Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft

Band 73

Digitale Archivierung von Abschlussarbeiten – eine Analyse mit Handlungsempfehlungen für den Dokumentenserver PubLIS Cologne

Theresa Vogt

März 2014

Fachhochschule Köln

Fakultät für Informations- und Kommunikationswissenschaften

Institut für Informationswissenschaft

Entstanden als Bachelorthesis im Studiengang Bibliothekswesen

Betreuerin: Prof. Dr. Selma Strahringer

Vogt, Theresa
Digitale Archivierung von Abschlussarbeiten – eine Analyse mit Handlungsempfehlungen für den Dokumentenserver PubLIS Cologne.
Köln: Fachhochschule Köln,
Fakultät für Informations- und Kommunikationswissenschaften,
Institut für Informationswissenschaft, 2014
(Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft; 73)

ISSN (elektronische Version) 1434-1115

Die Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft berichten über aktuelle Forschungsergebnisse des Instituts Informationswissenschaft der Fachhochschule Köln. Veröffentlicht werden sowohl Arbeiten der Dozentinnen und Dozenten als auch herausragende Arbeiten der Studierenden. Die Kontrolle der wissenschaftlichen Qualität der Veröffentlichungen liegt bei der Schriftleitung.
Jeder Band erscheint in elektronischer Version (über unsere Homepage: http://www.fbi.fh-koeln.de/institut/papers/arbeitspapiere.php).

Fachhochschule Köln
Fakultät für Informations- und Kommunikationswissenschaften
Institut für Informationswissenschaft
Claudiusstr.1 D-50678 Köln
Tel.: 0221/8275-3376, Fax: 0221/3318583
E-Mail: schriftenreihe@fbi.fh-koeln.de

Schriftleitung: Prof. Dr. Hermann Rösch, Susanne Röltgen

ABSTRACT (DEUTSCH)

Seit Mitte des Jahres 2012 werden alle Abschlussarbeiten der Studierenden des Instituts für Informationswissenschaft an der Fachhochschule Köln auf dem Dokumentenserver PubLIS Cologne abgelegt. Um den Zugriff auf das Originaldokument zu gewährleisten, wird zusätzlich ein gedrucktes Archivexemplar aufbewahrt. Die Frage ob eine ausschließlich elektronische Speicherung der Abschlussarbeiten prüfungsrechtlich ausreichend sein kann, wird in der vorliegenden Bachelorarbeit behandelt. Hierzu werden zunächst Kriterien vorgestellt, welche die organisatorischen und technischen Voraussetzungen für die ausschließlich digitale Aufbewahrung festlegen. Zudem wird die rechtliche Lage von Abschlussarbeiten dargelegt sowie der Dokumentenserver vorgestellt. Als Hauptteil der Arbeit werden aufbauend auf die vorgestellten Kriterien konkrete Handlungsempfehlungen für das Repositorium PubLIS Cologne gegeben. Diese beziehen sich auf das Vorgehen bei Verwaltung und Organisation am Institut für Informationswissenschaft sowie auf technische Verfahrensweisen zur Erhaltung von Integrität und Authentizität im Dokumentenbestand. Besondere Beachtung findet dabei die Vergabe von digitalen Signaturen in Verbindung mit Hashwerten. Zusammenfassend wird festgestellt, dass es durchaus vielversprechende Potentiale und Möglichkeiten zur sicheren Umsetzung gibt. Es fehlen jedoch konkret hochschul- und allgemeinrechtliche Vorschriften mit Bezug zu Abschlussarbeiten. Allgemein kann davon ausgegangen werden, dass diese Art der Archivierung im zunehmend von digitalen Prozessen geprägten Hochschulalltag an Bedeutung gewinnen wird.

ABSTRACT (ENGLISCH)

Since 2012 the Institute of Information Science at the University of Applied Sciences Cologne runs its own repository named PubLIS Cologne. All of the theses, which are handed in at the institute, are saved on this repository. In addition a printed copy of each thesis is saved. The present paper examines the question if it is possible, regarding the examination rules, to keep only the digital document. To clear this issue, relevant criteria are summed up and the legal situation of digital documents in companies is explained. Afterwards the organization of the repository at the Institute of Information Science and the technical aspects of the hosting are presented. The main part of the paper contains concrete suggestions to optimize the organization. Besides technical methods to save the authenticity and integrity of the documents are pointed out and the potential use for PubLIS Cologne is explained. Concerning these goals digital signatures and hash functions are important technics. In summary it is to be said, that possibilities for a reliable realization exist. Nevertheless concrete laws, in general and concerning universities, are missing. Regarding the increasing importance of digital processes in universities this subject offers great potentials.

Schlagwörter: Dokumentenserver, Repositorium, digitale Archivierung, revisionssichere Archivierung

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

AO	Abgabenordnung
BGB	Bürgerliches Gesetzbuch
BPO	Bachelorprüfungsordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSZ	Bibliotheksservice-Zentrum Baden-Württemberg
CA	Certification Authority
DIN	Deutsches Institut für Normung e. V.
DINI	Deutsche Initiative für Netzwerkinformation e. V.
DNB	Deutsche Nationalbibliothek
GoBIT	Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
HBZ	Hochschulbibliothekszentrum des Landes Nordrhein-Westfalen
HGB	Handelsgesetzbuch
IKS	Internes Kontrollsystem
ISO	International Organization for Standardization
KOBV	Kooperativer Bibliotheksverbund Berlin-Brandenburg
MARE	Museen, Archive und Repositorien
MD	Message Digest
NBN	National Bibliography Number
Nestor	Network of Expertise in Long-Term Storage of Digital Resources
NID	Namespace
NISS	Namespace Specific String
OAIS	Offenes Archiv-Informations-System
PAdES	PDF Advanced Electronic Signatures
PDF	Portable Document Format
PDF/A	PDF/Archivierung
PIN	persönliche Identifikationsnummer

SHA	Secure Hash Algorithm
SigG	Signaturgesetz
SNID	Subnamespace
URL	Uniform Resource Locator
URN	Uniform Resource Name
USV	unterbrechungsfreie Stromversorgung
XMP	Extensible Metadate Platform
ZPO	Zivilprozessordnung

1 EINLEITUNG

Seit Mitte des Jahres 2012 werden alle Abschlussarbeiten der Studierenden des Instituts für Informationswissenschaft an der Fachhochschule Köln auf dem Dokumentenserver PubLIS Cologne abgelegt. Zusätzlich wird ein gedrucktes Archivexemplar aufbewahrt, um den Zugriff auf das Originaldokument für die in der Archivordnung vorgeschriebenen fünf Jahre zu gewährleisten. Nun werden Überlegungen angestellt, ob eine ausschließlich elektronische Speicherung der Bachelor-, Master- sowie Diplomarbeiten prüfungsrechtlich ausreichend sein kann. Diese Fragestellung wird in der vorliegenden Arbeit untersucht.

Eine Antwort auf die grundsätzliche Frage, ob die ausschließliche elektronische Speicherung von Prüfungsunterlagen rechtskonform und eventuellen späteren Rechtsstreitigkeiten gewachsen ist, ist sehr schwer zu geben, da es sich bei diesem Thema um eine juristische Grauzone handelt. Als Orientierung werden deshalb verwandte Themen, wie z. B. Aufbewahrung von digitalen Geschäftsdokumenten in Unternehmen, dienen.

Dabei wäre mit der Aufklärung dieser Frage für viele Hochschulen eine attraktive Alternative zur umständlichen und platzraubenden Archivierung der Printexemplare geboten. Gerade da eine Vielzahl von Hochschulen bzw. Hochschulbibliotheken bereits eigene Repositorien betreibt. Zusätzlich bietet die elektronische Speicherung die Möglichkeit durch Recherche der Metadaten und unter Umständen sogar des Volltextes wesentlich schneller einen direkten Zugriff auf die Abschlussarbeiten zu erhalten.

Zur Klärung des Sachverhalts werden zunächst organisatorische, rechtliche und technische Voraussetzungen eines vertrauenswürdigen, digitalen Langzeitarchivs anhand ausgewählter Kriterien erläutert. Hierzu werden die DIN-Norm 31644, der Kriterienkatalog vertrauenswürdige digitale Langzeitarchive des Nestor-Kompetenznetzwerks und das DINI-Zertifikat 2010 herangezogen. Danach folgt eine Analyse des Repositoriums PubLIS Cologne, wobei die Organisation am Institut für Informationswissenschaft ausführlich erläutert wird. Ergänzend wird das Bibliotheksservicezentrum Baden-Württemberg vorgestellt, da dort das Institutsrepositorium gehostet wird und dieses demnach für die technischen Vorkehrungen bei der Archivierung verantwortlich ist.

Den Hauptteil der Arbeit bilden konkrete Handlungsempfehlungen, wie das Konzept der ausschließlichen digitalen Speicherung umgesetzt werden kann. Zudem sollen sie zur Verbesserung von Qualität und Vertrauenswürdigkeit des Repositoriums[1] beitragen. Hierzu zählen Maßnahmen, die die Organisation von PubLIS Cologne am Institut für Informationswissenschaft direkt betreffen, also Finanzierung, Personalbedarf und Arbeitsabläufe bei der Speicherung der Dokumente. Der zweite Aspekt umfasst die technischen Lösungen, um Integrität, Authentizität und Vertraulichkeit der studentischen Arbeitsergebnisse dauerhaft zu gewährleisten. Zudem werden Anpassungen von hochschulinternen Vorschriften, wie z. B. Prüfungsordnungen, vorgeschlagen, um diese dem Ziel der digitalen Archivierung entsprechend zu gestalten.

Es werden unterschiedliche Möglichkeiten zum Erreichen des Ziels der revisionssicheren digitalen Archivierung vorgestellt sowie begründete Empfehlungen speziell für den Dokumentenserver am Institut für Informationswissenschaft gegeben.

Die folgenden Ausführungen sollen den zuständigen Mitarbeitern[2] am Institut für Informationswissenschaft zum Erkenntnisgewinn und als Orientierungshilfe bei der Bewertung und Weiterführung von PubLIS Cologne dienen. Im besten Falle kann es gelingen eine fachliche Diskussion zum Thema digitaler Aufbewahrung von Prüfungsunterlagen anzustoßen.

---

[1] Die Begriffe Dokumentenserver und Repositorium werden im Folgenden synonym verwendet.

[2] Der Einfachheit halber wird in dieser Arbeit nur die männliche Form verwendet.

2 ALLGEMEINE ANFORDERUNGEN AN DIE DIGITALE ARCHIVIERUNG VON ABSCHLUSS-ARBEITEN

Im ersten Abschnitt der Arbeit werden Anforderungen an die digitale Archivierung von Dokumenten im Allgemeinen und von Abschlussarbeiten im Speziellen vorgestellt. Hierzu werden relevante Kriterien aus dem technischen und organisatorischen Bereich aus drei unterschiedlichen Quellen herausgearbeitet und zusammengefasst. Eine Vorstellung der Veröffentlichungen ist ebenso Teil der Ausführungen. Anschließend werden die rechtlichen Aspekte der digitalen Speicherung von Abschlussarbeiten beleuchtet. Da es hierfür keine expliziten Vorschriften gibt, wird Bezug auf die geltende Rechtslage von elektronischen Geschäftsdokumenten genommen. Empfehlungen, wie diese Kriterien beim Betrieb des Dokumentenservers PubLIS Cologne umgesetzt werden können, werden später in Kapitel 4 gegeben.

2.1 Kriterien zur Bewertung von Repositorien

Im folgenden Kapitel werden die DIN-Norm 31644, der Nestor-Kriterienkatalog und das DINI-Zertifikat 2010 vorgestellt. Sie nennen Kriterien für die Bewertung von Langzeitarchiven oder Publikationsservern.

Die genannte Veröffentlichung des Kompetenznetzwerks Nestor und die DIN-Norm 31644 beziehen sich in ihren Ausführungen auf den Standard des Offenen Archiv-Informations-Systems (OAIS). Dieser Standard stellt die Grundkonzepte für die Organisation eines Langzeitarchivs dar. Hierbei werden die konkreten Informationsobjekte mit den zugehörigen Metadaten zu einem Informationspaket zusammengefasst. Diese Pakete werden wiederum in Form eines Übergabeinformationspakets in das Langzeitarchiv aufgenommen und dort als Archivinformationspaket abgelegt. Schließlich werden die Inhalte bei Bedarf an die jeweiligen Bedürfnisse des Endnutzers angepasst und in Form eines Auslieferungsinformationspakets ausgegeben.[3]

Das OAIS-Modell spielt besonders im Bereich der Langzeitarchivierung eine tragende Rolle. Da sich die vorliegende Arbeit jedoch nicht mit den Methoden der Langzeitarchivierung beschäftigt, soll diese kurze Erläuterung lediglich zum Verständnis der folgenden Kriterien dienen. Es wird jedoch nicht auf das OAIS-Prinzip im Speziellen eingegangen.

2.1.1 DIN-Norm 31644: Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive

In der DIN-Norm 31644 werden generelle Anforderungen an den Aufbau und die Organisation eines vertrauenswürdigen digitalen Langzeitarchivs formuliert. Es werden Kriterien entwickelt, die zur Beurteilung der Langzeitarchive herangezogen werden können, wobei technische und organisatorische Gesichtspunkte berücksichtigt werden.[4] Das

[3] Vgl. Nestor – Kompetenznetzwerk Langzeitarchivierung/Arbeitsgruppe OAIS-Übersetzung/Terminologie: Referenzmodell für ein Offenes Archiv-Informations-System (2012), S. 21–24

[4] Vgl. Norm DIN 31644, S. 4–5

Dokument wurde im Auftrag des Deutschen Instituts für Normung (DIN) vom Arbeitskreis Vertrauenswürdige digitale Archive erstellt und im April 2012 veröffentlicht.[5]

2.1.2 Nestor-Kriterien – Kriterienkatalog vertrauenswürdige digitale Langzeitarchive

Das Network of Expertise in Long-Term Storage of Digital Resources[6], kurz Nestor, ist ein Kompetenznetzwerk, in welchem Gedächtnisorganisationen und Spezialisten zum Thema Langzeitverfügbarkeit und -archivierung zusammenarbeiten und forschen.[7] Diese Organisation veröffentlichte 2008 den Kriterienkatalog vertrauenswürdige digitale Langzeitarchive. Als Grundlage für diese Kriteriensammlung dienten unterschiedliche nationale und internationale Berichte, u. a. auch das DINI-Zertifikat für Dokumenten- und Publikationsserver aus dem Jahr 2007.[8] Wie aus dem Titel deutlich hervorgeht, bezieht sich die Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung in ihrer Veröffentlichung auf die Bewertung von digitalen Langzeitarchiven und berücksichtigt dabei insbesondere die Aspekte Organisation, Verwaltung der Informationsobjekte und IT-Infrastruktur.

Erstaunlicherweise stimmen die DIN-Norm 31644 und der Nestor-Kriterienkatalog stellenweise wortwörtlich überein, sodass in den folgenden Kapiteln oft auf Textpassagen in beiden Dokumenten verwiesen wird. Es finden sich jedoch in keiner der beiden Abhandlungen Hinweise darauf, welche Veröffentlichung Inhalte von der anderen übernommen hat.

2.1.3 DINI-Zertifikat – Dokumenten- und Publikationsservice 2010

Die Kriterien zur Erlangung des DINI-Zertifikats wurden innerhalb der Deutschen Initiative für Netzwerkinformation e. V. (DINI) von der Arbeitsgruppe Elektronisches Publizieren erarbeitet. Der Text entspricht im Wesentlichen dem Fragebogen, welcher als Grundlage für die Vergabe des DINI-Zertifikats an Dokumenten- und Publikationsservices dient. Nach den Veröffentlichungen aus den Jahren 2004 und 2007 liegt das Zertifikat nun in der dritten Auflage vor. Es werden Mindestanforderungen in technischer, organisatorischer und rechtlicher Hinsicht genannt sowie weiterführende Empfehlungen gegeben.[9] Im Gegensatz zu den beiden anderen aufgeführten Kriterienkatalogen bezieht sich das DINI-Zertifikat nicht auf die Bewertung digitaler Langzeitarchive sondern auf Dokumenten- und Publikationsservices.[10]

---

[5] Vgl. ebd., S. 2

[6] Vgl. Deutsche Nationalbibliothek: Projects – NESTOR – Network of Expertise in Long-term Storage of Digital Resources (2013)

[7] Vgl. Deutsche Nationalbibliothek: Nestor – Home

[8] Vgl. Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 9

[9] Vgl. Deutsche Initiative für Netzwerkinformation e.V.: DINI: DINI-Zertifikat 2010 für Dokumenten- und Publikationsservices

[10] Vgl. Deutsche Initiative für Netzwerkinformation e.V. / Arbeitsgruppe Elektronisches Publizieren: DINI-Zertifikat (2011), S. 31

2.2 Technische Anforderungen an die digitale Archivierung von Abschlussarbeiten

Als wichtigste Anforderung an das technische System eines Dokumentenservers ist der Erhalt von Authentizität und Integrität der gespeicherten Dokumente anzusehen, da es sich bei den beiden Begriffen um die „Kernkonzepte der Vertrauenswürdigkeit“[11] handelt.

