Literaturverwaltungsprogramme, Verbünde, OPACs) werden unterstützt.
- Linklisten zur Indexierung durch Roboter von Suchmaschinen (z. B. Google, Fast, Scirus etc.) werden angeboten.

---

<sup>13</sup> <http://edoc.hu-berlin.de/series/dini-schriften/2005-2-de2/PDF/2-de2.pdf>  
(urn:nbn:de:kobv:11-10049220)

<sup>14</sup> Für DC Qualified gibt es derzeit keine verbindliche Definition oder Norm.  
Vgl. <http://dublincore.org/documents/abstract-model/> als Rahmen.

<sup>15</sup> <http://www.editeur.org/onix.html>

<sup>16</sup> PREMIS: PREservation Metadata Implementation Strategies,  
<http://www.oclc.org/research/projects/pmwg/>

<sup>17</sup> LMER: Langzeitarchivierungsmetadaten für elektronische Ressourcen, <http://nbn-resolving.de/urn/resolver.pl?urn=urn:nbn:de:1111-2005041102> (urn:nbn:de:1111-2005041102)

## 2.6.3 Schnittstellen

### Mindeststandard:

- Webserverschnittstelle für Nutzer ist vorhanden.
- OAI-PMH 2.0 entsprechend den DINI-OAI-Empfehlungen wird unterstützt.

### Empfehlungen:

- Eine Nutzung des OAI-Protokolls zum Austausch komplexer Metadatenschemata wird unterstützt.
- Webserviceschnittstelle (z. B. SOAP)<sup>18</sup> ist vorhanden.
- Z39.50<sup>19</sup>- und /oder SRU<sup>20</sup>-Schnittstellen sind vorhanden.

## 2.7 Zugriffsstatistik

### Mindeststandard

- Jeder Dokumentenserver muss im Rahmen der rechtlichen Bestimmungen eine eigene konsistente Zugriffsstatistik führen (Webserver-Log).
- Webserver-Logs sind zur längerfristigen Speicherung zu anonymisieren<sup>21</sup>.
- Der Statistik muss eine Erklärung bzw. Dokumentation beigefügt sein, die beschreibt, nach welchen Kriterien die Statistik erstellt bzw. aufbereitet wurde. Es muss darauf hingewiesen werden, dass die Zugriffszahlen i. d. R. nicht zu einem Vergleich zwischen unterschiedlichen Dokumenten-Servern bzw. Diensten eingesetzt werden können, sondern dass die Zugriffszahlen allein eine Vergleichbarkeit der Dokumente auf einem Server erlauben.

### Empfehlungen

- Zugriffe auf Dokumente durch automatisierte Agenten, Roboter u. ä. werden herausgefiltert<sup>22</sup>.
- Webserver-Logs werden einheitlich nach dem Counter Code of Practice aufbereitet<sup>23</sup>.

---

<sup>18</sup> <http://www.w3.org/TR/soap/>

<sup>19</sup> [http://www.niso.org/standards/resources/Z3950\\_Resources.html](http://www.niso.org/standards/resources/Z3950_Resources.html)

<sup>20</sup> <http://www.loc.gov/standards/sru/>

<sup>21</sup> Gemäß den datenschutzrechtlichen Bestimmungen § 4 Abs. 4 Nr. 2 TDDSG, § 18 Abs. 4 Nr. 2 MDSfV. Beispiel unter <http://www.zendas.de/technik/sicherheit/apache/index.html>

<sup>22</sup> Z. B. <http://www.robotstxt.org/wc/active/all.txt>

<sup>23</sup> Orientierung v. a. an [http://www.projectcounter.org/cop\\_books\\_ref.html#rbr\\_5](http://www.projectcounter.org/cop_books_ref.html#rbr_5) und Anhang D [http://www.projectcounter.org/cop\\_books\\_appendix\\_d.html](http://www.projectcounter.org/cop_books_appendix_d.html)

- Einem Dokument ist seine Zugriffsstatistik als dynamisches Metadatum zugeordnet und für den Endnutzer sichtbar.<sup>24</sup>

## 2.8 Langzeitverfügbarkeit

### Mindeststandard:

- Dauerhafte Verbindung der Metadaten mit den Dokumenten (z. B. Verbindung über Persistent Identifier oder zusammen in einem Container)
- Definition einer Mindestzeit der Dokumentverfügbarkeit, die 5 Jahre nicht unterschreiten darf, ist in der Policy vorhanden.
- Die gegebenenfalls zusätzlich zu den eingereichten Originaldateien des Autors erstellten Archivkopien sind frei von Schutzmaßnahmen (DRM), die eine Anwendung von Strategien zur Langzeitverfügbarkeit (Migration, Emulation) verhindern.

### Empfehlungen:

- Sicherstellung der Langzeitverfügbarkeit, ggf. durch Kooperation mit einer Archivierungsinstitution
- Nutzung von offenen Dateiformaten, die zur Langzeitarchivierung geeignet (z. B. PDF/A, ODF, TXT, HTML, TEX) und frei von Schutzmaßnahmen (DRM) sind.
- Erstellung von technischen Metadaten zur Langzeitarchivierung (z. B. mit dem Tool JHOVE)<sup>25</sup>.
- Eindeutige Identifizierung des jeweiligen Dateiformats in den Metadaten mit Referenzen zu öffentlich zugänglichen File Format Registries.
- Eine Policy zum Umgang mit Löschungen von Dokumenten ist vorhanden.
- Unterstützung des Imports und Exports von Objektpaketen, die neben den eigentlichen Dokumenten auch Metadaten (bibliografische und technische Daten zur Langzeitarchivierung) enthalten (z. B. im Universellen Objektformat)<sup>26</sup>.

## 3 Vergabemodus und Evaluierung

Das „DINI-Zertifikat Dokumenten- und Publikationsservice“ wird durch die DINI-Geschäftsstelle bzw. eine von ihr beauftragte Arbeitsgruppe vergeben. Verbunden

---

<sup>24</sup> Z. B. in PsyDok (<http://psydok.sulb.uni-saarland.de/>) und MONARCH (<http://archiv.tu-chemnitz.de/>) jeweils von den Indexseiten (Document Splash Pages) aus realisiert.

<sup>25</sup> <http://hul.harvard.edu/jhove/>

<sup>26</sup> [http://kopal.langzeitarchivierung.de/index\\_objektspezifikation.php.de](http://kopal.langzeitarchivierung.de/index_objektspezifikation.php.de)

mit dem Zertifikat, das die Jahreszahl der entsprechenden Zertifikatsversion enthält, wird in einer Urkunde die Bescheinigung über die Erfüllung der Mindestanforderungen für Dokumenten- und Publikationsservices ausgestellt.