Ist ein Informationsobjekt authentisch, bedeutet es, dass die gespeicherte Information nachweisbar von der angegebenen Quelle stammt, zum genannten Zeitpunkt erstellt wurde[12] und dessen Quelle genau identifiziert werden kann.[13] In Bezug auf die Abschlussarbeiten des Instituts für Informationswissenschaft garantiert die Authentizität, dass das Dokument tatsächlich dem vom Prüfling abgegebenen Originaldokument entspricht.

Im Zusammenhang mit Authentizität spielt auch Integrität eine wichtige Rolle bei der Speicherung von Dokumenten. Integrität bezeichnet „die Vollständigkeit und Unversehrtheit der Daten, d. h. dass diese weder absichtlich noch unabsichtlich, noch durch einen technischen Fehler verändert oder zerstört wurden.“[14]

Kann die Authentizität eines Dokuments nachgewiesen werden, so ist auch die Integrität desselben sicher. Denn nur eine unveränderte Datei ist auch authentisch.[15] Wird eine Abschlussarbeit nach Abgabe und Aufnahme in das Repositorium verändert, so gilt der Prüfling nicht mehr als Verfasser des vorliegenden Dokuments.
Neben der Forderung nach Authentizität und Integrität werden in den Kriterien unterschiedliche technische Verfahren zur Gewährleistung dieser genannt. Für die Erhaltung der Authentizität wird im Nestor-Kriterienkatalog der Einsatz von digitalen Signaturen vorgeschlagen.[16] Dieses Verfahren wird bei den Empfehlungen in Kapitel 4.3.3 zum Thema Authentizität und qualifizierte digitale Signaturen erläutert.

Um die Integrität der gespeicherten Dokumente zu bewahren empfiehlt das DINI-Zertifikat den Dokumenten Hashwerte zuzuordnen.[17] Dieses Verfahren wird ebenfalls in einem eigenen Textabschnitt zu Integrität und Hashwerten (siehe Kapitel 4.3.2) behandelt.

Es ist erforderlich, dass die Administratoren des Dokumentenservers vollen Zugriff auf die Dokumente und damit Bearbeitungsfreiheit haben. Konkret bedeutet das, die Entfernung sämtlicher Benutzungseinschränkungen und Schutzmaßnahmen, wie z. B. Verschlüsselungen oder Passwortabfragen.[18] Dies wird durch die Verwendung frei zugänglicher und weit verbreiteter Dateiformaten realisiert. Bei diesen Formaten ist nämlich davon auszugehen, dass sie in Zukunft noch wiedergegeben werden können, da sie von einer großen Community genutzt und fortgeführt werden. Als geeignetes Format

---

[11] Norm DIN 31644, S. 14
[12] Vgl. Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 24
[13] Vgl. Köhler, Thomas R.; Kirchmann, Walter: IT von A bis Z (2008), S. 22
[14] Norm DIN 31644, S. 6
[15] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 15
[16] Vgl. Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 25
[17] Vgl. Deutsche Initiative für Netzwerkinformation e.V. / Arbeitsgruppe Elektronisches Publizieren: DINI-Zertifikat (2011), S. 26
[18] Vgl. Norm DIN 31644, S. 30 und Deutsche Initiative für Netzwerkinformation e.V. / Arbeitsgruppe Elektronisches Publizieren: DINI-Zertifikat (2011), S. 32

für formatierte Texte wird im Nestor-Kriterienkatalog und im DINI-Zertifikat PDF/A genannt, welches im Standard ISO 19005-1 definiert ist.[19] Eine konkrete Beschreibung des Standards und seiner Vorzüge für die Archivierung erfolgt im Kapitel 4.3.1.

Als weiteres Kriterium wird die eindeutige Identifikation der Dokumente genannt. Diese dient im Allgemeinen der genauen Verortung der Dokumente sowie intern der Verwaltung und extern der sicheren Zitierbarkeit der enthaltenen Informationen.[20] Konkret fordern die DINI-Kriterien die Vergabe von Persistenten Identifikatoren für jedes gespeicherte Dokument.[21] Ein Persistenter Identifikator oder Persistent Identifier ist eine „eindeutige elektronische Kennzeichnung online gespeicherter Dokumente".[22] Auf die Vorgehensweise bei der Vergabe von Persistenten Identifikatoren am Institut für Informationswissenschaft wird im Kapitel 3.3.3 eingegangen.

2.3 Organisatorische Erfordernisse für die digitale Archivierung von Abschlussarbeiten

Allgemein ist anzumerken, dass die Durchführung stets den Zielen des Dokumentenservers entsprechend organisiert sein muss. Hierzu zählen sowohl die Verteilung von Personalstellen und finanziellen Mitteln, als auch die Anwendung einer passenden Organisationsstruktur, um einen reibungslosen Ablauf der festgelegten Arbeitsschritte zu garantieren. Die Zuständigkeiten innerhalb des Organisationssystems müssen eindeutig vergeben und die Verantwortlichkeiten festgesetzt werden.[23]

Zu den organisatorischen Ansprüchen an den Betrieb eines Dokumentenservers zählt vor allem eine ausreichende Finanzierung. Konkret fordern DIN-Norm und Nestor-Kriterien für staatlich getragene Einrichtungen wörtlich übereinstimmend, dass „die Finanzierung […] in den formalen Planungsunterlagen (zumindest mittelfristig) enthalten"[24] ist. Nur so kann der dauerhafte Betrieb des Dokumentenservers und damit der Erhalt der enthaltenen Dokumente gewährleistet werden.

Mit der Finanzierung geht auch die Forderung nach genügend Personal, welches über eine entsprechende Qualifizierung verfügt, einher.[25] Falls nicht genügend eigene Personalressourcen vorhanden sind, können Arbeitsschritte durch Outsourcing an externe Dienstleister übergeben werden.[26] In diesem Fall spielt wiederum die langfristig gesicherte Finanzierung eine große Rolle, da der Betreib des Dokumentenservers unter Umständen gänzlich von Fremdleistungen abhängt und die Kosten dafür getragen werden müssen. Erhält die Fremdfirma keine Bezahlung mehr, so wird sie schließlich ihre Leistungen nicht mehr erbringen.

---

[19] Vgl. ebd., S. 32 und Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 29

[20] Vgl. Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 34

[21] Vgl. Deutsche Initiative für Netzwerkinformation e.V. / Arbeitsgruppe Elektronisches Publizieren: DINI-Zertifikat (2011), S. 25

[22] Technische Universität Kaiserslautern: Glossar zu Begriffen der Informationskompetenz

[23] Vgl. Norm DIN 31644, S. 13 und Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 17

[24] Norm DIN 31644, S. 27 und Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 16

[25] Vgl. Norm DIN 31644, S. 13 und Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 17

[26] Vgl. Norm DIN 31644, S. 27 und Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 17

Des Weiteren zählt die Vorsorge für einen Krisenfall zu den organisatorischen Aufgaben des Trägers eines Dokumentenservers. Da die abgelegten Dokumente für einen bestimmten Zeitraum erhalten werden müssen und den Dokumentenserver oder den Träger selbst unterschiedlichste Schwierigkeiten treffen können, muss für die Fortführung der Archivierung auch über das Bestehen des Betreibers hinaus gesorgt werden. Darum sollte mit einer höheren oder auch einer externen Stelle vereinbart werden, dass diese im Notfall die gespeicherten Informationen übernehmen und verwahren wird und die Aufträge des Trägers fortführt.[27] Für den Ablauf der Übergabe muss ein genauer Plan vorhanden sein und die Dokumente, falls nötig, in exportfähige Daten, die kompatibel zum System des Krisenverwalters sind, umgewandelt werden.[28]

Die bisher genannten Kriterien beziehen sich auf den allgemeinen Betrieb des Dokumentenservers. Im Folgenden werden nun Richtlinien, die beim Umgang mit den Dokumenten selbst eine Rolle spielen, erläutert. Besonders im Hinblick auf die im vorherigen Kapitel definierten Werte der Authentizität und Integrität, gelten für Dokumentenserver strenge Vorgaben, was die Aufnahme und Speicherung der Informationsobjekte betrifft.

Bereits beim Upload der Dokumente handelt es sich um einen kritischen Arbeitsschritt. Möglicherweise werden sie nicht in dem Dateiformat abgeliefert, welches für die digitale Archivierung nötig ist. In diesem Fall findet eine Migration in ein geeignetes Format statt. Hierbei muss gewährleistet sein, dass das entstandene Archivdokument inhaltlich und formal identisch mit dem Ausgangsdokument ist.[29]

Die Migration der abgelieferten Dokumente birgt wiederum ein Risiko für den Erhalt der Integrität. Um eine Umwandlung der Dateien zu umgehen, kann bereits vom Produzenten verlangt werden, dass die Dokumente im vom Betreiber gewünschten Format abgeliefert werden und dann direkt auf den Dokumentenserver geladen werden können. Vor dem Upload müssen die Dokumente jedoch erst auf Stabilität, Dateiformat und Vollständigkeit überprüft werden. Des Weiteren trägt der Betreiber Sorge dafür, dass das Dokument durch eine lückenlose Organisationsstruktur und eine sichere Schnittstelle auf den Dokumentenserver gelangt.[30]

2.4 Rechtliche Aspekte der digitalen Archivierung von Abschlussarbeiten mit Bezug zur revisionssicheren Archivierung von Geschäftsdokumenten

Im folgenden Kapitel sollen die rechtlichen Aspekte, die bei der ausschließlich digitalen Archivierung von Abschlussarbeiten eine Rolle spielen, erläutert werden. Leider finden sich keine gesetzlichen Vorschriften, die sich konkret auf die elektronische Speicherung von Abschlussarbeiten beziehen. Darum soll als vergleichbare Problemstellung die Archivierung von Geschäftsdokumenten in Unternehmen herangezogen werden.

Grundsätzlich werden aufbewahrungspflichtige und aufbewahrungswürdige Dokumente unterschieden. Dokumente sind aufbewahrungspflichtig, wenn die jeweilige Institution nicht selbst über die Aufbewahrung bestimmen kann. Sie ist vielmehr durch

---

[27] Vgl. Norm DIN 31644, S. 14 und Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 18
[28] Vgl. Norm DIN 31644, S. 28
[29] Vgl. Norm DIN 31644, S. 29
[30] Vgl. Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 22–23

übergeordnete Gesetze und Vorschriften zur Speicherung verpflichtet.[31] Dies trifft z. B. auf Bankbelege zu, die buchführungspflichtige Unternehmen zur Steuerprüfung bei Finanzbehörden vorlegen müssen. Für Abschlussarbeiten hingegen werden Art und Dauer der Aufbewahrung in den Prüfungsordnungen der jeweiligen Studiengänge von den Hochschulen selbst festgelegt.[32] Damit handelt es sich bei Prüfungsarbeiten nach der Definition um aufbewahrungswürdige Unterlagen, da es hierbei im Ermessen der zuständigen Institution liegt, ob und wie lange Dokumente gespeichert werden müssen.[33] Die speziellen Regelungen zur Abgabe und Aufbewahrung der Abschlussarbeiten am Institut für Informationswissenschaft werden in Kapitel 3.4 vorgestellt.

Generell gelten Prüfungsarbeiten, und somit auch Abschlussarbeiten, nach der Übergabe an die Hochschule rechtlich als amtliche Urkunde. Diese dient ebenso wie Unternehmensunterlagen als Beweismaterial. In Bezug auf die Ansprüche an die inhaltliche Verlässlichkeit sind Geschäftsdokumente und Abschlussarbeiten durchaus vergleichbar. Somit fällt der Erhaltung von Integrität und Authentizität bei beiden digitalen Dokumenttypen eine wichtige Rolle zu.[34] Die Verantwortung, Unveränderlichkeit, Ursprünglichkeit und Vertraulichkeit der Dokumente zu erhalten ist in beiden Fällen groß. Bei Geschäftsdokumenten könnte es z. B. zu einer Anklage des Unternehmens wegen Steuerhinterziehung kommen. Im Falle der Abschlussarbeit könnte beispielsweise ein Studierender nach der Notenvergabe gegen seine erhaltene Zensur klagen oder die Hochschule feststellen, dass bei der Erstellung der Arbeit getäuscht wurde. In all diesen Situationen müssen die digital aufbewahrten Dokumente als Beweis dienen und diese Belegfunktion ohne jeden Zweifel erfüllen können. Somit lässt sich die Rechtslage von Abschlussarbeiten und Geschäftsdokumenten bis zu einem gewissen Grad als vergleichbar ansehen.

Nun ist die Frage zu klären, ob digitale Medienformen für die Speicherung von Geschäftsdokumenten gesetzlich zulässig sind. Diese Möglichkeiten können dann teilweise auf die Rechtslage der Abschlussarbeiten übertragen werden oder zumindest als Anregung für eventuelle neue Regelungen dienen.

Im Hinblick auf die digitale Archivierung von Geschäftsunterlagen und auch von Abschlussarbeiten kann die generelle Aussage getroffen werden, dass digitale Dokumente „die gleiche Verbindlichkeit einschließlich der hiermit verbundenen Rechtsfolgen nach sich ziehen, wie eine papiergebundene Aufbewahrung.“[35]

Deshalb ist für Geschäftsunterlagen eine revisionssichere Speicherung, die den Zugriff jederzeit möglich macht, vorgeschrieben. Als revisionssicher wird digitale Speicherung dann bezeichnet, wenn sie die geltenden deutschen Rechtsvorschriften erfüllt.[36] Dies entspricht den allgemeinen Compliance-Anforderungen, denen ein Unternehmen gerecht werden muss. Compliance bezeichnet „die Sicherstellung der Regelkonformität eines Unternehmens durch Organisation.“[37] In seiner Abhandlung verweist Thorsten Brand auf §§ 238, 239 und 257 im Handelsgesetzbuch (HGB) und §§ 146 und 147 in

---

[31] Vgl. Brand, Thorsten: An Geschäftsdokumente stellen Gesetze hohe Anforderungen (2012), S. 37

[32] Vgl. Prüfungsordnung für den Studiengang Bibliothekswesen mit dem Abschlussgrad „Bachelor of Arts“ der Fakultät für Informations- und Kommunikationswissenschaften der Fachhochschule Köln (vom 16.10.2008)

[33] Vgl. Brand, Thorsten: An Geschäftsdokumente stellen Gesetze hohe Anforderungen (2012), S. 37

[34] Vgl. Keens, Walter. E-Mail an Autorin (24.05.2013)

[35] Odenthal, Roger: Digitale Archivierung (2007), S. 36

[36] Vgl. Köhler, Thomas R.; Kirchmann, Walter: IT von A bis Z (2008), S. 199

[37] Holzhauser, Guido: Gesellschafts- und kapitalmarktrechtliche Grundlagen von Compliance (2008)

der Abgabenordnung (AO) als maßgebliche Vorschriften für die Archivierung von Geschäftsdokumenten.[38]

Das HGB erlaubt mit Ausnahme von Eröffnungsbilanzen und Abschlüssen die Speicherung auf Datenträgern, wenn diese den Grundsätzen ordnungsmäßiger Buchführung gerecht wird. Diese Grundsätze werden im folgenden Abschnitt erläutert. Zudem müssen die Dokumente für die Dauer der jeweiligen Aufbewahrungsfrist erhalten bleiben und für eventuelle Prüfungen jederzeit zugänglich sein.[39] Hierbei muss die Unveränderlichkeit der Dokumente gewährleistet werden. Der Inhalt muss originalgetreu erhalten bleiben.[40] In der genannten Paragraphen 146 und 147 der AO werden identische Sachverhalte geregelt. Zusätzlich werden Unternehmen dazu verpflichtet, die von einer entsprechenden Behörde angeforderten Daten sofort zugänglich zu machen oder geeignete Kopien, z. B. Ausdrucke, zu erstellen.[41]

Weitere Vorschriften finden sich in den Grundsätzen ordnungsmäßiger Buchführung beim IT-Einsatz (GoBIT). Hierbei handelt es sich um den Entwurf eines neuen Regelwerks, welches die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) aus dem Jahr 1995 ersetzen soll. Sie werden von der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V. erarbeitet. Durch diese Überarbeitung soll den technischen und rechtlichen Neuerungen Rechnung getragen und entsprechend zeitgemäße Vorschriften erstellt werden.[42] Die folgenden Aussagen beziehen sich auf die GoBIT Version 5.1 mit dem Stand vom 13.10.2012. Obwohl es sich dabei um eine Entwurfsfassung handelt, wird es trotzdem für sinnvoll erachtet diese zu betrachten, da die GoBS als veraltet angesehen werden können. Laut den GoBIT steht es dem Unternehmen als Buchführungspflichtigem frei in welcher Form Dokumente aufbewahrt werden, es sei denn ein entsprechendes Gesetz schreibt eine andere Vorgehensweise vor.[43] In Bezug auf Abschlussarbeiten ist keine solche Verordnung bekannt.

Zusätzlich muss das verwendete Datenmanagement- und Archivsystem von einer unabhängigen Instanz geprüft und als revisionssicher anerkannt werden. Dabei werden nicht nur technologische Anforderungen, sondern auch organisatorische Arbeitsabläufe begutachtet.[44] Für die Erfüllung dieser Ansprüche könnte der Erwerb eines DINI-Zertifikats als Bestätigung dienen.

Als Unterschied zwischen der Archivierung von Abschlussarbeiten und Geschäftsdokumenten ist zu nennen, dass Abschlussarbeiten von der Hochschule selbst, also von einer öffentlichen Einrichtung, aufbewahrt werden, während Geschäftsdokumente vom Erzeuger selbst verwahrt und auf Anfrage einer Behörde, z. B. des Finanzamtes, vorgelegt werden müssen.[45]

Wie die oben genannten Vorschriften deutlich machen, ist eine digitale Speicherung von Geschäftsdokumenten rechtlich anerkannt. Folglich müsste diese Vorgehensweise für Abschlussarbeiten unter bestimmten Voraussetzungen ebenfalls möglich sein. Ob diese Umstände beim Dokumentenserver des Instituts für Informationswissenschaft

---

[38] Vgl. Brand, Thorsten: An Geschäftsdokumente stellen Gesetze hohe Anforderungen (2012), S. 37
[39] Vgl. Handelsgesetzbuch (vom 20.04.2013), § 239 Abs. 3
[40] Vgl. ebd., § 257 Abs. 3
[41] Vgl. Abgabenordnung (vom 01.10.2002), §§ 146–147
[42] Vgl. Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.: Fachinformationen: Aktueller Entwurf der GoBIT (2013)
[43] Vgl. Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.: Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz (GoBIT) (2012), S. 26
[44] Vgl. Ferle, Christoph H.: Marktstudie digitale Langzeitarchivierung (2012), S. 6
[45] Vgl. Keens, Walter. E-Mail an Autorin (24.05.2013)

PubLIS Cologne gegeben sind und welche Voraussetzungen noch erfüllt werden müssten, soll in den folgenden Kapiteln herausgearbeitet werden.

Die rechtlichen Besonderheiten, die sich bei der Verwendung von digitalen Signaturen ergeben, werden in Kapitel 4.3.3 mit Bezug auf das Signaturgesetz (SigG) erläutert.

3 VORSTELLUNG DES DOKUMENTENSERVERS PUBLIS COLOGNE

Das Repositorium PubLIS Cologne des Instituts für Informationswissenschaft wird vom Bibliotheksservice-Zentrum Baden-Württemberg (BSZ) auf vertraglicher Basis gehostet und betrieben. Da es dadurch für die revisionssichere Speicherung der Dokumente verantwortlich ist, soll diese Institution und ihre Vorgehensweise bei der Speicherung der Dokumente im folgenden Abschnitt vorgestellt werden. Darüber hinaus werden der Dokumentenserver selbst, dessen Abwicklung am Institut sowie relevante, hochschulrechtliche Aspekte beleuchtet.

3.1 Vorstellung des Bibliotheksservice-Zentrums Baden-Württemberg

Das Bibliotheksservice-Zentrum Baden-Württemberg entstand 1996 beim Zusammenschluss der Zentrale des Südwestdeutschen Bibliotheksverbunds, des Zentralkatalogs Baden-Württemberg und einer Initiative zur Entwicklung eines einheitlichen Lokalsystems. Es ist als unselbstständige Anstalt des öffentlichen Rechts dem Ministerium für Wissenschaft, Forschung und Kunst des Landes Baden-Württemberg angegliedert und hat seinen Sitz in Konstanz. Das BSZ bietet deutschlandweit IT-Dienstleistungen für Bibliotheken, Museen und Archive an.

Aktuell ist das BSZ Arbeitgeber für 65 Personen unterschiedlicher Berufe. Dazu zählt bibliothekarisches, IT-technisches und Fachpersonal aus dem Bereich der Museologie. Das Servicezentrum ist in drei organisatorische Bereiche gegliedert. Neben dem Südwestdeutschen Bibliotheksverbund Baden-Württemberg, Saarland, Sachsen und der Abteilung für das Integrierte Bibliothekssystem Baden-Württemberg fungiert der Bereich Museen, Archive und Repositorien (MARE) als Dienstleister für Gedächtnisinstitutionen.[46] MARE „betreibt und hostet für Museen, Archive und Bibliotheken Informationssysteme zur elektronischen Dokumentation und Publikation, zur Internetrecherche, zur Virtuellen Auskunft sowie zur digitalen Langzeitarchivierung.“[47] Hierzu zählt insbesondere der Betrieb institutioneller Repositorien. Der Dienstleister unterstützt die jeweilige Institution bei Auswahl und Installation der entsprechenden Software. In Zusammenarbeit mit dem Kunden werden Datenformate und Archivierungsmethoden für den eigenen Bedarf bestimmt.[48] Die Abteilung MARE ist dementsprechend für den Dokumentenserver PubLIS Cologne zuständig.

3.2 Vorstellung von PubLIS Cologne und seiner Organisation am Institut für Informationswissenschaft

Seit Mitte des Jahres 2012 kann der Dokumentenserver PubLIS Cologne unter der URL http://publiscologne.fh-koeln.de aufgerufen werden. Er verzeichnet Metadaten und Volltexte der Publikationen des Instituts für Informationswissenschaft. Hierzu zählen

---

[46] Vgl. Bibliotheksservice-Zentrum Baden-Württemberg: Willkommen beim Bibliotheksservice-Zentrum Baden-Württemberg!

[47] Bibliotheksservice-Zentrum Baden-Württemberg: Museen, Archive und Repositorien im Bibliotheksservice-Zentrum Baden-Württemberg

[48] Vgl. Bibliotheksservice-Zentrum Baden-Württemberg: Willkommen beim Bibliotheksservice-Zentrum Baden-Württemberg!

Veröffentlichungen der Institutsmitglieder sowie Abschlussarbeiten der Absolventen.[49] Hauptziel des Dokumentenservers ist die Speicherung aller Abschlussarbeiten, die am Institut für Informationswissenschaft erstellt und bewertet werden. Im Moment befindet sich das Repositorium im Aufbau, d. h. die Abschlussarbeiten und Metadaten werden nach und nach eingepflegt. Dies wird dem Nutzer durch einen Hinweis auf der Website mitgeteilt. Dadurch lässt sich auch die relativ geringe Anzahl von 89 enthaltenen Dokumenten erklären (Stand: August 2013).[50]

Bei der Speicherung der Abschlussarbeiten gelten unterschiedliche Vorgaben, die die Veröffentlichung der Arbeiten betreffen. Dies ist durch drei verschiedene Zugriffsebenen für den Volltext geregelt. Welche davon für eine Abschlussarbeit verwendet werden soll, wird vom Erstkorrektor in einem eigens dafür vorgesehenen Formular festgelegt (siehe Anhang 1). Voraussetzung für eine Veröffentlichung des Volltextes ist die Zustimmung des Prüflings als Urheber des Textes. Diese wird direkt bei der Anmeldung auf dem Antragsformular zur Zulassung zur Abschlussarbeit erfragt (siehe Anhang 2). Für sehr gute Abschlussarbeiten bis zur Note 1,7 ist nach Zustimmung des Erstbetreuers die weltweite Sichtbarkeit des Volltextes vorgesehen. Auf der zweiten Ebene ist der Volltext fachhochschulweit aufrufbar. Dies trifft auf gute bis befriedigende Arbeiten zu. Für alle übrigen Arbeiten, die eventuell auch firmeninterne Informationen enthalten und deshalb nicht veröffentlicht werden dürfen, sind lediglich die Metadaten sichtbar. Der Zugriff auf den Volltext ist in diesem Fall nur für angemeldete Administratoren möglich. Die Metadaten sind generell für alle Arbeiten öffentlich einsehbar.[51]

Somit ist zwar die Verfügbarkeit der Abschlussarbeiten für Außenstehende teilweise eingeschränkt, sämtliche Dokumente sind jedoch auf dem Dokumentenserver gespeichert und für die Mitarbeiter bei Bedarf aufrufbar.

Zusätzlich wird die Langzeitarchivierung der Dokumente angestrebt. Im Rahmen dieser Arbeit beschränken sich die Betrachtungen zur Aufbewahrung jedoch auf die Erhaltung von Authentizität und Integrität der Arbeiten für einen Zeitraum von fünf bzw. zehn Jahren (siehe Kapitel 3.4). Daher werden die Aspekte und Vorgehensweisen der digitalen Langzeitarchivierung mit dem Ziel des zeitlich uneingeschränkten Erhalts der Informationsobjekte größtenteils außer Acht gelassen.

Im Folgenden wird die konkrete Verwaltung und Organisation des Dokumentenservers vorgestellt. Die Kosten für die Haltung der Daten beim BSZ werden vom Institut für Informationswissenschaft übernommen und belaufen sich auf 300 Euro im Jahr. Dies geht aus der Entgeltordnung des BSZ hervor, wo das Institut in der untersten Kategorie, d. h. Einrichtungen mit weniger als 2000 aktiven Nutzern, eingeordnet wird.[52]

Insgesamt zwei Personen am Institut für Informationswissenschaft sind im Moment an der Verwaltung von PubLIS Cologne beteiligt. Ein Dozent des Instituts mit einem Forschungs- und Lehrschwerpunkt auf Repositorien übernimmt neben seinen sonstigen Aufgaben die fachliche Leitung. Unterstützt wird er von einer angestellten Diplom-Bibliothekarin, die, ebenfalls neben weiteren Tätigkeitsfeldern, für die Administration zuständig ist. [53] Ab dem 1. Oktober 2013 wird eine studentische Hilfskraft mit einer

---

[49] Vgl. Institut für Informationswissenschaft der Fachhochschule Köln: PubLIS Cologne – Institutionelles Repositorium (ab Mitte 2012)

[50] Vgl. Fachhochschule Köln / Fakultät für Informations- und Kommunikationswissenschaften: OPUS 4 – Übersicht der Dokumenttypen

[51] Vgl. Rösch, Hermann. Mündliche Auskunft an Autorin (09.04.2013)

[52] Vgl. Bibliotheksservice-Zentrum Baden-Württemberg: Entgeltordnung des Bibliotheksservice-Zentrums Baden-Württemberg vom 27.04.2011 (2011), S. 9

[53] Vgl. Hofferberth, Dorothee. E-Mail an Autorin (05.06.2013)

Arbeitszeit von sechs Stunden pro Woche für den Upload der Dokumente und die Eingabe der Metadaten beschäftigt werden.[54]

Dieser Upload-Prozess läuft wie folgt ab. Die Abschlussarbeiten werden vom Prüfling als PDF-Datei auf einem Datenträger, z. B. einer CD oder DVD, abgeliefert. Das Dokument wird anschließend im Originalzustand übernommen und auf den Dokumentenserver geladen. Dies wird nicht, wie bei manchen Repositorien üblich, vom Prüfling selbst, sondern von Mitarbeitern des Instituts übernommen.[55]

Außerordentlich gute Abschlussarbeiten werden mitunter in die Schriftenreihe des Instituts Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft aufgenommen. Diese Reihe gibt einen Einblick in die wissenschaftlichen Ergebnisse, die am Institut für Informationswissenschaft sowohl von Lehrenden als auch von Studierenden erarbeitet worden sind.[56] Die ausgewählten Arbeiten werden dann als Titel innerhalb der Reihe auf dem Dokumentenserver veröffentlicht. Meistens müssen vor der Publikation jedoch noch Änderungen vorgenommen werden, um die Arbeit in optimierter Form innerhalb der Schriftenreihe zur Verfügung zu stellen. Somit entspricht das archivierte Dokument unter Umständen nicht mehr der ursprünglichen Prüfungsleistung und die Originalabschlussarbeit muss als weiteres Dokument aufbewahrt werden.[57] Daher werden im Moment am Institut beide Dateien auf den Dokumentenserver geladen und dort gespeichert.[58]

3.3 Technische Vorgehensweise bei Upload und Speicherung der Dokumente

3.3.1 Vorstellung der verwendeten Software OPUS 4

Das System, das dem Repositorium PubLIS Cologne zugrunde liegt, ist die Open-Source-Software OPUS 4. Die Software OPUS ist speziell für den Betrieb von fachlichen und institutionellen Dokumentenservern erarbeitet und in einem Projekt der Deutschen Forschungsgemeinschaft zur Version 4.0 weiterentwickelt worden. Das Projekt ist von einem Zusammenschluss von Bibliotheken und Bibliotheksverbünden, dem das Bibliotheksservice-Zentrum Baden-Württemberg und die Universitätsbibliothek der Universität Stuttgart vorstanden, durchgeführt worden. Im Jahr 2010 wurde die weitere Verantwortung auf den Kooperativen Bibliotheksverbund Berlin-Brandenburg (KOBV) und die Abteilung Wissenschaftliche Information des Zuse-Instituts Berlin übertragen. OPUS 4 ermöglicht eingeloggten Nutzern, im Falle des Instituts sind das die verantwortlichen Mitarbeiter, Dokumente über einen redaktionellen Bereich zu erschließen, zu verwalten und der Öffentlichkeit zur Recherche zur Verfügung zu stellen. Die Metadaten der Dokumente werden über ein Online-Formular erfasst und können schließlich mit oder ohne Volltext veröffentlicht werden.[59]

---

[54] Vgl. Hofferberth, Dorothee. E-Mail an Autorin (26.07.2013)
[55] Vgl. Hofferberth, Dorothee. Mündliche Auskunft an Autorin (12.04.2013)
[56] Vgl. Institut für Informationswissenschaft der Fachhochschule Köln: Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft
[57] Vgl. Hofferberth, Dorothee. Mündliche Auskunft an Autorin (12.04.2013)
[58] Vgl. Hofferberth, Dorothee. E-Mail an Autorin (26.07.2013)
[59] Vgl. Maiwald, Gunar: OPUS 4 (2012)

Für die Bedürfnisse des Instituts für Informationswissenschaft wurden lediglich Anpassungen am Layout vorgenommen und einige zusätzliche Angaben im Metadatenformular hinzugefügt.[60]

3.3.2 Speicherung der Dokumente beim Bibliotheksservice-Zentrum Baden-Württemberg

Die Abschlussarbeiten, welche auf den Dokumentenserver geladen werden, werden im ursprünglichen Format der vom Prüfling abgegebenen Datei gespeichert. Es findet also keine Migration in ein speziell für die langfristige Aufbewahrung geeignetes Dateiformat statt. Als beschreibende Metadaten werden Dateiname und -größe im Format MAB 2[61] abgelegt.

Um die Integrität der Dokumente zu gewährleisten werden in einem Hash-Verfahren Prüfsummen nach MD5 und SHA512 errechnet. Beide Verfahren werden bei der Empfehlung zur Integritätserhaltung in Kapitel 4.3.2 näher erläutert.