Die Ausstellung des DINI-Zertifikats ist kostenpflichtig:

- Nonprofit-Organisationen  
Mitglieder von DINI 50,00 €, Nichtmitglieder von DINI 100,00 €
- Profit-Organisationen  
Mitglieder von DINI 150,00 €, Nichtmitglieder von DINI 250,00 €

Der Anbieter des Dokumenten- und Publikationsservice bewirbt sich bei DINI um die Zertifizierung. Dazu füllt er ein auf den DINI-WWW-Seiten angebotenes Formular aus, das in Form einer Checkliste die in Kapitel 2 aufgelisteten Kriterien enthält. Mittels des Formulars legt der Betreiber dar, ob und in welchem Umfang die einzelnen Kriterien durch den Service erfüllt werden. Neben Erläuterungen im Formular können URLs oder andere Bezugsmöglichkeiten für weitere der Erläuterung dienende Informationen angegeben werden.

Durch eine von der DINI-Geschäftsstelle beauftragte Arbeitsgruppe erfolgt die Überprüfung der Angaben. Dazu ist der Arbeitsgruppe der freie Zugang zum zu zertifizierenden Service zu gestatten. Gegebenenfalls werden an die Betreiber Rückfragen gerichtet. Eine Kontrolle vor Ort ist nur im Ausnahmefall vorgesehen. Sollten im Rahmen der Überprüfung zusätzliche Kosten entstehen, so sind diese durch den Service-Anbieter zu tragen. Der Anbieter wird durch DINI darüber zuvor informiert.

Für die Ausstellung eines DINI-Zertifikats wird im Regelfall ein Zeitraum von zwei Monaten angesetzt. Das Zertifikat ist zeitlich nicht befristet. Aufgrund des eingetragenen Jahres der Zertifikatsversion ist jederzeit überprüfbar, welchen Leistungsanforderungen der Service genügt.

Der Anbieter des zertifizierten Service hat das Recht, seinen Service als von DINI „Zertifizierten Dokumenten- und Publikationsservice“ zu bezeichnen und dies durch ein Logo auf der Startseite oder in einer anderen geeigneten Form anzuzeigen. Jede missbräuchliche Verwendung der Bezeichnung und des Logos wird gemäß dem Urheberrecht verfolgt.

Das neue Zertifikat 2007 trägt der aktuellen, internationalen Entwicklung Rechnung und fördert die Positionierung der deutschen Dokumenten- und Publikationsservices als Institutional Repositories im Sinne von vertrauenswürdigen, zukunftsorientierten Services, die auch die Entwicklungen des Open Access berücksichtigen.

Dadurch ergeben sich eine Reihe neuer Mindeststandards sowie zugleich neue Empfehlungen zur Weiterentwicklung der Dokumenten- und Publikationsservices. Alle bisher ausgestellten Zertifikate behalten auch weiterhin entsprechend der Zertifikatsversion ihre Gültigkeit.

Für die bisher zertifizierten Institutionen besteht die Möglichkeit, das Zertifikat 2007 innerhalb eines Jahres nach Veröffentlichung durch ein verkürztes Zertifizierungsverfahren zu erreichen. Es werden dann nur die neuen Mindeststandards geprüft, und es fällt eine um 50% ermäßigte Zertifizierungsgebühr an. Bei nachträglich festgestellten Verstößen gegen die Kriterien des Zertifikats kann das Zertifikat von DINI aberkannt werden.

## 4 Erläuterungen und Beispiele

Im Folgenden sind zu den Kriterien des Zertifikats Erläuterungen und praktische Umsetzungsbeispiele angeführt.

Ein lokaler Dokumentenserver (Institutional Repository) soll die Speicherung, Verwaltung, Bereitstellung, Archivierung, Recherche und den Zugriff auf elektronische Quellen einer Institution gewährleisten.

### 4.1 Sichtbarkeit des Service

Eine gute Sichtbarkeit des Service ist hier zum einen innerhalb der Institution zu verstehen, für die bzw. in der er angeboten wird. Zum anderen ist damit die Integration des Service in andere fachliche oder institutionenbezogene Dienste gemeint. Registrierungsinstanzen wie openarchives.org oder OpenDOAR sind dabei allgemeine Vermittler zwischen Dokumenten- und Publikationsservices und darauf aufbauenden Diensten. Technisch sind für die Integration die im Abschnitt 2.6 angesprochenen Metadaten und Schnittstellen entscheidend.

### 4.2 Leitlinien (Policy)

#### 4.2.1 Beispiel: Leitlinien für den Dokumenten- und Publikationsserver der Humboldt-Universität zu Berlin

*1 Ziele und inhaltliche Kriterien für den Dokumenten- und Publikationsserver der Humboldt-Universität*

*Der Dokumenten- und Publikationsserver bietet allen Angehörigen der Humboldt-Universität die organisatorischen und technischen Rahmenbedingungen zur elektronischen Publikation wissenschaftlicher Dokumente. Im Rahmen*

dieses Gemeinschaftsangebotes von Rechenzentrum und Universitätsbibliothek der Humboldt-Universität werden wissenschaftliche Dokumente von hoher Relevanz unter Einhaltung von Qualitätsstandards im Internet für Forschung und Lehre bereitgestellt.

Die elektronischen Dokumente erhalten dauerhafte Adressen und werden über nationale und internationale Bibliothekskataloge, Suchmaschinen sowie andere Nachweisinstrumente erschlossen. Der Dokumenten- und Publikationsserver bietet durch besondere Maßnahmen wie digitale Signaturen und Zeitstempel einen Schutz gegen Verfälschungen. Darüber hinaus wird eine Langzeitarchivierung der elektronischen Dokumente gewährleistet.

Betrieb und Weiterentwicklung des Dokumenten- und Publikationsservers sind eingebunden in nationale und internationale Initiativen und Projekte wie die »Networked Digital Library of Theses and Dissertations« (NDLTD) oder die »Open Archives Initiative« (OAI).

2 Der Sammelauftrag der Universitätsbibliothek der Humboldt-Universität für elektronische Dokumente

Der Sammelauftrag der Universitätsbibliothek umfasst die Speicherung, Katalogisierung und Archivierung aller durch Mitarbeiterinnen und Mitarbeiter der Humboldt-Universität veröffentlichten elektronischen wissenschaftlichen Dokumente. Dies bezieht sich sowohl auf rein elektronische Publikationen als auch auf elektronische Versionen gedruckter Dokumente.

Einbezogen sind bedeutsame, aus inhaltlichen, konservatorischen oder aus Gründen der ortsunabhängigen Benutzung retrodigitalisierte ältere Bestände der Universitätsbibliothek und anderer Einrichtungen.

Die Urheberrechte der Autorinnen und Autoren bleiben gewahrt. Die Veröffentlichung auf dem Dokumenten- und Publikationsserver steht einer weiteren Veröffentlichung der Dokumente in Fachzeitschriften oder Monographien sowie auf anderen Servern nicht entgegen. Gemäß den Empfehlungen des Wissenschaftsrats werden alle Wissenschaftlerinnen und Wissenschaftler der Humboldt-Universität aufgefordert, sich beim Abschluss von Verlagsverträgen ein entsprechendes weiteres Nutzungsrecht zu sichern und die von ihnen verfassten Dokumente zusätzlich – eventuell nach einer Sperrfrist – auf dem Dokumentenserver zu veröffentlichen.

Die Einhaltung von Urheber- und Verwertungsrechten Dritter liegt in der Verantwortung der Autorinnen und Autoren bzw. der Herausgeber der elektronischen Dokumente.

### 3 Das elektronische Dokument

Unter dem Begriff »elektronisches Dokument« wird im Sinne dieser Leitlinien ein Dokument verstanden, welches auf Text und Grafik basiert, in digitaler Form auf einem Datenträger gespeichert ist und über Rechnernetze verbreitet wird. Künftig wird angestrebt, den Begriff auf multimediale Dokumente, die Audio- und Video-Sequenzen enthalten, zu erweitern.

Ein über den Dokumenten- und Publikationsserver zu veröffentlichendes elektronisches Dokument erfüllt folgende Bedingungen:

Es ist zur Verbreitung in der Öffentlichkeit bestimmt.

Es stellt kein dynamisches Dokument dar. Sind Veränderungen notwendig, wird das geänderte elektronische Dokument als neue Version gespeichert.

Es entspricht den von Rechenzentrum und Universitätsbibliothek der Humboldt-Universität vorgegebenen technischen Parametern.

4 Elektronische Dokumente, die über den Dokumenten- und Publikationsserver veröffentlicht und verbreitet werden

Folgende Kategorien elektronischer Dokumente werden gespeichert und über den Dokumenten- und Publikationsserver verbreitet:

Publikationen und Publikationsreihen der Humboldt-Universität mit wissenschaftlichen Inhalten wie die Öffentlichen Vorlesungen der Humboldt-Universität oder die Schriftenreihe der Universitätsbibliothek,

durch Angehörige der Humboldt-Universität herausgegebene Publikationen und Publikationsreihen wie Sammelwerke, Kongressbände, Forschungsberichte, Zeitschriften (E-Journals) oder Reihen,

Dokumente, deren Veröffentlichung durch Prüfungsordnungen vorgeschrieben ist (Dissertationen und Habilitationsschriften),

Publikationen und Publikationsreihen von mit der Humboldt-Universität assoziierten Einrichtungen und Personen,

Dokumente von Studierenden der Humboldt-Universität wie Diplom-, Magister- und Seminararbeiten, wenn die Publikation auf Empfehlung durch ein Mitglied des Lehrkörpers erfolgt.

Die Verbreitung der elektronischen Dokumente kann räumlich eingeschränkt – etwa auf den Campus der Humboldt-Universität – oder zeitlich befristet werden.

### 5 Technische Besonderheiten des Dokumenten- und Publikationservers

Durch die Vergabe und den Nachweis qualifizierter elektronischer Signaturen erhalten die elektronischen Dokumente ein rechtswirksames Echtheitszertifikat.

Die Vergabe der qualifizierten elektronischen Signaturen erfolgt entsprechend dem Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG).

Die elektronischen Dokumente werden mit individuellen und dauerhaften Adressen versehen, welche einen unmittelbaren Zugriff auf die Dokumente erlauben.

Das Auffinden der elektronischen Dokumente ist über Bibliothekskataloge, Recherchen in bibliographischen Metadaten, Suchterme innerhalb der Strukturen der elektronischen Dokumente und über alphabetische und klassifikatorische Ordnungen sowie dynamisch erstellte Listen und Indizes möglich.

Für die Erschließung, Speicherung und Archivierung der elektronischen Dokumente werden internationale Standards wie die Richtlinien der Open Archives Initiative (OAI) genutzt und weiterentwickelt.

Bei Verwendung des Formates SGML/XML wird eine Archivierungsgarantie von 50 Jahren gegeben. Die Archivierungsdauer anderer Formate hängt von der Verfügbarkeit des Formates, der Betrachtungssoftware sowie den Konvertierungsmöglichkeiten ab.

## 6 Organisatorische Regelungen

Der Dokumenten- und Publikationsserver wird von Rechenzentrum und Universitätsbibliothek der Humboldt-Universität gemeinsam betrieben.

Die elektronische Veröffentlichung ist für Angehörige der Humboldt-Universität und Angehörige von mit der Humboldt-Universität assoziierten Einrichtungen kostenfrei.

Die Abgabe der elektronischen Dokumente zur Verbreitung über den Dokumentenserver erfolgt in der Universitätsbibliothek der Humboldt-Universität.

Für die Veröffentlichung notwendige zusätzliche Arbeiten wie die Aufbereitung der elektronischen Dokumente oder die Konvertierung in andere Formate werden von den Mitarbeiterinnen und Mitarbeitern des Rechenzentrums und der Universitätsbibliothek nach Absprache betreut oder durchgeführt. Arbeiten, die einen bedeutenden Mehraufwand erfordern, werden nach den Sätzen der Gebührenordnungen des Rechenzentrums und der Universitätsbibliothek in Rechnung gestellt.

Ansprechpartner für alle den Dokumenten- und Publikationsserver betreffenden Fragen ist die gemeinsame Arbeitsgruppe des Rechenzentrums und der Universitätsbibliothek »Elektronisches Publizieren«.

#### 4.2.2 Beispiel: Open Access Politik der Georg-August-Universität Göttingen

Die Open Access Politik der Georg-August-Universität Göttingen  
Das Internet als Kommunikations-, Informations- und Publikationsmedium ist inzwischen für die globale Wissenschaftsgemeinschaft unverzichtbar geworden. Zugleich ist das wissenschaftliche Kommunikations- und Publikationswesen in eine kostenträchtige Abhängigkeit vom kommerziell dominierten Verlagsmarkt geraten. Dies zeigt sich vor allem in überproportionalen Preisanstiegen für wissenschaftliche Zeitschriften, mit denen die Etats der Universitäten belastet werden. Da viele Titel abbestellt werden müssen, wird der schnelle Zugriff auf relevante wissenschaftliche Literatur zunehmend erschwert. Weltweit wird deshalb daran gearbeitet, immer mehr relevante Dokumente nach dem Prinzip des Open Access bereitzustellen.

Das Präsidium der Universität Göttingen empfiehlt den Autoren und Autorinnen der Universität nachdrücklich, veröffentlichte, wissenschaftlich referierte Artikel, soweit rechtlich zulässig, als Kopie auf den Publikationenserver der Universität bei der SUB Göttingen abzulegen. Dies betrifft die Publikationen einer großen Zahl von Verlagen, die dieser Selbst-Archivierung durch Autoren an ihren Institutionen zustimmen.

Im Online-Verzeichnis SHERPA/ROMEO können Sie nachlesen, welche wissenschaftlichen Verlage Ihnen das Selbstarchivieren unter welchen Bedingungen gestatten. Hierzu gehören große Verlagskonsortien wie Elsevier und Springer. Gemäß § 38a des UrhG fällt nach einem Jahr das Recht, einen Zeitschriftenartikel anderweitig zu veröffentlichen, an den Autor zurück, sofern es keine besondere Regelung im Vertrag gab. Publikationen, die vor 1995 erschienen sind, können Sie ohne Probleme bereitstellen, da die Rechte an der Veröffentlichung im Internet generell bei Ihnen als Autor liegen. Für das konkrete Vorgehen bei der Speicherung und bei Fragen zur rechtlichen Zulässigkeit wenden Sie sich bitte an [...].