Nach Ablage der Dokumente mitsamt der zugehörigen Metadaten und Prüfsummen, werden die Daten täglich in einem Backup gesichert und abgespeichert. Somit kann im Falle eines Serverausfalls der letzte Stand innerhalb eines Werktages wieder hergestellt werden. Zudem verfügt das BSZ über eine unterbrechungsfreie Stromversorgung (USV) für die Server.[62] Bei einer USV handelt es sich um ein System, welches einen kurzzeitigen Ausfall der lokalen Stromversorgung überbrücken kann. Somit kann Datenverlust bei den angeschlossenen IT-Geräten verhindert werden.[63] Die Informationsobjekte werden nach der Speicherung jedoch nicht mehr auf Dateifehler o.ä. kontrolliert.

Wie in Kapitel 3.2 erwähnt, werden die Abschlussarbeiten mit unterschiedlichen Zugriffsmöglichkeiten gespeichert. Technisch wird dies über eine Einschränkung auf einen bestimmten IP-Adressenbereich verwirklicht. Die Dokumente, welche lediglich fachhochschulweit einsehbar sein sollen, werden der Nutzerrolle Hochschule zugeordnet, welche den IP-Adressraum der Fachhochschule Köln beinhaltet. Dementsprechend können diese Arbeiten nur im Hochschulnetz bzw. über eine entsprechende VPN-Verbindung eingesehen werden. Wenn nur die Metadaten öffentlich zugänglich sein sollen und der Zugriff auf den Volltext allein für Administratoren möglich sein soll, so werden diese Arbeiten in die Nutzerrolle Administrator eingeordnet. Somit sind die Volltexte dieser Dokumente nur nach dem Login mit einem Administratorpasswort über den redaktionellen Bereich des Dokumentenservers zugänglich.[64]

3.3.3 URN-Generierung am Institut für Informationswissenschaft

Um die Dokumente der obersten Zugriffsebene langfristig verfügbar zu machen, werden zusätzlich Persistent Identifier für jede Arbeit vergeben. Persistent Identifier „dienen der dauerhaften Sicherung der Auffindbarkeit elektronisch zugänglicher Dokumente. Während eine URL (Uniform Resource Locator) sich aus verschiedenen Gründen ändern kann, bleibt ein Persistent Identifier für das ihm zugewiesene Dokument stabil.“[65]

---

[60] Vgl. Hofferberth, Dorothee. Mündliche Auskunft an Autorin (12.04.2013)
[61] Vgl. ebd.
[62] Vgl. Gerland, Friederike. E-Mail an Autorin (29.05.2013)
[63] Vgl. IT-Wissen – Das große Online-Lexikon für Informationstechnologie (2013)
[64] Vgl. Gerland
[65] Technische Universität Kaiserslautern: Glossar zu Begriffen der Informationskompetenz

Ein mögliches System für das Referenzieren digitaler Medien ist das Uniform-Resource-Name-Schema (URN-Schema). Am Institut wird deshalb über das Persistent-Identifier-Management der Deutschen Nationalbibliothek (DNB) ein URN für jede weltweit publizierte Abschlussarbeit generiert.

Zunächst wird der allgemeine Aufbau von URNs und die Vorgehensweise bei deren Vergabe durch die Deutsche Nationalbibliothek erläutert.

Ein Uniform Resource Name ist in mehrere Abschnitte aufgeteilt, die untereinander in hierarchischen Beziehungen stehen. An erster Stelle, nach der Bezeichnung URN, steht der Namensraum auch Namespace (NID) genannt. Zur weiteren Spezifizierung wird zuerst der Unternamensraum bzw. Subnamespace (SNID) und schließlich der Namesraumbezeichner oder auch Namespace Specific String (NISS) ergänzt. Der Namesraumbezeichner, welcher als letzter Teilbereich nach einem Bindestrich angefügt wird, dient hierbei zur eigentlichen Identifikation des Dokuments. Somit ergibt sich folgendes grundsätzliches Schema:

URN:[NID]:[SNID]-[NISS]

Die europäischen Nationalbibliotheken administrieren kooperativ einen eigenen Namensraum, welcher als Namespace die National Bibliography Number (NBN) und ein Kürzel für das jeweilige Land enthält. Folglich liegen alle URNs mit dem Namensraum URN:NBN:DE in der Verantwortlichkeit der Deutschen Nationalbibliothek. [66]

Um das beschriebene URN-System der DNB nutzen zu können, muss eine interessierte Institution zunächst einen Unternamensraum innerhalb des in Deutschland gültigen Namensraums beantragen.[67] Ist der entsprechende Unternamensraum registriert, so kann die Institution selbst nach dem festgelegten Schema URNs erzeugen und für ihre zu veröffentlichenden Dokumente vergeben. Voraussetzung ist immer, dass die URN-Bezeichnungen korrekt und vor allem global eindeutig sind.[68]

Üblich ist bei deutschen Bibliotheken den Unternamensraum aus einer Kombination aus der Abkürzung des eigenen Bibliotheksverbundes und einer Sigelnummer zu bilden.

Der letzte Abschnitt des URN schließlich, der Namesraumbezeichner, wird von der jeweiligen Institution selbstständig und unabhängig gestaltet und vergeben. Dieser kann z. B. aus einer fortlaufenden Nummer bestehen oder aus einer Datumsangabe und einer fortlaufenden Nummer zusammengesetzt sein. Zuletzt wird eine Prüfziffer errechnet, anhand derer der URN-String verifiziert werden kann. Das URN-Schema eines Repositoriums an einer deutschen Bibliothek ist also üblicherweise folgendermaßen aufgebaut:

URN:NBN:DE:[Verbundkürzel]:[Sigelnummer]-[eindeutige Nummer] [Prüfziffer][69]

An diesem Schema orientiert sich auch die Erzeugung von URNs am Institut für Informationswissenschaft. Der genaue Aufbau wird anhand der URN einer Masterarbeit, deren Metadaten in Abbildung 1 zu sehen sind, aufgezeigt. Diese lautet wie folgt:

URN:NBN:DE:HBZ:79pbc-2013072503

Als Unternamensraum wird die Abkürzung des Hochschulbibliothekszentrums des Landes Nordrhein-Westfalen (HBZ) in Verbindung mit dem Sigel verwendet. PubLIS

---

[66] Vgl. Ackermann, Uta; Berner, Christiane; Elbert, Natalie; Kett, Jürgen: Policy für die Vergabe von URNs im Namensraum urn:nbn:de (2012), S. 9

[67] Vgl. Deutsche Initiative für Netzwerkinformation e.V. / Arbeitsgruppe Elektronisches Publizieren: DINI-Zertifikat (2011), S. 41–42

[68] Vgl. Neuroth, Heike; Oßwald, Achim; Scheffel, Regine; Strathmann, Stefan; Huth, Karsten: Nestor-Handbuch (2010), S. 9:51-9:52

[69] Vgl. Deutsche Nationalbibliothek: Persistent Identifier (2008)

Cologne wurde als virtueller Bibliothek das eigene Sigel 79pbc zugeordnet, welches in der Zeitschriftendatenbank recherchiert werden kann.[70] Der Namensraumbezeichner wird, wie es als übliche Methode bereits erwähnt wurde, aus dem Datum, hier der 25.07.2013, und einer laufenden Nummer, welche in diesem Fall 0 ist, gebildet. Die letzte Ziffer ist die Prüfziffer, welche nach einem bestimmten Algorithmus berechnet wird. Nähere Informationen hierzu finden sich auf der Website der DNB zum Thema Persistent Identifier.[71]

Die erzeugten URNs werden den Dokumenten direkt beim Upload zugeordnet, regelmäßig über eine offene Schnittstelle von der Deutschen Nationalbibliothek geharvestet und daraufhin in den Bestand der DNB aufgenommen.[72]

Metadaten

Verfasserangaben:	Anke Petschenka
Dokumentart:	Masterarbeit
Jahr der Erstveröffentlichung:	2013
Datum der Abschlussprüfung:	03.05.2013
Betreuer:	Hermann Rösch
Gutachter:	Inka Tappenbeck
Studiengang:	MALIS
Sprache:	Deutsch
Seitenzahl:	87: III.
Freies Schlagwort / Tag:	Hochschulbibliothek; Hochschule; Physischer Lernraum; Virtueller Lernraum
URN:	urn:nbn:de:hbz:79pbc-2013072503

Abbildung 1: Beispiel für Metadatenangaben mit URN in PubLIS Cologne

Obwohl dieses Sicherungssystem nur für einen Teil der Dokumente angewendet werden kann, da nur ausgewählte Arbeiten für eine Veröffentlichung bereitgestellt werden, wird eine Erläuterung des URN-Systems als sinnvoll erachtet. Es handelt sich nämlich um ein wirksames und äußerst zuverlässiges Verfahren zur Sicherung der Dokumente, da die Abschlussarbeiten mit der oben erwähnten Aufnahme in den Bestand der Deutschen Nationalbibliothek verlässlich und dauerhaft archiviert werden.

3.4 Rechtliche Aspekte der digitalen Aufbewahrung von Abschlussarbeiten am Institut für Informationswissenschaft der Fachhochschule Köln

Die juristische Grundlage für die Abgabe und anschließende Aufbewahrung von Prüfungsarbeiten findet sich in der Einschreibungsordnung der Fachhochschule Köln und den Bachelor- bzw. Masterprüfungsordnungen der jeweiligen Studiengänge. Der Übersichtlichkeit wegen werden für die weitere Untersuchung die Prüfungsordnungen der Bachelor-Studiengänge Bibliothekswesen und Informationswirtschaft herangezogen.

---

[70] Vgl. ZDB-OPAC – Sigelsuche
[71] Vgl. Deutsche Nationalbibliothek: Persistent Identifier
[72] Vgl. Hofferberth, Dorothee. Mündliche Auskunft an Autorin (12.04.2013)

§ 13 Abs. 4 der Einschreibeordnung der Fachhochschule Köln besagt, dass „Prüfungsarbeiten […] nach Ablegung der jeweiligen Prüfung fünf Jahre aufbewahrt“[73] werden müssen. Unter dem Begriff Prüfungsarbeiten sind Abschlussarbeiten einzuordnen und müssen somit ebenfalls fünf Jahre aufbewahrt werden, bevor sie auf Anfrage dem Prüfling übergeben werden.[74]

Weitere Hinweise zur Aufbewahrungsdauer liefern die Bachelorprüfungsordnungen (BPO) der Studiengänge Bibliothekswesen und Informationswirtschaft. Die zitierten Paragraphen sind für beide BPOs identisch, weshalb im Folgenden lediglich Bezug zur BPO des Studiengangs Bibliothekswesen genommen wird. Wird nach der Übergabe des Abschlusszeugnisses bekannt, dass der Prüfling bei einer seiner Arbeiten getäuscht hat, so können ihm nachträglich die erreichten Leistungspunkte der betroffenen Prüfung aberkannt werden. Unter Umständen kann der Prüfungsausschuss den gesamten Bachelorabschluss als nicht bestanden erklären.[75] Die Aberkennung eines unrechtmäßig erteilten Abschlusszeugnisses kann innerhalb einer Frist von zehn Jahren nach Übergabe des Zeugnisses erfolgen.[76]

Folglich ist es erforderlich, dass alle abgegebenen und korrigierten Prüfungs- und somit auch Abschlussarbeiten für diesen Zeitraum von der Fachhochschule verwahrt werden. Schließlich dienen sie als Beleg für rechtmäßig oder unrechtmäßig erhaltene Leistungspunkte und müssen so die Nachvollziehbarkeit der entsprechenden Notenvergabe gewährleisten. Dies bewahrt die Rechtsicherheit sowohl für die Hochschule als auch für die Studierenden im Falle eines Rechtsstreits bezüglich der Abschlussarbeit.

[73] Einschreibungsordnung der Fachhochschule Köln (vom 11.07.2007), § 13 Abs. 4
[74] Vgl. ebd., § 13 Abs. 4
[75] Vgl. Prüfungsordnung für den Studiengang Bibliothekswesen mit dem Abschlussgrad „Bachelor of Arts“ der Fakultät für Informations- und Kommunikationswissenschaften der Fachhochschule Köln (vom 16.10.2008), § 41, Abs. 1
[76] Vgl. ebd. § 41, Abs. 3

4 HANDLUNGSEMPFEHLUNGEN FÜR DIE AUSSCHLIESSLICH DIGITALE AUFBEWAHRUNG VON ABSCHLUSSARBEITEN AUF DEM DOKUMENTENSERVER PUBLIS COLOGNE

Im bisherigen Teil dieser Arbeit ist die Möglichkeit der ausschließlich digitalen Archivierung von Abschlussarbeiten auf dem Repositorium PubLIS Cologne ausführlich nach unterschiedlichen Gesichtspunkten besprochen worden. Im nun folgenden Abschnitt werden, unter Beachtung der angeführten Kriterien, Empfehlungen an das Institut für Informationswissenschaft ausgesprochen. Diese beziehen sich auf organisatorische, technische und institutsinterne Bereiche. All diese Handlungsempfehlungen sollen als Anregungen, zum Teil aber auch als konkrete Hinweise, an die Verantwortlichen dienen.

4.1 Handlungsempfehlungen für die Organisation des Dokumentenservers

Laut der in Kapitel 2.3 vorgestellten Kriterien kommt der Organisation eines Dokumentenservers eine entscheidende Rolle zu. Denn nur durch klare Kompetenzfestlegungen, eine genaue Planung der Arbeitsabläufe und die Regelung des personellen und finanziellen Rahmens, kann der laufende Betrieb und der langfristige Erhalt eines Repositoriums garantiert werden. Konkrete Empfehlungen für die Organisation des Dokumentenservers PubLIS Cologne am Institut für Informationswissenschaft und der Fachhochschule Köln als übergeordnete Institution werden im folgenden Kapitel gegeben.

4.1.1 Sicherstellung von langfristiger Finanzierung und ausreichend qualifiziertem Personal

Für die Garantie eines langfristigen, zuverlässigen Betriebs des Repositoriums und somit zur Erlangung von Vertrauenswürdigkeit ist die Bereitstellung von Geldern und Personal unbedingt erforderlich. Dies wird bei den genannten organisatorischen Erfordernissen in Kapitel 2.3 deutlich gemacht und wird im Folgenden auf die Situation des Instituts für Informationswissenschaft übertragen.

Um eine ausreichende und langfristige Finanzierung des Dokumentenservers zu gewährleisten, sollte sich das Institut für Informationswissenschaft bzw. die Fachhochschule Köln als übergeordnete Instanz schriftlich dazu bereiterklären, das Repositorium auf unbestimmte Zeit zu betreiben und zu unterhalten. Da die Kosten, wie in Kapitel 3.2 erwähnt, mit 300 Euro pro Jahr keine einschneidende finanzielle Belastung für die Hochschule bzw. das Institut darstellen, ist der Erhalt einer solchen Zusicherung durchaus realistisch. Zusätzlich sollte der Dokumentenserver als feste Kostenstelle in den jährlichen Haushaltsplan der Hochschule aufgenommen werden.

Des Weiteren kann die Überlegung angestellt werden, ob der Arbeitsbereich des Repositoriums als eigene Unterabteilung in die Organisation des Instituts eingegliedert werden sollte. Nicht zu vergessen sind dabei die nötigen Personalstellen und die damit verbundenen Kosten. Es sollte also gewährleistet sein, dass immer eine ausreichende Anzahl von Arbeitsstunden für die Betreuung des Repositoriums vorgesehen ist. Diese sollten im Arbeitsvertrag der betroffenen Institutsmitarbeiter genau festgelegt sein. Folglich sind eventuell Entlastungen in anderen Arbeitsbereichen der Mitarbeiter nötig,

damit die Betreuung von PubLIS Cologne zuverlässig durchgeführt werden kann und es zu keiner Überlastung der integrierten Mitarbeiter kommt. Gleichzeitig besteht die Notwendigkeit Verantwortlichkeiten zu klären und zu vergeben, um Kompetenzüberschneidungen oder fehlende Zuständigkeitsbereiche zu vermeiden. Ungeordnete Verantwortlichkeitsbereiche führen sonst dazu, dass sich bei einem auftretenden Problem keine der Parteien zuständig fühlt und dieses somit ungelöst bleibt. Eine solche Entwicklung kann die sichere digitale Archivierung gefährden. Gerade wenn ein externer Dienstleister beauftragt wurde, einen Teil der Archivierungsaufgaben zu übernehmen, müssen die Verantwortungsbereiche deutlich getrennt und schriftlich festgehalten werden.