Die Selbstarchivierung der Publikationen hat Vorteile für Autoren wie Verlage: Nachweisbar werden Ihre Publikationen häufiger zitiert, wenn sie zusätzlich Open Access bereit stehen. Dies führt zu einer größeren Sichtbarkeit und Wirkung Ihrer wissenschaftlichen Arbeitsergebnisse. Zugleich wird damit der Impactfaktor der Zeitschrift erhöht, was auch im Interesse der kommerziellen Verlage ist. Darüber hinaus werden die Forschungsleistungen der Universität

über den international vernetzten lokalen Universitätsserver weltweit besser wahrgenommen.

Wissenschaftliche Artikel auf so genannten Preprint-Servern – noch vor der Veröffentlichung in Zeitschriften, Sammelwerken usw. – abzulegen, wird in vielen Fachgebieten praktiziert. Erfolgreichstes Beispiel ist das Portal arXiv: Es ist zu einer unverzichtbaren Plattform für viele Wissenschaftler geworden, die auf diesem Wege zeitnah den aktuellen Forschungsstand verfolgen können. Begonnen hat arXiv als Server für Physiker; mittlerweile wird er auch in der Mathematik, Biologie und Informatik vielfach genutzt. Diese Methode, eigene Forschungsergebnisse auf einem internationalen, kostenfrei zugänglichen Server bereit zu stellen, wird von wissenschaftlichen Verlagen akzeptiert und bisweilen durchaus erwünscht, da sie hier die Arbeit in ihrer Rohform und eventuelle Reaktionen anderer Wissenschaftler darauf einsehen können.

Weltweit gehen zunehmend Wissenschaftler und Bibliotheken dazu über, auch Preprints auf die lokalen Universitätsserver zu legen. Sind sie, wie der Göttinger Server, mit einer OAI-Schnittstelle (Open Archives Initiative) versehen, werden sie von global arbeitenden Verzeichnissen wie OAIster zugänglich gemacht. Auch Dienste wie Google Scholar oder kommerzielle Produkte wie Web of Science und SCOPUS weisen inzwischen Preprints nach, wenn sie auf einem anerkannten Server wie dem der Universität Göttingen abgelegt werden.

Das Institute for Scientific Indexing (ISI) ermittelt laufend die Zitierraten wissenschaftlicher Zeitschriften. Unter den Naturwissenschaften liegen die traditionellen Spitzenreiter Nature und Science zwar noch immer vorne. Doch es gibt inzwischen Open Access-Zeitschriften, z. B. die Public Library of Science (PLoS) oder BioMed Central (BMC), die Zitierraten („impact factors“) von bis zu 13,9 erreichen und sich damit Plätze an der Spitze erobert haben. PLoS oder BMC finanzieren sich nicht über den Verkauf ihrer Zeitschriften an die Leser oder Bibliotheken, sondern durch Gebühren, die auf Seiten der Autoren erhoben werden. Zum Teil kann die SUB Göttingen diese Kosten ganz oder teilweise durch günstige Gemeinschaftskonditionen übernehmen. Die großen Forschungsförderinstitutionen haben sich darüber hinaus in der „Berlin Declaration“ für die Unterstützung des Open Access-Ansatzes ausgesprochen und signalisiert, dass bei der Beantragung von Forschungsgeldern auch Publikationsgebühren für die Open Access-Veröffentlichung eingeworben werden können.

Für die Gründung neuer Publikationsorgane können Sie die Angebote der Universität wie den Universitätsverlag und den Dokumentenserver nutzen,

die von der SUB betreut werden. Sie als wissenschaftlicher Autor arbeiten häufig auch als Gutachter, Herausgeber oder Redakteur für wissenschaftliche Zeitschriften. Achten Sie darauf, welche Preispolitik der Verlag gegenüber den Abnehmern verfolgt und wirken Sie gegebenenfalls auf eine bessere Open Access-Politik der Verlage hin.

LINKS ZU ERWÄHNTEN SEITEN:

- ArXiv <http://www.arxiv.org>
- Berliner Erklärung zu Open Access  
<http://www.zim.mpg.de/openaccess-berlin/berlindeclaration.html>
- BioMed Central <http://www.Biomedcentral.com>
- DOAJ (Directory of Open Access Journals) <http://www.doaj.org>
- Elektronische Zeitschriftenbibliothek <http://www.bibliothek.uni-regensburg.de>
- Google Scholar <http://scholar.google.com>
- Institute for Scientific Indexing <http://www.isinet.com/cit>
- OAI (Open Archives Initiative) <http://www.openarchives.org>
- OAIster (OAI-Harvester) <http://www.oaister.org>
- Open Access-Server der Universität Göttingen <http://webdoc.sub.gwdg.de/>
- Public Library of Science <http://www.plos.org>
- SCOPUS <http://www.scopus.com>
- SHERPA/ROMEO <http://www.sherpa.ac.uk/romeo.php>
- Universitätsverlag Göttingen <http://univerlag.uni-goettingen.de>
- Web of Science <http://www.isinet.com/products/citation/wos/>

### 4.3 Autorenbetreuung

Eine wichtige Zielstellung des elektronischen Publizierens an Hochschulen besteht darin, alle an der Hochschule entstehenden Publikationen zu archivieren, um den wissenschaftlichen Output gezielt vermarkten und einsetzen zu können. Für eine Langzeitarchivierung und eine Weiterverarbeitung der digitalen Publikationen ist die einheitliche Speicherung bezogen auf Datenformat, Signierung, Metadaten etc. sinnvoll.

Die Realisierung dieses Ziels beginnt bereits bei der Beratung und Betreuung von Autoren und Herausgebern. So bildet die Benutzung bestimmter Formatvorgaben für ausgewählte Textverarbeitungssysteme eine Grundlage für das strukturierte Schreiben im digitalen Zeitalter.

Deshalb wird empfohlen, ein gezieltes Weiterbildungsangebot an der Hochschule im Bereich elektronisches Publizieren aufzubauen und strategische Vorteile in

Form von Hilfen oder Vergünstigungen zu erarbeiten, um die Attraktivität des elektronischen Publizierens für Autoren zu erhöhen.

Dies alles sollte in eine universitätsweite Infrastruktur „Elektronisches Publizieren“ münden. Nur so können die Weiterentwicklung der Beratungsleistungen und der Technologien sichergestellt sowie technische Anforderungen an die Autoren formuliert und umgesetzt werden, die eine langfristige Speicherung und Verfügbarkeit der Dokumente ermöglichen, wie z. B. die Nutzung von DTDs für Dissertationen nach internationalen Standards oder die Unterstützung von Winword-Dokumentvorlagen für Dissertationen oder die Festlegung und Durchsetzung von Richtlinien für LaTeX, wie dies zurzeit bereits an der Humboldt-Universität zu Berlin geschieht.