Da es sich im Moment und auch in näherer Zukunft um lediglich drei Personen handelt, welche am Institut mit dem Dokumentenserver PubLIS beschäftigt sind, so wird es nicht als sinnvoll erachtet ein eigenes Organigramm zu erstellen. Es muss lediglich geklärt werden, wer welche Aufgaben übernimmt. Somit sollten die Bereiche der fachlichen und administrativen Leitung, wie sie bereits in Kapitel 3.2 erwähnt worden sind, weiter spezifiziert und mit konkreten Aufgabenbeschreibungen versehen werden. Vor allem beim Vertrag der studentischen Hilfskraft sind besondere Regelungen erforderlich. So muss dieser den studentischen Mitarbeiter auf Stillschweigen verpflichten, was z. B. nicht-bestandene Abschlussarbeiten und Sperrvermerke angeht. Zusätzlich muss deutlich gemacht werden, dass das Verändern oder das Löschen von Dokumenten bzw. Metadaten nicht zulässig ist.

Neben Anzahl und Finanzierung der Mitarbeiter ist auch deren Qualifizierung von großer Wichtigkeit. Die konkrete Handhabung und Funktionsweise des Archivierungssystems darf sich zu keinem Zeitpunkt dem Verständnis der verantwortlichen Mitarbeiter entziehen. Trotz möglicher steigender Komplexität muss das Vorgehen für die Verantwortlichen nachvollziehbar sein, sodass keine Unklarheiten zwischen der Fachabteilung, dem Institut, und dem IT-Bereich, dem BSZ, entstehen.[77]

Um dies zu erreichen müssen sich qualifizierte Mitarbeiter für den Dokumentenserver verantwortlich zeigen. Mit einer ausgebildeten Diplom-Bibliothekarin und einem Dozenten ist diese Voraussetzung am Institut gut erfüllt worden. Die studentische Hilfskraft, welche sich in Zukunft mit dem Upload der Dokumente beschäftigen wird, muss daher eine gründliche Einarbeitung erfahren. Des Weiteren muss das zuständige Personal laufend über Neuerungen informiert werden, sowohl die Vorgehensweise des BSZ als auch allgemeine Entwicklungen betreffend. Dies kann z. B. durch die Teilnahme an Kongressen oder Weiterbildungen zum Thema digitale Archivierung realisiert werden.

4.1 2 Einführung eines Internen Kontrollsystems

Um den reibungslosen Ablauf beim Upload der eingereichten Abschlussarbeiten zu gewährleisten und somit die Gefahr von Verfälschungen, ob gewollt oder ungewollt, einzudämmen, wird von den aufgeführten Kriterien ein funktionierendes Organisationssystem gefordert (siehe Kapitel 2.3). Zu diesem Zweck sollte ein Internes Kontrollsystem eingeführt werden.

Unter dem Begriff Internes Kontrollsystem (IKS) werden „die vom Management im Unternehmen eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) verstanden, die auf organisatorische Umsetzung der Entscheidungen des Managements gerichtet sind, und zwar zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Ge-

[77] Vgl. Odenthal, Roger: Digitale Archivierung (2007), S. 37

schäftstätigkeit […] sowie zur Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften."[78]

Ein Internes Kontrollsystem setzt sich aus manuellen und programmierten Kontrollmaßnahmen zusammen. Letztere werden automatisch vom IT-System durchgeführt und sind programmabhängig. Die manuellen Kontrollmaßnahmen wiederum werden von den jeweiligen Mitarbeitern auf Grundlage von vorgegebenen Anweisungen übernommen. Wie immer bei menschlicher Arbeit, können, beabsichtigt oder unbeabsichtigt, durch mangelnde Sorgfalt oder Unterlassung Fehler auftreten. Je genauer die Arbeitsanweisungen, je ausführlicher die Dokumentation und je gründlicher die Überwachung sind, umso geringer ist die Fehleranfälligkeit.[79]

Die folgenden Ausführungen werden sich lediglich auf die organisatorischen Aspekte eines IKS, also auf die manuellen Ausführungsbestimmungen, beziehen. Hinzu kommt, dass am Institut für Informationswissenschaft nur ein sehr kleiner Personenkreis für die Organisation des Dokumentenservers zuständig ist. Aus diesem Grund ist es nicht zweckmäßig, ein komplettes IKS zu erarbeiten, da dies meist erst für komplexere Prozesse mit vielen beteiligten Personen nötig ist. Stattdessen sollen einige Grundsätze des IKS und Möglichkeiten zu deren konkreten Umsetzung am Institut vorgestellt werden. Ziel dieser Festlegungen ist es, die Vertrauenswürdigkeit von PubLIS Cologne und dessen Organisation zu steigern und zu erhalten.

Zunächst werden die Risiken, welche auftreten können und durch den Einsatz des IKS eingedämmt werden sollen, genannt. Die Dokumente könnten beabsichtigt oder unbeabsichtigt falsch bzw. überhaupt nicht vom abgegebenen Datenträger auf den Dokumentenserver hochgeladen werden. Bei der Übertragung besteht zudem die Gefahr, dass die Arbeiten willentlich manipuliert oder unabsichtlich verändert werden. Des Weiteren könnte eine fehlerhafte Eingabe oder eine falsche Zuordnung der Metadaten dazu führen, dass die Dokumente nicht mehr auffindbar sind.[80]

Um diese Risiken einzudämmen, ist der Einsatz einiger Prinzipien des IKS hilfreich. Die für den vorliegenden Fall wichtigsten Grundsätze sind das Vier-Augen-Prinzip und das Prinzip der Transparenz. Zudem findet das Prinzip der Funktionstrennung beim IKS Anwendung.

Beim Prinzip der Funktionstrennung ist vorgesehen, dass verwaltende und durchführende Instanzen organisatorisch voneinander getrennt werden. In Bezug auf das Institut sollten deshalb die am Upload der Dokumente beteiligten Mitarbeiter, also die Institutsmitarbeiterin und die studentische Hilfskraft, unabhängig von der fachlichen Leitung agieren. Dadurch behält die Leitung einen unabhängigen Überblick und kann so bei Kontrollen Fehler schneller entdecken. Ansonsten fällt das Funktionstrennungsprinzip nicht zu sehr ins Gewicht, da die Anzahl der agierenden Mitarbeiter sehr gering ist. Das Prinzip der Vier Augen besagt, dass jeder bedeutende Arbeitsschritt kontrolliert und dokumentiert werden muss. Eng damit zusammen hängt das Transparenzprinzip, da hierbei genau festgelegt wird, wie ein bestimmter Prozess durchzuführen und in welchem Umfang er in der Verfahrensdokumentation festzuhalten ist.[81]

---

[78] Heinrich, Gert; Horstschäfer, Anna: Das interne Kontrollsystem beim Einsatz elektronischer Archivierungsverfahren (2013), S. 70–71

[79] Vgl. Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.: Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz (GoBIT) (2012), S. 20–21

[80] Vgl. Heinrich, Gert; Horstschäfer, Anna: Das interne Kontrollsystem beim Einsatz elektronischer Archivierungsverfahren (2013), S. 73

[81] Vgl. Q-Perior AG: Optimierung und Prüfung des Internen Kontrollsystems (IKS) (2012), S. 13

Für die Vorgehensweise bei Entgegennahme und Upload der Abschlussarbeiten sollte, nach dem Vorbild des Internen Kontrollsystems, eine genaue Handlungsvorgabe erarbeitet werden. Diese könnte in Form einer Checkliste realisiert werden, welche alle nötigen Arbeitsschritte klar verständlich und chronologisch aufführt, um Fehler und Versäumnisse zu vermeiden. Gerade beim Einarbeiten neuer Mitarbeiter, z. B. einer studentischen Hilfskraft, ist eine solche Zusammenstellung von großem Nutzen. Ferner muss vermieden werden, dass nur eine einzige Person um das richtige Vorgehen weiß und dieses durchführt, da diese z. B. in der Urlaubszeit vertreten werden muss.

Bei solchen Vorgaben müssen auch die Punkte Dokumentation und Kontrolle berücksichtigt werden, welche beim IKS eine zentrale Rolle spielen. So sollte nach jedem Upload überprüft werden, ob die Metadaten korrekt eingegeben wurden und der Volltext entsprechend der vorgesehenen Zugriffsebene eingesehen werden kann. Somit findet hierdurch das Vier-Augen-Prinzip Anwendung, denn die Kontrolle sollte nicht vom bearbeitenden Mitarbeiter, sondern von einer zweiten Person übernommen werden. Nur so können eventuelle Unzulänglichkeiten in der Aufnahme entdeckt werden, da man oft die eigenen Fehler nicht wahrnimmt oder diese eventuell im Glauben richtig zu handeln begangen hat.

Die folgende Erläuterung zeigt auf, wie der Prozess der Annahme und Speicherung der Abschlussarbeiten ablaufen könnte und soll als Hilfsmittel für alle beteiligten Mitarbeiter dienen.

Zunächst gehen die Dokumente auf einem Datenträger gespeichert als Dateien beim zuständigen Mitarbeiter ein. Dieser überprüft, ob das Dateiformat korrekt ist (siehe Kapitel 4.3.1). Danach wird die Einverständniserklärung des Prüflings bezüglich der Veröffentlichung gesichtet. Ist der Student mit der Veröffentlichung einverstanden, so wird anhand des entsprechenden Empfehlungsformulars des Betreuers die festgelegte Zugriffsebene geprüft. Schließlich werden die Angaben auf den Formularen mit denen des Titelblatts des Dokuments verglichen, um sicherzugehen, dass die formale Korrektheit der Arbeit gegeben ist.

Darauffolgend werden die Metadaten des Dokuments in der Eingabemaske im redaktionellen Bereich des OPUS-Systems erfasst. Dabei wird die entsprechende Zugriffsebene eingestellt. Wird das Dokument veröffentlicht und der Volltext weltweit zugänglich gemacht, so wird zusätzlich, nach dem in Kapitel 3.3.3 beschriebenen Verfahren, ein URN zur eindeutigen Identifikation erzeugt und vergeben.

Schließlich wird das Dokument mit den Metadaten über die Erfassungsmaske auf den Server hochgeladen. Damit ist es jedoch noch nicht sichtbar, sondern muss nach der Kontrolle in einem extra Arbeitsschritt freigegeben werden. Beim Hochladen ist darauf zu achten, dass die Datei in einer standardisierten Weise benannt wird. Diese könnte z. B. lauten: Art der Abschlussarbeit_Name des Verfassers_Semesterangabe. Eine Übernahme des Titels in die Dateibezeichnung scheint nicht sinnvoll, da die gewählten Titel durch den hohen Spezialisierungsgrad oft sehr lang sind.

Nachdem die Abschlussarbeit hochgeladen worden ist, muss vor der Veröffentlichung eine umfassende Überprüfung der erfassten Daten und der Wiedergabe des Dokuments erfolgen. Um dem Vier-Augen-Prinzip des IKS zu entsprechen, sollte diese Abschlusskontrolle, wie bereits oben erwähnt, von einer zweiten Person, welche nicht an der Erfassung der Daten und dem Prozess des Hochladens beteiligt war, durchgeführt werden. Zuerst werden die Metadaten auf Vollständigkeit und Korrektheit überprüft. Schließlich wird getestet, ob die Arbeit nur von der vorgesehenen Zugriffsebene aus aufgerufen werden kann. Denn ist eine Arbeit, die nach Wunsch des Prüflings nicht veröffentlicht werden darf, hochschulweit bzw. sogar weltweit einsehbar, so wird die Abschlussarbeit gegen den Willen des Prüflings veröffentlicht. Dadurch würde das

Institut die schriftliche Vereinbarung missachten und sich somit strafbar machen. Um das zu überprüfen wird der Volltext zunächst aus der Administratorsicht und aus dem Hochschulnetz heraus aufgerufen. Da sich die Mitarbeiter durch Ihren Arbeitsplatz im Institut stets im Hochschulnetz befinden, müsste ihnen für die Kontrolle der weltweiten Zugänglichkeit über einen VPN-Client eine IP-Adresse außerhalb des Hochschulnetzes zugeordnet werden. Nach Abschluss der Kontrollen und der Beseitigung eventuell aufgetretener Fehler, können das Dokument und die zugehörigen Metadaten veröffentlicht werden. Dafür wird das Dokument über die Administratorseite freigeschaltet.

Als letzte Phase im Prozessablauf folgt die Dokumentation. Um den Upload-Vorgang festzuhalten, werden das Einverständnisformular des Prüflings und die Bewertung des Betreuers in den dafür vorgesehenen Ordnern abgeheftet und vom Institut aufbewahrt. Die vergebenen URNs sowie eventuelle Besonderheiten werden im Moment in Excel-Tabellen festgehalten. Solche Abweichungen können z. B. sein, dass die Arbeit nicht bestanden oder mit einem Sperrvermerk versehen wurde, da sie firmeninterne Daten enthält. Ist die Arbeit in die Schriftenreihe Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft aufgenommen worden, so müssen zwei Versionen des Dokuments mit unterschiedlichen Zugriffsebenen gespeichert werden.[82]

Der komplette Prozessablauf unterteilt in die Prozessphasen Eingang, Datenerfassung, Upload, Kontrolle und Dokumentation sowie die einzelnen Arbeitsschritte werden in Abbildung 2 veranschaulicht.

Der Aspekt der qualifizierten elektronischen Signatur wird in dieser Darstellung nicht berücksichtigt. Zum einen da diese im Moment am Institut nicht vergeben wird und zum anderen da vor einer Einführung die Festlegung auf eine der in Kapitel 4.3.3 vorgestellten Durchführungsmöglichkeiten stattfinden müsste, was wiederum unterschiedliche Organisationslösungen nach sich ziehen würde.

[82] Vgl. Hofferberth, Dorothee. E-Mail an Autorin (26.07.2013)

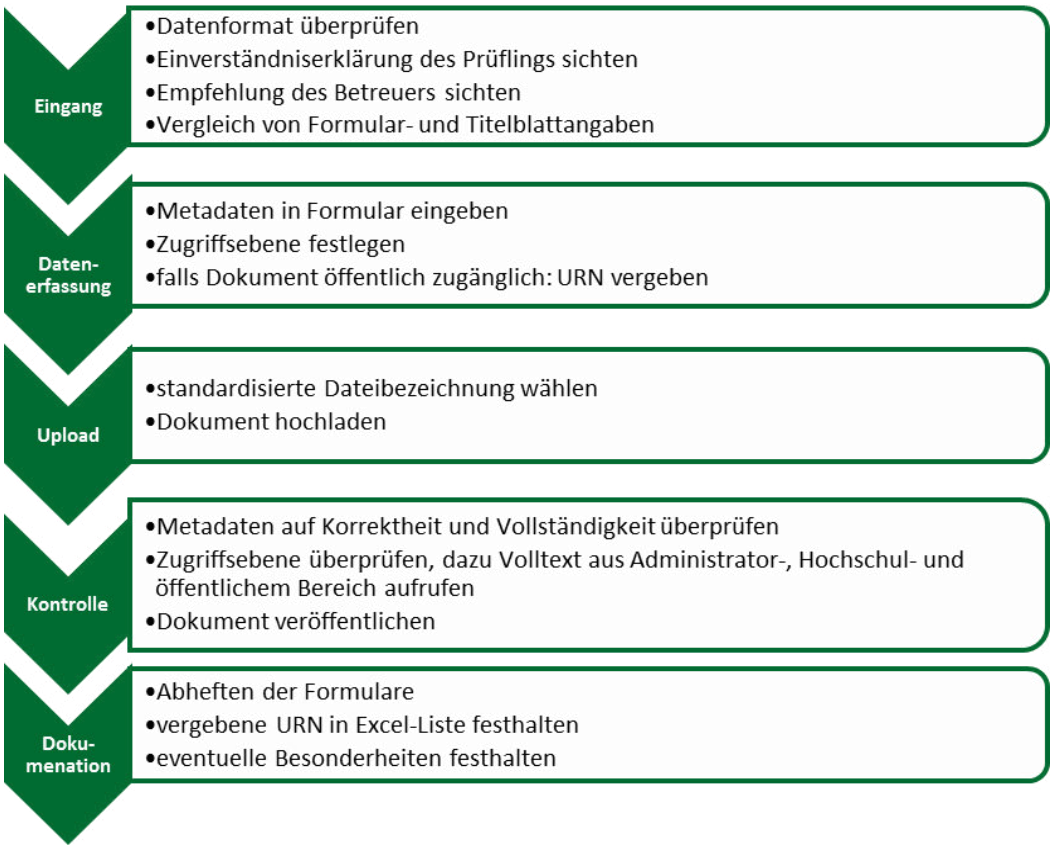

Abbildung 2: Vorschlag eines Prozessablaufmodells für Annahme und Speicherung der Abschlussarbeiten auf dem Dokumentenserver PubLIS Cologne

4.1.3 Vorgehensweise für Gutachten und eidesstattliche Erklärung

Im Folgenden werden Vorschläge gemacht, wie mit der Abgabe der eidesstattlichen Erklärung durch den Prüfling und der Einreichung des Gutachtens durch die Korrektoren im Falle einer ausschließlich digitalen Archivierung der Abschlussarbeit verfahren werden könnte.

Um die Rechtmäßigkeit der Bewertung einer Abschlussarbeit auch zu einem späteren Zeitpunkt nachvollziehen zu können, müssen die Gründe, die zu der entsprechenden Note geführt haben, dokumentiert werden. Zu diesem Zweck wird vom Erst- und vom Zweitkorrektor jeweils ein Gutachten verfasst. Zudem können direkt im Prüfungsexemplar eingetragene Randbemerkungen und Notizen der Korrektoren von Bedeutung sein. Dies ist unter anderem ein Grund dafür, warum im Moment eine gedruckte Version der Abschlussarbeit archiviert wird.[83] Um eine ausschließlich digitale Aufbewahrung möglich zu machen, müssten sich die Begründungen für die Notenvergabe auf das erstellte Gutachten beschränken. Ohnehin bestünde für die Dozenten keine Möglichkeit mehr die Arbeiten mit handschriftlichen Randbemerkungen zu versehen, wenn sie nur in elektronischer Form vorliegen. Das in Kapitel 4.3.1 vorgestellte Archivformat PDF/A erlaubt es jedoch Anmerkungen und Notizen zu erstellen, sodass die Korrektoren wei-

[83] Vgl. Keens, Walter. E-Mail an Autorin (08.05.2013)

terhin den Text direkt kommentieren können.[84] Es ist abzuwarten, welche Meinungen und Reaktionen die Einführung dieses elektronischen Korrekturverfahrens bei den prüfenden Dozenten hervorrufen würde.

Ein weiterer wichtiger Beleg bildet die eidesstattliche Erklärung, welche jeder Prüfling unterschrieben an seine Arbeit anfügen muss. Hiermit bestätigt der Studierende, dass er die Arbeit eigenständig erstellt und hierfür nur die genannten Quellen und Hilfsmittel verwendet hat.[85] Die Signierung dieser Erklärung durch den Prüfling spielt vor allem für eventuelle spätere Plagiatsvorwürfe eine Rolle, da der Studierende durch seine Unterschrift bestätigt hat, keine außer den genannten Informationen für das Schreiben der Abschlussarbeit genutzt zu haben. Wird dem Prüfling nachgewiesen, dass er ohne Kennzeichnung zitiert hat oder eine andere Person die Arbeit bzw. Teile davon hat schreiben lassen, so verstößt er damit gegen die unterzeichnete eidesstattliche Erklärung.

Nachdem das Gutachten, mit der kompletten Begründung für die jeweilige Bewertung erstellt und die eidesstattliche Erklärung abgegeben worden sind, müssen diese ebenso wie die Abschlussarbeiten zuverlässig aufbewahrt werden. Es besteht die Möglichkeit die beiden Unterlagen entsprechend der Abschlussarbeit digital zu archivieren. Dafür sollte der zugehörige Hashwert errechnet und eine qualifizierte elektronische Signatur vergeben werden. Im Falle des Gutachtens übernimmt dies der Prüfer selbst oder ein verantwortlicher Institutsmitarbeiter. Die eidesstattliche Erklärung wird vom Prüfling digital signiert. Dadurch können Authentizität und Integrität der Dokumente rechtskräftig nachgewiesen werden. Zudem bietet es sich in diesem Fall an, die Abschlussarbeit, das zugehörige Gutachten und die eidesstattliche Erklärung über ein Hashbaumverfahren miteinander zu verknüpfen. Die genannten Verfahren und deren Anwendung werden in den Kapiteln 4.3.2 und 4.3.3 erläutert.

Ist eine digitale Version des Gutachtens und auch der eidesstattlichen Erklärung nicht gewünscht, so besteht dennoch die Möglichkeit diese gedruckt und getrennt von der eigentlichen Abschlussarbeit in der Prüfungsakte aufzubewahren. Die eidesstattliche Erklärung müsste in diesem Fall zeitgleich mit der Abschlussarbeit eingereicht werden.[86] Zudem werden dann genaue Angaben zum Studierenden und zu Abschlussarbeit auf der eidesstattlichen Erklärung benötigt, um eine zuverlässige Zuordnung zur jeweiligen Prüfungsleistung zu gewähren. Da die Erklärung momentan im gedruckten, gebundenen Exemplar enthalten ist, sind dort keine weiteren Informationen zu Arbeit oder Autor aufgeführt.

4.2 Handlungsempfehlungen für Abgabe und Upload der Abschlussarbeiten

Die folgenden Empfehlungen beziehen sich nicht in erster Linie auf die eingangs erläuterten Kriterien zur vertrauenswürdigen Speicherung von Dokumenten im Allgemeinen. Vielmehr nehmen sie Bezug auf institutsspezifische Vorschriften, welche die Abgabe und Speicherung der Abschlussarbeiten am Institut für Informationswissenschaft regeln.

---

[84] Vgl. PDF-Association: FAQ zu PDF/A

[85] Vgl. Fachhochschule Köln / Fakultät für Informations- und Kommunikationswissenschaften: Informationen zur Bachelorarbeit (2013), S. 13

[86] Vgl. Keens, Walter. E-Mail an Autorin (23.07.2013)

4.2.1 Speicherung ausnahmslos aller Abschlussarbeiten

Um eine sichere Grundlage für den Nachweis der abgegebenen Abschlussarbeiten zu bilden, muss zunächst geklärt werden, welche Informationsobjekte in das Repositorium übernommen werden. Die Antwort dazu ist eindeutig: Ausnahmslos alle Abschlussarbeiten, die am Institut für Informationswissenschaft erstellt werden, müssen auf dem Dokumentenserver abgelegt werden.

Hierzu zählen natürlich die bestandenen Arbeiten der Studierenden, welche aktuell schon auf dem Repositorium abgespeichert und zum Teil veröffentlicht werden. Jedoch müssen zusätzlich einige Sonderfälle beachtet werden.

Abschlussarbeiten, welche nicht bestanden wurden, müssen ebenfalls am Institut erhalten werden. Denn es kann diesbezüglich zu Rechtsstreitigkeiten kommen, wenn z. B. ein Prüfling die Bewertung der Gutachter anzweifelt und Klage einreicht. Hierbei muss das erstellte Gutachten zur Begründung der Note ebenso wie die Abschlussarbeit selbst so aufbewahrt werden, dass die Authentizität der Dokumente erhalten bleibt. Bei einer nicht bestandenen Arbeit muss das Dokument vertraulich behandelt werden. Der Volltext und die zugehörigen Metadaten dürfen also nur über den administrativen Bereich des Systems einsehbar sein. Dennoch muss das Arbeitsergebnis nach denselben Kriterien wie veröffentlichte Arbeiten, also revisionssicher, gespeichert werden.

Eine weitere Besonderheit stellen Dokumente dar, welche in die Schriftenreihe Arbeitspapiere zur Bibliotheks- und Informationswissenschaft aufgenommen werden. Dass in diesem Fall zwei Dateien, die Prüfungsversion und die Version der Schriftenreihe gespeichert werden, wird bereits in Kapitel 3.2 erläutert und begründet. Zusätzlich ist zu empfehlen, dass hierbei nur der Teil der Schriftenreihe weltweit zugänglich gemacht wird. Die Prüfungsversion sollte nur für Administratoren einsehbar sein. Dies betrifft den Volltext, ebenso wie die Metadaten. Andernfalls würde es zu Redundanzen im Datenbestand kommen und es ist gewiss im Sinne des Prüflings und des Instituts das für die Publikation vorgesehene, optimierte Arbeitsergebnis öffentlich zur Verfügung zu stellen.

Bei nicht fristgerecht abgegebenen Arbeiten ist es fraglich, ob eine Speicherung auf dem Dokumentenserver nötig ist. Einerseits besteht die Möglichkeit das zu spät eingereichte Dokument mit einem Zeitstempel (siehe Kapitel 4.3.3) zu versehen, um die Verletzung der Frist zu dokumentieren. Beim Ablegen auf den Dokumentenserver darf der Zugriff auf Metadaten und Volltext, entsprechend den nicht bestandenen Arbeiten, nur über den redaktionellen Bereich möglich sein. Andererseits ist zu berücksichtigen, dass die verspätete Abgabe in den Prüfungsakten dokumentiert wird, wie es in § 37 der Prüfungsordnung vorgeschrieben ist.[87] Das Dokument und dessen Inhalt haben für die Bewertung keine Bedeutung mehr, da mit dem Versäumen der Abgabefrist die Abschlussarbeit automatisch als nicht bestanden gilt. Ob dennoch eine Aufbewahrung der nicht fristgemäß eingereichten Arbeiten erfolgen soll, liegt im Ermessen des Instituts für Informationswissenschaft.

4.2.2 Anpassung der Prüfungsordnung

Die Prüfungsordnungen der Bachelorstudiengänge Bibliothekswesen und Informationswirtschaft, auf welche bereits in Kapitel 3.4 Bezug genommen worden ist, regeln die

---

[87] Vgl. Prüfungsordnung für den Studiengang Bibliothekswesen mit dem Abschlussgrad „Bachelor of Arts“ der Fakultät für Informations- und Kommunikationswissenschaften der Fachhochschule Köln (vom 16.10.2008), § 37, Abs. 1

Abgabeform der Bachelorarbeiten. Diese werden herangezogen, um beispielhaft eine Anpassung der Prüfungsordnungen der am Institut für Informationswissenschaft angesiedelten Studiengänge aufzuzeigen.

In beiden BPOs wird eine Abgabe „in dreifacher Ausfertigung gebunden und in dreifacher Ausfertigung auf CD-ROM (pdf-Format)“[88] gefordert. Obwohl der Prüfling eine gedruckte und eine digitale Version abgeben muss, wird im Normalfall die Printversion als zulässiges Original angesehen. Dies gilt, da bis vor einigen Jahren überhaupt keine digitale Version gefordert wurde und da die gedruckte Fassung in der Prüfungsordnung vor der digitalen genannt wird.[89]

Würde die Prüfungsordnung jedoch in der Form angepasst werden, dass die Abschlussarbeit nur noch als digitales Dokument abgegeben werden muss und eine Printversion nicht mehr erforderlich ist, so würde die digitale Version als maßgebliche Fassung gelten. In diesem Fall ist es erforderlich, dass auch das Korrekturverfahren digital abgewickelt wird. Zudem muss die Integrität und Authentizität der Abschlussarbeit sowie der Bewertungsdokumentation gewährleistet sein. Nur so ist eine ausschließlich digitale Aufbewahrung der Abschlussarbeiten zulässig.[90] Als Alternative zum elektronischen Korrekturvorgehen kann ein umfassendes Gutachten, wie in Kapitel 4.1.3 vorgestellt, verfasst werden. Um die Aufbewahrung von zusätzlichen Printexemplaren nicht mehr erforderlich zu machen, sollte also die Prüfungsordnung in Zukunft von den Studierenden nur noch die Abgabe einer digitalen Form fordern.

Zusätzlich sollten die Anforderungen an das Dateiformat präzisiert werden. Statt lediglich die Abgabe eines PDF-Dokuments zu fordern, sollte eine Speicherung als PDF/A von den Prüflingen verlangt werden. Die Vorteile des Archivierungsformats und die Konvertierungsmöglichkeiten werden in Kapitel 4.3.1 erläutert. Somit wäre es für die Institutsmitarbeiter nicht erforderlich die Datei vor dem Hochladen auf den Dokumentenserver von PDF in PDF/A zu konvertieren. Neben dem Vorzug der Arbeitsersparnis wird dadurch vermieden, dass das abgegebene Dokument verändert werden muss. Die Datei kann also im Originalzustand und gleichzeitig in einem für die Archivierung geeigneten Format hochgeladen werden.

Ebenso besteht die Möglichkeit die genaue Dateibezeichnung vorzugeben. Hierzu könnten die bereits in Kapitel 4.1.2 vorgeschlagenen Angaben genutzt werden. Somit müsste der Prüfling seine Datei in folgender Weise benennen: Art der Abschlussarbeit_Name des Verfassers_Semesterangabe. Dadurch wäre es für die Institutsmitarbeiter nicht mehr nötig, die Datei vor dem Upload umzubenennen, was wiederum Zeit sparen würde. Des Weiteren wird durch eine solche Vereinheitlichung der eingereichten Dateien die Identifizierung und Sortierung der eingehenden Dokumente wesentlich vereinfacht.

4.3 Handlungsempfehlungen für den sicheren Erhalt der Abschlussarbeiten

Um eine vertrauenswürdige Speicherung der Abschlussarbeiten auf dem Dokumentenserver PubLIS Cologne zu erreichen, müssen vor allem technische Aspekte beachtet werden. Darum werden in den folgenden Ausführungen Empfehlungen gegeben, wie

---

[88] Ebd. und Prüfungsordnung für den Studiengang Informationswirtschaft mit dem Abschlussgrad „Bachelor of Science“ der Fakultät für Informations- und Kommunikationswissenschaften der Fachhochschule Köln (vom 01.09.2008), § 37, Abs. 1

[89] Vgl. Keens, Walter. E-Mail an Autorin (24.05.2013)

[90] Vgl. Keens, Walter. E-Mail an Autorin (08.05.2013)

die Authentizität und Integrität der Dokumente durch IT-Lösungen erhalten werden können. Die zur Beurteilung herangezogenen Kriterien werden in Kapitel 2.2 aufgelistet.

Grundsätzlich liegt die Verantwortung für den sicheren Erhalt der Abschlussarbeiten beim BSZ, da dieses den Dokumentenserver hostet und damit technisch betreut. Dennoch gibt es einige Hinweise, die vom Institut für Informationswissenschaft selbst beachtet und durchgeführt werden sollten.

4.3.1 Speicherung der Dokumente im PDF/A-Format

Wie bereits in Kapitel 4.2.2 erwähnt schreiben die Prüfungsordnungen der Studiengänge Bibliothekswesen und Informationswissenschaft eine Abgabe der Abschlussarbeiten im PDF vor. Ebenso wird in Kapitel 2.2 darauf verwiesen, dass der Nestor-Kriterienkatalog und das DINI-Zertifikat eine Speicherung von formatierten Texten im PDF/A-Standard empfehlen. Im Folgenden wird dargelegt, was sich hinter dem Begriff PDF/A verbirgt, welche Vorteile dieses Format bietet und warum eine Ablieferung der Abschlussarbeiten als PDF/A-Dateien gefordert werden sollte.

Zunächst ist zu klären, welche Eigenschaften das PDF, welches 1993 von der Firma Adobe veröffentlicht wurde[91], allgemein auszeichnet. „PDF (Portable Document Format) ist ein Dokumentformat, bei dem neben der Strukturinformation von elektronischen Dokumenten auch wesentliche Layout-Informationen mitgespeichert werden.“[92] Das konkrete Aussehen des Dokuments wird über eine binäre Datenreihe beschrieben, was zu einer relativ geringen Dateigröße führt und zu einer festen Bestimmung des Erscheinungsbildes. [93] Dadurch ist es nicht möglich eine PDF-Datei in einem Texteditor zu bearbeiten. Die Datei ist also schreibgeschützt.[94] Zudem wird es ermöglicht, das Dokument unabhängig von der Software, mit der die PDF-Datei erzeugt worden ist, stets in gleicher Weise darzustellen. Um dies zuverlässig zu gewährleisten, können die verwendeten Schriftarten in die Datei eingebettet werden, sodass sie unabhängig von der verwendeten Lesesoftware stets korrekt wiedergegeben werden.[95] Zusammenfassend bestehen die wesentlichen Vorteile des PDFs in der schreibgeschützten und bildlich korrekten Speicherung von Dokumenten mit Text- und Bildanteilen.