#### **4.4 Rechtliche Aspekte**

Unabhängig von der Tatsache, ob es sich um eine Primärpublikation oder um eine sog. Autorkopie handelt, müssen die im „DINI-Zertifikat – Dokumenten- und Publikationsservice“ geforderten Leitlinien Rechte und Pflichten von Autoren/Herausgebern sowie der betreibenden Institution beschreiben. Aus dieser Policy leiten sich die rechtswirksamen Vereinbarungen zwischen Serviceanbietern einerseits und Autoren/Herausgebern bzw. Nutzern andererseits ab.

Geregelt muss sein, dass Autoren dem Anbieter folgende, nicht ausschließliche Nutzungsrechte einräumen:

- Das Recht zur elektronischen Speicherung, insbesondere in Datenbanken, und zum Verfügbarmachen für die Öffentlichkeit zum individuellen Abruf, zur Wiedergabe auf dem Bildschirm und zum Ausdruck beim Nutzer (Online-Nutzung), auch auszugsweise
- Das Recht zur Meldung und Weitergabe der Daten an eine Langzeitarchivierungsstelle
- Das Recht zur Konvertierung zum Zwecke der Archivierung unter Beibehaltung der inhaltlichen Integrität

Diese Rechte gelten auch für die vom Autor gelieferten Metadaten (z.B. Abstracts)

Die Einräumung dieser Rechte dient neben der Publikation zur Sicherstellung der Langzeitverfügbarkeit der elektronischen Dokumente auf den Dokumenten- und Publikationsservern.

Im Gegenzug sollen die Anbieter des Service den Autoren folgende Rechte einräumen:

- Das Recht des Verfassers/Herausgebers, das Werk, auch auszugsweise, auf persönlichen Servern oder Servern von Institutionen verfügbar zu machen. Dieses Recht soll für das unveränderte Werk gelten. Veränderte Versionen des Werkes sind kenntlich zu machen.
- Das Recht des Autors/Herausgebers, die veröffentlichten Inhalte nach einem Lizenzmodell zu lizenzieren und damit das Verhältnis zwischen Autor/Herausgeber und Nutzer zu regeln.

Bei derartigen Regelungen ist zu berücksichtigen, dass bestimmte Nutzungsrechte bei anderweitig veröffentlichten Dokumenten durch bereits getroffene vertragliche Vereinbarungen schon geregelt sind. Die SHERPA/RoMEO-Liste liefert hier i. d. R. eine gute Orientierung.

### **Rechte Dritter:**

- Die Autoren/Herausgeber müssen gegenüber dem Anbieter versichern, dass durch das zu veröffentlichende Werk oder Teile desselben (z. B. Bilder) keine Rechte Dritter verletzt werden. Im Falle der sog. Autorenkopie ist dies üblicherweise bereits in den bestehenden Autorenverträgen geregelt.
- Die Autoren/Herausgeber sollen versichern, in Zweifelsfällen oder bei Entstehen vermeintlicher oder tatsächlicher diesbezüglicher Rechtshindernisse den Anbieter hiervon unverzüglich in Kenntnis zu setzen.
- Die Haftungsfrage bei Schadenersatz und/oder Rechtsverfolgung ist zwischen Autoren/Herausgebern und Anbieter vertraglich zu regeln.

### **Print-Publikationen:**

Das Folgende bezieht sich in erster Linie auf einen ggf. anzubietenden Extra-Service durch Hochschulen/Hochschulverlage.

Bei Ausgaben in gedruckter Form sollten Hochschulen/Hochschulverlage prüfen, ob sie von Autoren/Herausgebern zum Schutz für ihre Investitionen in die Druckausgabe das ausschließliche Verwertungsrecht an der gedruckten Form benötigen und sich dies ggf. übertragen lassen. In diesem Falle sollten sich die Autoren/Herausgeber verpflichten, über einen festzulegenden Zeitraum hinweg von jeder anderweitigen Vervielfältigung und Verbreitung und/oder unkörperlichen Übermittlung und Wiedergabe des Werkes abzusehen. (Enthaltungspflicht, Vermeidung von Mehrfachmeldung bei der VG Wort). Ferner sollte gegebenenfalls die Erstellung der gesamten oder von Teilen der Auflage in einem Print-on-Demand-Verfahren verbindlich geregelt werden.

Im Falle einer vollwertigen Print-Publikation (ISBN-Vergabe, Vertrieb über den Buchhandel) sollten zwischen Autoren/Herausgebern und den Hoch-

schulen/Hochschulverlagen rechtswirksame Verträge geschlossen werden, in denen u.a. Fragen des Nutzungs- und Verwertungsrechtes eindeutig geklärt sind.

## **4.5 Sicherheit, Authentizität und Integrität**

### **4.5.1 Server**

In der Dokumentation des technischen Systems müssen das eingesetzte System beschrieben und die Verantwortlichen (Administratoren) genannt werden. Die Dokumentation ist stets aktuell zu halten. Datum und Autor der letzten Änderung sind jeweils zu vermerken.

Zu allen eingesetzten Komponenten müssen die genaue Bezeichnung und der Hersteller genannt werden. Hardwarekomponenten sind mit den jeweils relevanten technischen Parametern (Geschwindigkeit, Speichergröße etc.) zu beschreiben. Bei Softwarekomponenten sind die Versionsnummern anzugeben.

#### **Zugangsregelung zum Server:**

Es ist anzugeben,

- welcher Personenkreis räumlichen Zugang zum Server hat,
- wer sich in das System einloggen kann, wobei zwischen Administrator- und Benutzerrechten und ggf. weiteren Berechtigungsstufen zu unterscheiden ist,
- wer für das System verantwortlich und wie die Vertretung geregelt ist,
- wo das Administratorpasswort hinterlegt ist.

#### **Regelung der Wartung des Systems:**

Wer ist für die routinemäßige Wartung des Systems verantwortlich? Wie und in welcher Zeit erfolgt die Reaktion auf Störungen des Betriebs?

#### **Sicherung und Wiederherstellung:**

Die Sicherung ist täglich durchzuführen und so zu gestalten, dass daraus ein komplett ausgefallenes System ohne Daten- und Funktionsverlust wiederhergestellt werden kann. Die Nutzung eines zentralen und automatisch ablaufenden Backupservice ist anzustreben.

#### **Verlässliche Installation des Systems und der Software-Komponenten:**

Für einen sicheren Betrieb darf ein System nur aus erprobten und stabilen Komponenten bestehen, über die keine Konflikte in der Zusammenarbeit bekannt sind. Für den Betrieb eines Dokumentenservers nicht erforderliche Dienste und Programmpakete sind zu deaktivieren oder zu deinstallieren. Es sind Produkte zu bevorzugen, zu denen die Hersteller Aktualisierungsdienste anbieten.

### **Regelmäßige Wartung des Systems:**

Ein Administrator muss für die Wartung des Systems zuständig sein und regelmäßig einen festen Teil seiner Arbeitszeit dafür zur Verfügung haben. Die Wartung umfasst insbesondere das Einspielen von Sicherheitsupdates aber auch die Aktualisierung von Einzelkomponenten und die Reaktion auf Störungen.

### **Kontrollierte und nachweisbare Aufnahme von Dokumenten aus technischer Sicht:**

Der kontrollierte Zugang von Dokumenten stellt sicher, dass nur Dokumente auf den Server gelangen, die den Kriterien der Richtlinien des Dokumentenservers entsprechen. Die Realisierung entsprechender Geschäftsgänge liegt in der Verantwortung des Betreibers. Die Geschäftsgänge müssen so gestaltet sein, dass der Zugang der Dokumente technisch überprüfbar ist.

### **SSL-Zertifizierung:**

Eine SSL-Zertifizierung des Servers ist die Voraussetzung, um die Authentizität der Dokumente für den Leser sicherzustellen. Die Zertifizierung muss über eine autorisierte Zertifizierungsstelle (Certification Authority, CA) erfolgen. Die Integrität der Dokumente wird durch digitale Signaturen gewährleistet.

### **Aufteilung der Dokumentation:**

Die Dokumentation sollte aus einem veröffentlichten, frei zugänglichen und einen internen Teil, der sicherheitssensible Informationen enthalten kann, bestehen.

### **Autonome Überwachungs- und Alarmfunktion:**

Ein derartiges System überwacht permanent den Betrieb des Servers im Ganzen sowie einzelner Dienste (Webseiten, Datenbankfunktionen etc.). Bei Ausfall des Servers oder einzelner Komponenten erfolgen Alarmierungen per E-Mail oder SMS<sup>27</sup>.

### **Havarieszenarien:**

Für jeden Schweregrad einer Havarie, vom Ausfall einzelner Soft- oder Hardwarekomponenten bis zum Totalausfall des Servers, sollten Handlungsanweisungen bereit liegen, mittels derer der Betrieb des reparierten oder ggf. neu installierten Systems in kürzest möglicher Zeit wieder aufgenommen werden kann. Havarien umfassen sowohl technische Ausfälle als auch Beschädigungen etwa durch Fehlbedienungen oder Angriffe von außen (Hacker).

---

<sup>27</sup> Beispiel: Nagios ([www.nagios.org](http://www.nagios.org))

## 4.5.2 Dokumente

### Persistent Identifier

Jedes Dokument muss einen Persistent Identifier erhalten. Als mögliche Realisierung bietet sich die URN-Vergabe an.

Die Dokumentspeicherung kann mittels eines Dokumentenmanagementsystems (Datenreplikation, Datensicherung) erfolgen, das die Verwaltung, Speicherung und Archivierung von digitalen Ressourcen über deren gesamten Lebenszyklus hinweg organisiert. Der Zugriff auf diese Ressourcen muss langfristig gewährleistet sein. Dies wird durch die Anwendung von eindeutigen, standortunabhängigen Identifizierungssystemen (Persistent Identifiers, PI) sichergestellt. Darüber hinaus können Persistent Identifiers als Unterstützung beim Harvesting (Ingest) genutzt werden. PIs eignen sich zur Workflow-Steuerung, wenn eine eindeutige Identifizierung der Objekte erforderlich ist wie z. B. bei dezentralen Geschäftsprozessen, für Dubletten-Checks, Authentifizierungsmechanismen, Alarmsysteme, oder Multimedia- oder modular aufgebaute Ressourcen. Verteilt gespeicherte Dokumente können durch PIs effektiv zusammengeführt werden. Bei modular aufgebauten Dokumenten erfolgt durch die Identifizierung eines bestimmten Teils eine selektive Zusammenführung der gewünschten Version, ohne diese Version extra speichern zu müssen. Digitale Objekte können in einer digitalen oder nicht-digitalen Umgebung mit Hilfe von PIs zuverlässig zitiert werden.

Damit ein Persistent Identifier nutzbar ist, muss das Schema des Identifikators als auch sein Namensraum bekannt sein. Der Persistent Identifier muss innerhalb dieses Namensraumes und Schemas (ein-)eindeutig sein. Beides sollte offengelegt, dokumentiert und in einem Persistent Identifier Registry wie z. B. dem IANA Registry für URN-Namensräume registriert sein. Für den genutzten Persistent Identifier muss ein Resolving-Dienst existieren.

Das Schema der Persistent Identifiers sollte den in RFC 1737<sup>28</sup> formulierten Anforderungen gerecht werden.

Der Persistent Identifier muss mit seinem Typ (Schema) und dem eindeutigen Wert für das betreffende Objekt in den Metadaten verankert sein. Referenzen auf über- bzw. untergeordnete Objekte sollten mit demselben Persistent-Identifier-Schema abgebildet werden.

Persistent Identifiers sind im Bereich der Bibliotheken z. B. National Bibliography Number (NBN), ein Unterraum der URNs (Uniform Resource Names), im Bereich

---

<sup>28</sup> <http://rfc.net/rfc1737.html>

der Verlage und zunehmend auch bei Rohdaten Digital Object Identifier (DOI), des weiteren: Persistent URL (PURL), Handle, Archival Resource Key (ARK) etc.

### Beispiele

1. urn:nbn Beispiel:

**urn:nbn:de:bsz:93-opus-15563**

2. DOI Beispiel ohne Metadatenyntax:

**DOI: 10.1045/april2004-dobratz**

3. Handle Beispiel (D-Space System):

**URI: <http://hdl.handle.net/1721.1/30592>**

Weitere Informationen zu verwendbaren Systemen findet man unter:

- NBNs: Homepage des Projektes EPICUR:  
<http://www.persistent-identifizier.de/>
- Allgemeine Anforderungen an URNs:  
<ftp://ftp.rfc-editor.org/in-notes/rfc1737.txt>
- Registrierung von Unternehmensräumen: IANA Registry:  
<http://www.iana.org/assignments/urn-namespaces>
- Digital Object Identifier homepage: <http://www.doi.org/>
- Handle-System homepage: <http://www.handle.net/>
- URI: <http://info-uri.info/>
- PURL: <http://purl.oclc.org/>

### Hash-Verfahren

Um die Unversehrtheit des Dokuments gegenüber dem Leser zu gewährleisten, muss zumindest ein Hash-Wert für jedes Dokument existieren. Da sich die Sicherheitsanforderungen durch die Weiterentwicklung der Kryptographie ändern, müssen die Algorithmen entsprechend angepasst werden. Zur Zeit empfiehlt sich der Einsatz des MD5-Message-Digest-Algorithmus oder des Secure-Hash-Algorithmus (SHA-1). Der Einsatz sollte für den Leser dokumentiert werden. Die folgenden Beispiele sind der Informationsseite des Dokumentenservers der Universität Chemnitz „MONARCH“ entnommen.<sup>29</sup>

Die in MONARCH archivierten Publikationen werden mittels verschiedener Hash-Verfahren und digitaler Signatur gesichert. Zum Grundprinzip des Sicherheitssystems gehören:

- Für jede Publikation im MONARCH existiert eine sogenannte Hash-Datei.