Beim PDF/A (PDF/Archivierung) handelt es sich um eine Spezifizierung des PDFs, welche 2002 von einer Arbeitsgruppe in den USA entwickelt wurde. An der Entstehung beteiligten sich unter anderem Bundesbehörden sowie Vertreter aus dem Bibliotheks- und Archivbereich und der Industrie. Als Ergebnis dieser Kooperation wurde am 1. Oktober 2005 der PDF/A-1-Standard auf der PDF-Version 1.4 basierend als ISO 19005-1 von der International Organization for Standardization (ISO) veröffentlicht. Dadurch wurde zum ersten Mal ein Dateiformat für die digitale Langzeitarchivierung in einem Standard festgelegt.[96]

Der Standard wurde 2011 um die Weiterentwicklung PDF/A-2 als ISO 19005-2 ergänzt, welchem die PDF-Version 1.7 zugrunde liegt. Dieser zweite Normteil ergänzt den Standard unter anderem um die Möglichkeit digitale Signaturen in Übereinstim-

---

[91] Vgl. Borghoff, Uwe M.; Rödig, Peter; Scheffczyk, Jan; Schmitz, Lothar: Langzeitarchivierung (2003), S. 112
[92] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge (2009), S. 2887
[93] Vgl. ebd., S. 2887–2888
[94] Vgl. Borghoff, Uwe M.; Rödig, Peter; Scheffczyk, Jan; Schmitz, Lothar: Langzeitarchivierung (2003), S. 113
[95] Vgl. ebd., S. 112
[96] Vgl. Oettler, Alexandra: PDF/A kompakt 2.0 (2013), S. 7

mung mit dem PAdES-Standard in die PDF/A-Datei einzubetten.[97] Hinter dieser Abkürzung verbirgt sich ein Bündel an Standards bezüglich der Kombination von PDF-Dateien und elektronischen Signaturen. Diese werden unter dem Begriff PDF Advanced Electronic Signatures (PAdES) zusammengefasst und sollen eine zuverlässige Langlebigkeit digitaler Signaturen in Verbindung mit PDF-Dateien unterstützen.[98] Die Erklärung des Begriffs digitale Signaturen erfolgt in Kapitel 4.3.3.

Im Jahr 2012 erfolgte wiederum die Veröffentlichung der aktuellsten Version PDF/A-3 als ISO 19005-3. Diese ermöglicht die Einbindung von PDF-Dateien oder anderen Dateiformaten in die PDF/A-Datei. Somit kann z. B. die ursprüngliche Textverarbeitungsdatei eingebettet werden. Allerdings wird hierbei keine Garantie für die Langzeitverfügbarkeit der eingefügten Dateien gegeben.[99]

Nun wird dargelegt, welche zusätzliche Eignung für die Archivierung PDF/A gegenüber PDF aufweist. Bei der Verwendung von PDF/A sind einige Vorgehensweisen, die der Langzeiterhaltung schaden könnten, nicht möglich und es wird eine strengere Einhaltung von Vorgaben zur zuverlässigen visuellen Darstellung gefordert. Somit ist es nicht erlaubt, das Dokument per Passwortvergabe zu schützen, da es sonst zu einem späteren Zeitpunkt unter Umständen nicht mehr zugänglich ist. Es wurde bereits angesprochen, dass PDF die Möglichkeit bietet Schriftarten einzubetten. Bei der Verwendung von PDF/A werden alle verwendeten Schriften in die Datei eingebettet, um eine einwandfreie Wiedergabe auch in einer anderen Softwareumgebung zu gewährleisten. Entsprechend werden auch die genutzten Farben nach international festgelegten Farbschemata gekennzeichnet und wiedergegeben.[100]

Durch öffentliche Festschreibung des Formats in einem ISO-Standard können PDF/A-Dokumente plattformunabhängig von einer Vielzahl von frei verfügbaren Programmen dargestellt werden, wodurch der Nutzer unabhängig von einem bestimmten Softwarehersteller ist. Einen speziellen Vorteil für digitale Archive bietet die Einheitlichkeit des Dateiformats, was automatisierte Vorgänge vereinfachen kann, ebenso wie die mögliche Volltextsuche in den Dokumenten.[101] Um die Auffindbarkeit der Dokumente zu unterstützten werden ferner Metadaten vergeben. Hierbei ist lediglich die Belegung des Metadatenfelds PDF/A-Kennung Pflicht, was jedoch zumeist vom Konvertierungsprogramm automatisch belegt wird. Dennoch empfiehlt es sich zusätzliche Informationen anzugeben, um dadurch die Recherche- und Sortiermöglichkeiten zu erweitern. Zusätzlich müssen alle Metadaten so vorliegen, dass sie mit dem Format Extensible Metadate Platform (XMP) kompatibel sind. XMP ist ein Metadatenformat, welches die Integration der Metadaten in die Binärstruktur der PDF/A-Datei ermöglicht.[102]

Die genannten Eigenschaften tragen dazu bei, dass sich der Standard PDF/A sehr gut eignet, um Dokumente für eine lange Zeit aufzubewahren und lesbar zu erhalten.

Zudem werden bei PDF/A unterschiedliche Konformitätsstufen unterschieden. Während Konformitätsstufe B, welche für Basic steht und je nach Normteil die Dateibezeichnung PDF/A-1b, PDF/A-2b oder PDF/A-3b trägt, lediglich die eindeutige visuelle Wiedergabe des Dokuments gewährleistet, stellt Konformitätsstufe A zusätzlich die inhaltliche Struktur des Dokuments in der vorgegebenen Lesereihenfolge dar. [103] Dies

---

[97] Vgl. ebd., S. 18
[98] Vgl. European Telecommunications Standards Institute: ETSI – PDF Advanced Electronic Signature (PAdES) FAQ
[99] Vgl. Oettler, Alexandra: PDF/A kompakt 2.0 (2013), S. 8
[100] Vgl. ebd., S. 6
[101] Vgl. 3rd international PDF/A Conference, 2009, S. 32
[102] Vgl. Drümmer, Olaf; Oettler, Alexandra; Seggern, Dietrich von: PDF/A kompakt (2007), S. 48
[103] Vgl. Oettler, Alexandra: PDF/A kompakt 2.0 (2013), S. 8

wird durch die Vergabe von Tags realisiert. Außerdem wird die uneingeschränkte Zugänglichkeit z. B. durch alternative Bildunterschriften und der Abbildung jeglicher verwendeter Buchstaben im Unicode-Standard unterstützt. Mit der Verwendung von Konformitätsstufe A wird eine vollständige Übereinstimmung der PDF/A-Dateien unabhängig von der darstellenden Software erreicht.[104] Das A steht hierbei für Accessible und die jeweilige Datei wird je nach Verwendung der unterschiedlichen Standards mit PDF/A-1a, PDF/A-2a oder PDF/A-3a benannt.[105]

Zur Erstellung der PDF/A-Dateien bietet sich den Prüflingen die Möglichkeit, dies direkt aus einer Textverarbeitungsdatei heraus zu tun. Hierzu bieten mit Open Office, Libre Office sowie Microsoft Office ab der Version von 2007 die gängigsten Textverarbeitungsprogramme eine Konvertierungsfunktion an.[106] Obwohl die Datei direkt aus dem Office-Programm heraus als PDF/A-Dokument abgespeichert werden kann, garantiert dies dennoch nicht, dass das erstellte PDF/A-Dokument dem Originaldokument hundertprozentig, sowohl inhaltlich als auch optisch, entspricht. Daher ist stets eine Kontrolle der erzeugten Archivdatei erforderlich.[107]

Ist die Abschlussarbeit als PDF/A-Dokument beim Institut für Informationswissenschaft eingereicht worden, so muss vor dem Upload auf den Dokumentenserver überprüft werden, ob es sich tatsächlich um eine PDF/A-Datei handelt. Denn auch wenn das Dokument korrekt in eine PDF/A-Datei konvertiert wurde, so kann es dennoch vorkommen, dass die Datei durch beabsichtigte oder unbeabsichtigte Vorkommnisse verändert wurde und nicht mehr dem Standard entspricht. Dies kann nicht durch die bloße Betrachtung der Dateiendung festgestellt werden.[108] Für eine solche Validierung muss entsprechende Software herangezogen werden, die von unterschiedlichen Anbietern auf dem Markt angeboten wird. Eine Auflistung aktueller Programme ist auf der Website der PDF-Association zu finden.[109]

Im Folgenden wird lediglich eine Auswahl von zwei Anwendungen vorgestellt. Beim Einsatz des Programms Adobe Acrobat Pro ist ab Version 8 das Modul Preflight integriert, welches PDF/A-Dateien erstellen und überprüfen kann. Bei einer fehlgeschlagenen Validierung erhält der Anwender bei diesem Programm eine Auflistung der festgestellten Verstöße gegen den Standard mit weiterführenden Informationen.[110] Als weiteres Validierungsprogramm soll hier pdfaPilot, ein Produkt der Callas Software GmbH, genannt werden. Dieses Programm, welches als eigenständige Desktopanwendung oder als Plug-In für Adobe genutzt werden kann[111], bietet ebenfalls die Möglichkeit zur Erzeugung und Validierung von PDF/A-Dateien. Auch hier werden bei einer nichtkonformen Datei die Fehlermeldungen aufgelistet. Zusätzlich ist es bei geringen Abweichungen durch ein Reparaturtool möglich, die Dateien automatisiert in ein gültiges PDF/A umzuwandeln. Bei gravierenden Problemen werden Hinweise aufgezeigt, in welcher Weise die Originaldatei angepasst werden muss, um diese in ein standardkonformes PDF/A konvertieren zu können.[112]

---

[104] Vgl. Drümmer, Olaf; Oettler, Alexandra; Seggern, Dietrich von: PDF/A kompakt (2007), S. 13
[105] Vgl. Oettler, Alexandra: PDF/A kompakt 2.0 (2013), S. 8
[106] Vgl. ebd., S. 7
[107] Vgl. 3rd international PDF/A Conference, 2009, S. 36
[108] Vgl. Drümmer, Olaf; Oettler, Alexandra; Seggern, Dietrich von: PDF/A kompakt (2007), S. 36
[109] Vgl. Merz, Thomas: Validierung von PDF/A (2011)
[110] Vgl. Drümmer, Olaf; Oettler, Alexandra; Seggern, Dietrich von: PDF/A kompakt (2007), S. 38
[111] Vgl. Callas Software GmbH: pdfaPilot – PDF/A-Unterstützung für Einsteiger, als Standalone oder in Acrobat (2013)
[112] Vgl. Drümmer, Olaf; Oettler, Alexandra; Seggern, Dietrich von: PDF/A kompakt (2007), S. 39

Nach einer positiven Validierung kann das Dokument in das Repositorium aufgenommen werden. Werden Abweichungen vom ISO-Standard festgestellt, so können diese, wie bereits beschrieben, mithilfe der Software behoben werden oder die PDF/A-Datei kann neu erstellt und schließlich hochgeladen werden.[113]

4.3.2 Angabe von Hashwerten zur Sicherung der Integrität der Dokumente

Um die Integrität der im Repositorium enthaltenen Dokumente zu erhalten, wird in Kapitel 2.2 die Vergabe von Hash-Werten empfohlen. Des Weiteren ist bereits erwähnt worden, dass die Abschlussarbeiten vor der Speicherung beim BSZ mit Prüfsummen nach MD5 und SHA-512 versehen werden (siehe Kapitel 3.3.2).

In diesem Kapitel soll zunächst erläutert werden, was Einweg-Hashfunktionen und daraus errechnete Hashwerte sind und welchen Einsatzmöglichkeiten Sie im Hinblick auf die Aufbewahrung der Abschlussarbeiten und in Verbindung mit elektronischen Signaturen haben.

„Eine Hashfunktion ist eine Rechenvorschrift, durch die eine Eingabe beliebiger Länge in einen Ausgabewert fester (im Allgemeinen kürzerer) Länge umgewandelt wird.“[114] Die genannte Eingabe einer beliebig langen Bitfolge kann z. B. ein PDF/A-Dokument sein, dessen binärer Aufbau bereits in Kapitel 4.3.1 erwähnt worden ist. Der Ausgabewert entspricht ebenfalls einer Abfolge von Bits. Dies ist der sogenannte Hashwert. Da es sich um eine Einweg-Hashfunktion handelt, wirkt diese nur in eine Richtung. Aus einem Dokument lässt sich also leicht der Hashwert errechnen. Umgekehrt ist es sehr schwierig bzw. fast unmöglich aus einem Hashwert die Ausgangsdaten herzuleiten.[115] Zusätzlich muss es ebenso annähernd unmöglich sein, ein Dokument zu finden, aus welchem der gleiche Hashwert wie der vorliegende resultiert. Diese Eigenschaft wird als Kollisionswiderstand bezeichnet.[116] Die Gewährleistung der Sicherheit des Hashverfahrens, und kryptographischer Verfahren allgemein, beruht nicht darauf, ein ungewöhnliches, geheimes Vorgehen zu entwickeln und anzuwenden, sondern die Anzahl der möglichen Ergebnisse so groß zu halten, dass es nicht möglich ist alle auszuprobieren.[117]

Die Vorgehensweise bei der Prüfung der Integrität eines Dokuments mithilfe eines Hashwerts wird im Folgenden erläutert und durch Abbildung 3 illustriert.

Bevor ein Dokument d auf eine Datenbank geladen wird, wird mittels einer Hashfunktion h der Hashwert des Dokuments d als # errechnet. Dieser sogenannte digitale Fingerabdruck wird abgespeichert. Es ist zu empfehlen für die Aufbewahrung der Hashwerte einen zuverlässigen, separaten Server zu nutzen.[118] Wenn nun eine Person überprüfen möchte, ob das Dokument nicht verändert wurde, so ruft sie es auf und erzeugt erneut einen Hashwert mit derselben Hashfunktion h. Da die vollständige Übereinstimmung mit dem Originaldokument nicht sicher ist, wird das zu prüfende Dokument mit d‘ bezeichnet. Das Ergebnis des Hashverfahrens ist der Hashwert #‘. Die bei-

---

[113] Vgl. Oettler, Alexandra: PDF/A kompakt 2.0 (2013), S. 12
[114] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge (2009), S. 3493
[115] Vgl. ebd., S. 3493
[116] Vgl. ebd., S. 2298
[117] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 2
[118] Vgl. Fromm, Niels: Signatur und Zeitstempel zur Wahrung von Authentizität und Integrität (2009), S. 66

den Hashwerte # und #‘ werden nun miteinander verglichen. Sind sie identisch, so kann man sicher sein, dass das Dokument im Originalzustand vorliegt.[119]

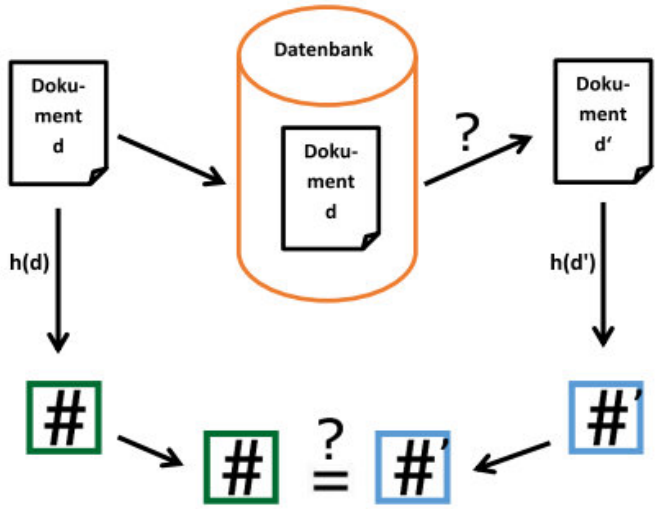

Abbildung 3: Vergabe und Überprüfung von Hashwerten

Vom Bundesamt für Sicherheit in der Informationstechnik wird diese Maßnahme zur Integritätssicherung mit einer mittleren Zuverlässigkeit bewertet. Stellt man bei der Überprüfung der beiden Hashwerte fest, dass sie nicht übereinstimmen, so kann man zwar schlussfolgern, dass die Datei manipuliert wurde. Auf welche Art und in welchem Umfang die Veränderung vorliegt, kann jedoch nicht festgestellt werden.[120]

Im Falle der Abschlussarbeiten am Institut für Informationswissenschaft würde eine Abweichung der beiden Hashwerte konkret bedeuten, dass die Datei nicht mit der ursprünglichen Version des Prüflings übereinstimmt, man allerdings die Originaldatei nicht wiederherstellen kann. Nichtsdestotrotz bietet die Errechnung von Hashwerten eine zuverlässige Möglichkeit, um die Integrität von nicht-manipulierten Dateien zu beweisen.