---

<sup>29</sup> <http://archiv.tu-chemnitz.de/integrity.html>

- Für jede Datei einer Publikation werden drei verschiedene Hash-Werte berechnet und in dieser Hash-Datei gespeichert.
- Die Hash-Datei wird außerdem durch den Archivar digital signiert.
- Mit Hilfe der Hash-Werte kann jederzeit überprüft werden, ob die Publikation verändert wurde. Die Signatur der Hash-Datei garantiert weiterhin, dass die Hash-Werte seit Erstellung der Hash-Datei durch den Archivar unverändert sind.

Verwendete Hash-Verfahren:

- Secure Hash Algorithmus (SHA)
- MD5-Message-Digest-Algorithmus
- RIPE-MD-Algorithmus

Signieren der Hash-Datei:

- Die Hash-Datei wird durch den Archivar digital signiert.
- Zum Signieren der Hash-Datei wird das Programm PGP (Pretty Good Privacy) Version 2.6.3 verwendet.<sup>30</sup>

Jede inhaltliche Veränderung des Dokuments führt zu einem neuen Dokument. Dieses neue Dokument erhält auch einen neuen Persistent Identifier. Durch eine Versionsnummerierung kann auf die vorherige Version des Dokuments hingewiesen werden. Diese Versionierung sollte in den Metadaten verzeichnet sein, um zwischen den Generationen eines Dokuments Verknüpfungen herzustellen.

## Digitale Signatur

Das Signaturgesetz unterscheidet zwischen den folgenden Signaturstufen. Im Sinne dieses Gesetzes sind:

1. „elektronische Signaturen“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,
2. „fortgeschrittene elektronische Signaturen“ elektronische Signaturen nach Nummer 1, die
  - ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
  - die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
  - mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
  - mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,

---

<sup>30</sup> <http://www.pgpi.org/>

3. „qualifizierte elektronische Signaturen“ fortgeschrittene elektronische Signaturen nach Nummer 2, die
  - auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
  - mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Wir empfehlen, mindestens die „fortgeschrittene elektronische Signatur“ einzusetzen. Um die Langzeitarchivierung zu erleichtern, ist es ratsam, dass schon die annehmende Institution ein Archivierungsformat aus den eingereichten Originaldateien erzeugt.

Hier sollte der Anbieter der Dokumenten- und Publikationsservices eine Übereinkunft mit dem Betreiber eines Archivservers schließen. Konkrete Empfehlungen zu Archivierungsformaten existieren bisher nicht. Die Dokumente auf dem Dokumentenserver sollten in einem gängigen Präsentationsformat angeboten werden. Das zur Zeit gängigste Format ist das PDF-Format. Wird ein anderes Format genutzt, so sollte entweder eine Viewer-Software zum Herunterladen angeboten oder eine Internet-Adresse für diese angegeben werden.

## **4.6 Erschließung**

### **4.6.1 Sacherschließung**

Es muss eine schriftlich fixierte Strategie (Policy) zur sachlichen Erschließung der Dokumente vorhanden sein. Freie Schlagworte sind langfristig nicht ausreichend, um gute Suchergebnisse bezüglich Precision und Recall zu gewährleisten.

Um einheitliche inhaltliche Suchen über mehrere Dokumentenserver hinweg zu ermöglichen, sollten internationale Erschließungssysteme gemäß den DINI-OAI-Empfehlungen benutzt werden.

### **4.6.2 Metadatenexport und Schnittstellen**

Zur internen Datenstruktur der Dokumentenserver werden bewusst keine Empfehlungen gegeben, es sollten jedoch standardisierte Metadaten ausgegeben und ausgetauscht werden können.

Zur Archivierung und Sicherung der Langzeitverfügbarkeit sind die elektronischen Ressourcen mit standardisierten administrativen und technischen Metadaten zu versehen. Hierauf zielen die empfohlenen Standards wie z.B. PREMIS oder LMER ab (s. 2.6.2). Entwicklungen im Rahmen nationaler und internationaler Bestrebungen zur Verbesserung der Langzeitverfügbarkeit digitaler Dokumente sind hierbei zu berücksichtigen. Derzeit können keine konkreten Schnittstellen zu Langzeitarchivierungssystemen benannt werden.

## 4.7 Zugriffsstatistik

In den Dokumentenserver integrierte dokumentbezogene Zugriffsstatistiken können relativ zu anderen Dokumenten ein Indiz für inhaltliche Relevanz darstellen. Serverbezogene Zugriffsstatistiken können sowohl qualitativ/quantitativ als auch technologisch die Basis für die Bewertung eines Dokumentenservers sein. Weiterhin kann der zeitliche Verlauf einer dokumentspezifischen Zugriffsstatistik über den gesamten Zeitraum der Existenz des Dokuments ein Indiz für dessen andauernde Relevanz sein. Um eine Vergleichbarkeit der Statistiken verschiedener Dokument- und Publikationsservices zu ermöglichen, müssen Standards bestehen und eingehalten werden. Entsprechende Standards für Zugriffsstatistiken institutioneller Dokumentenserver existieren zurzeit jedoch nicht. Probleme bei der Erfassung und Auswertung von Statistiken entstehen z. B. durch unterschiedliche Protokolle wie auch Zugriffstechnologien. Somit existiert aktuell keine Basis zur vergleichenden Bewertung von Dokumenten unterschiedlicher Dokumentenserver wie auch der Services selbst. Es wird empfohlen, die Zugriffsstatistik mindestens 5 Jahre aufzubewahren.

DINI beobachtet die internationalen Entwicklungen wie z. B. das Standardisierungsprojekt COUNTER („Counting Online Usage of Networked Electronic Resources“)<sup>31</sup> und das Anwendungsprojekt Interoperable Repository Statistics (IRS)<sup>32</sup> und wird gegebenenfalls neue Empfehlungen geben. Alternative Ansätze wie die Auswertung von Linkresolver-Logs werden ebenfalls verfolgt werden<sup>33</sup>.

## 4.8 Langzeitverfügbarkeit

Während einer Frist, die fünf Jahre ab Veröffentlichung auf dem Server nicht unterschreiten darf und in der Policy festgeschrieben ist, hat der Anbieter des Service gemäß den Anforderungen im Abschnitt 2.5 eigenständig die Verfügbarkeit der Dokumente zu gewährleisten. Gleichzeitig muss die Langzeitverfügbarkeit dieser elektronischen Ressourcen sichergestellt werden. Dies sollte durch Beachtung der jeweils aktuellen Empfehlungen des Kompetenznetzwerkes nestor<sup>34</sup> erfolgen. Im

---

<sup>31</sup> <http://www.projectcounter.org/>

<sup>32</sup> <http://irs.eprints.org/>

<sup>33</sup> <http://www.dini.de/veranstaltung/workshop/oaimpact/presentations/bollen.ppt>

<sup>34</sup> Aktuelle Informationen zu geeigneten Maßnahmen zur Sicherstellung der Langzeitverfügbarkeit sowie Detailinformationen und Werkzeuge findet man über die Website des nestor Kompetenznetzwerks Langzeitarchivierung und Langzeitverfügbarkeit digitaler Ressourcen für Deutschland <http://www.langzeitarchivierung.de>

Rahmen ihrer technischen und finanziellen Möglichkeiten kann eine Institution dies selbst gewährleisten (Depotsystem nach OAIS). Alternativ kann unter Beachtung der jeweiligen Anforderungen (siehe Abschnitt 2.6) zur Übergabe der Ressourcen und der zur Archivierung und Nutzung nötigen Metadaten der Aufbau von administrativen und organisatorischen Strukturen zur externen Archivierung in Zusammenarbeit mit Archivierungsinstitutionen erfolgen.

Gegenwärtig sind durch das Kompetenznetzwerk nestor keine konkreten Empfehlungen zu Archivierungsformaten veröffentlicht, aber die benutzten Dateiformate sollten offen beschrieben sein, damit sie zur Langzeitarchivierung geeignet sind. Der zertifizierte Service muss die Dokumente selbst dauerhaft archivieren oder dazu weiterreichen können. Um die Langzeitverfügbarkeit sicherzustellen, müssen die Originaldokumente selbst oder eine erstellte Archivkopie in einem offenen Format archiviert werden. Die archivierten vom Autor gelieferten Originaldateien entsprechen nicht notwendigerweise den Archivkopien. Offene Formate sind solche, die auch in ferner Zukunft sicher lesbar sind, weil ihre Quellcodes offen gelegt sind (als DIN/ISO oder OASIS) und auf alle Zeiten die Entwicklungserlaubnis für jeden gegeben ist. Dies sind zum Beispiel die Formate Open Document Format (ODF), ASCII-Text (TXT), Hypertext Markup Language (HTML), Portable Document Format für Langzeitarchivierung (PDF/A) und TeX/LaTeX (TEX). Eindeutige Benennungen der jeweiligen Dateiformate, die über den MIME-Type hinausgehen, sind wichtig für die Wahl nötiger Erhaltungsstrategien. Besonders hilfreich sind Referenzen zu öffentlich verfügbaren Datenbanken mit Formatbeschreibungen, sog. File Format Registries. Zusätzliche technische Metadaten (Informationen zu Kodierungen, Farbtiefe von Bildern, etc.) erleichtern die spätere Anwendung von Langzeitarchivierungsverfahren wie Migration oder Emulation. Diese Metadaten können mit automatisch arbeitenden Tools wie JHOVE erstellt werden. Diese technischen Metadaten sollten zusammen mit Informationen zu ggf. erfolgten Migrationen und weiteren Metadaten dem eigentlichen Objekt bei einem Export mitgegeben werden. Für eine strukturierte Form eignen sich dazu spezielle Paketformate, die z. B. auf METS<sup>35</sup> basieren, wie etwa das Universelle Objektformat (UOF). Kopierschutzmaßnahmen, wie sie beim Digital Rights Management (DRM) Anwendung finden, sind dann für Archivexemplare völlig ungeeignet, wenn sie Konvertierungen (Migration) und die Ausführung in anderen Systemumgebungen (Emulation) ausschließen.

---

<sup>35</sup> <http://www.loc.gov/standards/mets/>

## Autoren dieses Dokumentes

Nachname	Institution	E-Mail
Margo Bargheer	Niedersächsische Staats- und Universitätsbibliothek Göttingen	bargheer@sub.uni-goettingen.de
Kim Braun	Carl von Ossietzky Universität Oldenburg, Informations-, Bibliotheks- und IT-Dienste	braun@bis.uni-oldenburg.de
Susanne Dobratz	Humboldt-Universität zu Berlin, AG Elektronisches Publizieren, Universitätsbibliothek	dobratz@cms.hu-berlin.de
Dr. Stefan Gradmann	RRZ der Universität Hamburg	stefan.gradmann@rrz.uni-hamburg.de
Prof. Dr. Eberhard Hilf	Universität Oldenburg, Institute for Science and Networking	hilfe@physnet.physik.uni-oldenburg.de
Dr. Wolfram Horstmann	Niedersächsische Staats- und Universitätsbibliothek Göttingen	horstmann@sub.uni-goettingen.de
Prof. Dr. Elmar Mittler	Niedersächsische Staats- und Universitätsbibliothek Göttingen	mittler@sub.uni-goettingen.de
Prof. Dr. Peter Schirnbacher	Humboldt-Universität zu Berlin, Computer- und Medienservice	schirnbacher@cms.hu-berlin.de
Frank Scholze	Universität Stuttgart, Universitätsbibliothek	scholze@ub.uni-stuttgart.de

Dr. Silke Schomburg	Hochschulbibliothekszenrum des Landes Nordrhein-Westfalen	schomburg@hbz-nrw.de
Thomas Severiens	Universität Osnabrück, Fachbereich Mathematik/Informatik	Severiens@Mathematik.Uni-Osnabrueck.de
Dr. Heinrich Stamerjohanns	International University Bremen	h.stamerjohanns@iu-bremen.de
Tobias Steinke	Deutsche Nationalbibliothek	t.steinke@d-nb.de
Bert Wendland	Humboldt-Universität zu Berlin, AG Elektronisches Publizieren, Computer- und Medienservice	bwendland@cms.hu-berlin.de
Christoph Ziegler	Technische Universität Chemnitz, Rechenzentrum	christoph.ziegler@hrz.tu-chemnitz.de

# Aufnahmeantrag für die Mitgliedschaft in DINI e.V.

(auch online unter <http://www.dini.de/dini/mitgliedschaft/mitgliedschaft.php>)

## Angaben zum Antragsteller:

Name:

Vorname:

Sind Sie Bevollmächtigte/r der antragstellenden Institution?  Ja  Nein

Institution:

URL der Institution:

## Die antragstellende Institution ist Mitglied in:

AMH  dbv  ZKI  Fachgesellschaften und Sonstige

## Anzahl der Beschäftigtenvollzeitäquivalenz (BVZÄ):

## Weitere Angaben (entweder zu Ihrer Person oder der Institution):

Anschrift (Straße, Nummer):

PLZ, Ort:

Telefon:

Fax:

E-Mail-Adresse:

## Wer soll Mitglied werden

Hochschule  Institution  Fachgesellschaft  Sie selbst

## Welche Art der Mitgliedschaft wünschen Sie?

Zur Definition der Mitgliedschaft siehe Satzung § 3

Ordentliches Mitglied  Assoziiertes Mitglied

## Bemerkungen

---

Ort, Datum

---

Unterschrift





[Version 2.0, September 2006]

## **Impressum**

DINI – Deutsche Initiative für Netzwerkinformation e.V.

– Geschäftsstelle –

c/o Niedersächsische Staats- und Universitätsbibliothek Göttingen

Papendiek 14

37073 Göttingen

Tel.: 0551-39-38 66

Fax: 0551-39-38 56

E-Mail: [gs@dini.de](mailto:gs@dini.de)

[www.dini.de](http://www.dini.de)