Zum Errechnen von Hashwerten werden unterschiedliche Einweg-Hashfunktionen genutzt. Es ist bereits erwähnt worden, dass vom BSZ Hashwerte nach den Verfahren MD5 und SHA-512 erzeugt werden. Beide zählen zu den eigenständigen Hashfunktionen und werden im Folgenden kurz vorgestellt und bewertet. Da die Vergabe der Hashwerte vom BSZ übernommen wird und deshalb nicht direkt am Institut vorgenommen werden wird, beschränken sich die nachfolgenden Ausführungen auf Basisinformationen.

Message Digest zählt zu den ersten Hashfunktionen überhaupt und bildete die Grundlage für viele weitere Methoden. Die neueste Version Message Digest 5 (MD5) wurde bereits 1992 vorgestellt und erzeugt einen Hashwert mit einer Länge von 128 Bit. In den letzten Jahren wurden erheblich Sicherheitsschwächen festgestellt. So ist es mög-

[119] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 96

[120] Vgl. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge (2009), S. 3212–3213

lich innerhalb von einer Stunde auf einem PC mehrere Dokumente mit dem gleichen Hashwert zu finden.[121] Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bescheinigt MD5 Sicherheitsmängel.[122]

Allgemein kann die Sicherheit eines Hashwerts vor allem durch seine Länge ausgedrückt werden. So können Hashwerte mit einem Umfang von weniger als 128 Bit als nicht zuverlässig eingestuft werden, da sonst der Kollisionswiderstand nicht mehr gewährleistet werden kann.[123] Eine Verwendung von Hashwerten mit einer längeren Zeichenfolge, wie sie die folgende Hashfunktion SHA erzeugt, ist zu empfehlen.

Die Hashfunktion Secure Hash Algorithm (SHA) wurde 1993 von der National Security Agency entwickelt und in den Jahren 2001 und 2002 um SHA-2 ergänzt. SHA-2 besteht aus den beiden Funktionen SHA-256 und SHA-512, welche Hashwerte mit einer Bitlänge von 256 bzw. 512 Bit erzeugen.[124] Im Gegensatz zu SHA-1 sind für SHA-2 noch keine erfolgreichen Angriffe durchgeführt worden. Zudem unterstützt das National Institute of Standards and Technology die kontinuierliche Weiterentwicklung der Hashfunktion.[125]

Die folgende Erläuterung soll lediglich einen kurzen Einblick in die prinzipielle Arbeitsweise von Hashfunktionen geben. Sowohl MD5 als auch SHA arbeiten mit einer Aufteilung der Datenmenge in Blöcke von je 512 Bit, welche wiederum in die kleinere Einheit Wörter unterteilt werden. Jeder dieser Blöcke wird in unterschiedlich vielen Runden, durch einen Algorithmus komprimiert bis die festgelegte Länge des Hashwerts erreicht ist. MD5 führt 64 und SHA-2 80 Runden durch.[126] Wie bereits erwähnt, ergibt sich das Maß der Sicherheit nicht ausschließlich durch die Art der Errechnung des Hashwerts, sondern ebenso durch dessen Länge.

Das Hashverfahren bietet außerdem die Möglichkeit, mehreren Dokumenten einen gemeinsamen Hashwert zuzuordnen. Dies wird über einen sogenannten Hashbaum oder auch Merkle-Baum, nach dem Erfinder Ralph Merkle benannt, realisiert. Hierbei wird für jedes Dokument, z. B. für die Abschlussarbeit selbst und das zugehörige Gutachten, ein eigener Hashwert berechnet. Aus den Hashwerten der beiden Dokumente wird nun wiederum ein Hashwert gebildet. Abbildung 4 zeigt einen solchen, allerdings sehr kleinen, Hashbaum. $Hash_3(h_1|h_2)$ wird aus $Hash_1(a)$, dem Hashwert der Abschlussarbeit, und $Hash_2(g)$, dem Hashwert des Gutachtens, erzeugt. Die beiden untergeordneten Hashwerte werden als Kinder des oberen Hashwerts bezeichnet. Nun kann man z. B. durch das digitale Signieren des obersten Hashwerts und die zusätzliche Vergabe eines Zeitstempels beweisen, dass die untergeordneten Dokumente zu einem bestimmten Zeitpunkt in einem bestimmten Zustand vorlagen und seitdem nicht verändert wurden.[127] Somit besteht die Möglichkeit die Abschlussarbeit mit der zugehörigen Bewertung in Form des Gutachtens zu verketten und deren Integrität zu gewährleisten. Die Vorgehensweise beim digitalen Signieren wird im folgenden Kapitel 4.3.3 erläutert.

---

[121] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 101–102

[122] Vgl. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge (2009), S. 3654

[123] Vgl. ebd., S. 720

[124] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 102

[125] Vgl. ebd., S. 106

[126] Vgl. ebd., S. 103–106

[127] Vgl. Neuroth, Heike; Oßwald, Achim; Scheffel, Regine; Strathmann, Stefan; Huth, Karsten: Nestor-Handbuch (2010), S. 5:12-5:13

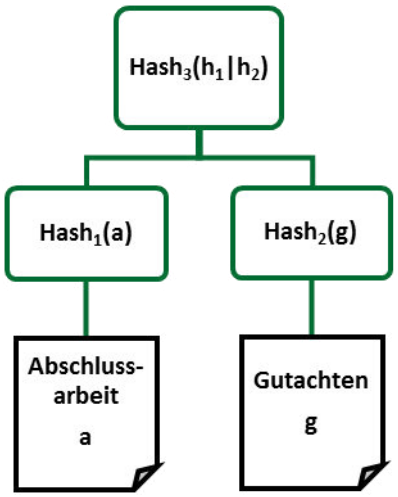

Abbildung 4: Anwendung eines Merkle-Hashbaums für die Integritätserhaltung der Abschlussarbeiten und der zugehörigen Gutachten

Dennoch wird im DINI-Zertifikat darauf hingewiesen, dass die alleinige Berechnung eines Hashwerts rechtlich keine Aussagekraft hat. Theoretisch könnte nämlich bei einer willentlichen Manipulation eines Dokuments auch dessen Hashwert verändert worden sein. Wie bereits erwähnt, kann bei einer Überprüfung keine Aussage darüber getroffen werden, inwieweit das Dokument verändert wurde. DINI empfiehlt für den zuverlässigen Nachweis von Integrität die zusätzliche Vergabe von digitalen Signaturen und Zeitstempeln.[128]

Somit kann als Empfehlung angegeben werden, dass die Erzeugung von Hashwerten auf jeden Fall weitergeführt werden sollte. Hierbei sollte das Augenmerk auf besonders zuverlässige Hashfunktionen gelegt werden. Die Verwendung von SHA-512 bietet mit einer Hashwertlänge von 512 Bit eine solide Absicherung. MD5 dagegen sollte durch eine sicherere Methode ersetzt werden. Es stellt sich ohnehin die Frage, ob die Vergabe von zwei Hashwerten sinnvoll und nötig ist. Wenn z. B. nur ein Hashwert dem des ursprünglichen Dokuments entspricht, so wird die Integrität dadurch nicht bestätigt. Des Weiteren wird die zusätzliche Vergabe von elektronischen Signaturen und Zeitstempeln befürwortet, welche im folgenden Kapitel 4.3.3 beschrieben wird.

4.3.3 Vergabe von qualifizierten elektronischen Signaturen zur Gewährleistung der Authentizität der Dokumente

Authentizität bedeutet, wie bereits in Kapitel 2.2 erläutert, die Sicherheit, dass das Dokument von der angegebenen Quelle stammt und zum vorgegebenen Zeitpunkt verfasst wurde. Im Alltag wird die Authentizität eines Dokuments durch eine handschriftliche Unterzeichnung und die Angabe eines Datums bestätigt.

Hierbei übernimmt die Unterschrift stets eine der folgenden Funktionen. Bei der Identifikationsfunktion wird Auskunft über die Identität des Unterzeichners gegeben. Wenn eine Unterschrift bestätigt, dass das vorliegende Dokument dem Unterzeichner vorgelegen hat und von ihm anerkannt worden ist, so handelt es sich um die Echtheits-

[128] Vgl. Deutsche Initiative für Netzwerkinformation e.V. / Arbeitsgruppe Elektronisches Publizieren: DINI-Zertifikat (2011), S. 42–43

funktion. Die weiteren Funktionen Warnung und Abschluss sind für den vorliegenden Fall nicht von Bedeutung.[129]

Um jene Authentizität auch bei digitalen Dokumenten zu gewährleisten und glaubwürdig nachzuweisen, besteht die Möglichkeit die Abschlussarbeiten mit elektronischen Signaturen[130] und entsprechenden Zeitstempeln zu versehen, wie es vom Nestor-Kriterienkatalog empfohlen wird (siehe Kapitel 2.2).[131]

Im folgenden Kapitel werden zunächst die rechtlichen Rahmenbedingungen von Dokumenten mit qualifizierten elektronischen Signaturen beleuchtet und die Vorgehensweise erläutert. Schließlich werden konkrete Vorschläge für eine mögliche Realisierung am Institut für Informationswissenschaft gemacht.

Im juristischen Zusammenhang spielt die Beweisfähigkeit digitaler Dokumente und somit der Begriff Verbindlichkeit eine wichtige Rolle. Verbindlichkeit bedeutet, „dass auch gegenüber Dritten eindeutig nachgewiesen werden kann, wer der Autor einer Nachricht war."[132] In Bezug auf Abschlussarbeiten ist gemeint, dass ein Prüfling nicht abstreiten kann, eine Arbeit verfasst und schließlich unterschrieben bzw. eine digitale Arbeit erstellt und elektronisch signiert zu haben. Deshalb kann statt Verbindlichkeit auch der Begriff Nicht-Abstreitbarkeit genutzt werden. Verbindlichkeit setzt Authentizität und damit Integrität eines Dokuments voraus. Die beiden letzteren Eigenschaften können folglich unter dem Begriff Verbindlichkeit zusammengefasst werden.[133]

Gesetzliche Regelungen, die die Verbindlichkeit digitaler Dokumente betreffen, finden sich unter anderem im Bürgerlichen Gesetzbuch (BGB). § 126a BGB schreibt vor, dass, wenn „die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden [soll], so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen."[134]

Auch in den IT-Grundschutz-Katalogen des Bundesamts für Sicherheit in der Informationstechnik wird digitalen Signaturen nach dem Signaturgesetz eine hohe Beweissicherheit vor Gericht zugestanden. Demnach kann eine digital signierte Datei und die darin enthaltenen Aussagen dem Signierenden verbindlich zugeordnet werden.[135]

Weiterhin wird in § 371a Satz 2 der Zivilprozessordnung (ZPO) festgelegt, dass elektronische Dokumente, „die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind"[136], in ihrer Beweiskraft öffentlichen Urkunden entsprechen.[137]

Um eine solche öffentliche Behörde handelt es sich auch bei der Fachhochschule Köln, welche als Prüfungsbehörde die Abschlussarbeiten der Studierenden entgegennimmt, die Bewertung vornimmt und die entsprechenden Prüfungsergebnisse ausgibt. Bei Abgabe der Abschlussarbeit geht diese in den Besitz der Fachhochschule über und erhält so den Rechtscharakter einer amtlichen Urkunde mit Beweisfunktion. Im Gegen-

---

[129] Vgl. Eckert, Claudia: IT-Sicherheit (2012), S. 392

[130] Die Begriffe elektronische und digitale Signatur werden im Folgenden synonym verwendet.

[131] Vgl. Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 25

[132] Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 17

[133] Vgl. ebd.

[134] Bürgerliches Gesetzbuch (vom 02.01.2002), § 126a

[135] Vgl. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge (2009), S. 2301

[136] Zivilprozessordnung (vom 05.12.2005), § 371a Satz 2

[137] Vgl. ebd., § 371a Satz 2

satz zu privaten Urkunden, welche ebenfalls Beweiszwecken dienen, werden die Prüfungsarbeiten bei der öffentlichen Behörde, in diesem Fall dem Prüfungsamt der Fachhochschule Köln, verwahrt.[138] Folglich ist die Fachhochschule für den korrekten Erhalt der Originaldokumente verantwortlich, um im Falle einer Rechtsstreitigkeit die Beweiskraft dieser Dokumente eindeutig nachweisen zu können.

Es kann als Schlussfolgerung festgehalten werden, dass digitale Dokumente, wenn sie als ursprünglich digitale Dokumente mit qualifizierter elektronischer Signatur versehen vorliegen, laut BGB und ZPO im Bereich der Beweiskraft gleichwertig gegenüber handschriftlich unterschriebenen Printdokumenten sind.[139]

Wie aus den oben beschriebenen Gesetzesauszügen ersichtlich wird, liegt die Beweisfähigkeit bei digitalen amtlichen Urkunden eben nur dann vor, wenn eine qualifizierte elektronische Signatur vergeben worden ist.

Die entsprechende Empfehlung des Nestor-Kriterienkatalogs lautet wie folgt: „Das dLZA [digitale Langzeitarchiv, Anmerkung der Autorin] registriert sich bei einer autorisierten Stelle, z. B. bei der Regulierungsbehörde für Post- und Telekommunikation, und erhält dort ein digitales Signaturschlüssel-Zertifikat, welches es zum Erzeugen digitaler Signaturen benutzt.“[140]

Im Folgenden wird nun erläutert, was eine elektronische Signatur ist, welche Aussagekraft sie besitzt und welche Eigenschaften sie zu einer qualifizierten elektronischen Signatur machen.

Die Vergabe von elektronischen Signaturen und den entsprechenden Zertifikaten wird im Signaturgesetz (SigG) geregelt. In diesem Gesetzestext ist auch der Begriff qualifizierte elektronische Signatur definiert, was eine besonders sichere Form der digitalen Signatur ist. Es handelt sich dabei nämlich um eine elektronische Signatur, welche sich auf ein gültiges qualifiziertes Zertifikat beruft und mit einer sicheren Softwarekomponente erstellt wurde.[141]

Ein Zertifikat übernimmt die Funktion eines Ausweises, da es die Identität einer Person und deren Zugehörigkeit zu einer bestimmten Gruppe bestätigt. Konkret handelt es sich dabei um einen Datensatz, der Informationen über den Schlüsselinhaber enthält und von einer Zertifizierungsstelle, auch Certification Authority (CA) genannt, erstellt wird. Die enthaltenen Angaben sind: die ausstellende Behörde, Name, Geburtstag und Adresse der Person sowie deren eigenhändige Unterschrift und die Gültigkeitsdauer. Zudem sind Merkmale zum Fälschungsschutz enthalten.[142] Um ein solches Zertifikat zu erhalten, muss sich die Person zunächst bei der CA ausweisen.[143] Diese Zertifizierungsstellen müssen laut SigG bestimmte Anforderungen erfüllen und erhalten die zu vergebenden qualifizierten Zertifikate von der zuständigen, übergeordneten Behörde.[144] Bei dieser Behörde handelt es sich um das BSI, welches die CAs zertifiziert und akkreditiert.[145]

---

[138] Vgl. Keens, Walter. E-Mail an Autorin (24.05.2013)
[139] Vgl. Odenthal, Roger: Digitale Archivierung (2007), S. 38
[140] Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung: Nestor-Kriterien (2008), S. 25
[141] Vgl. Signaturgesetz (vom 17.07.2009), § 2 Nr. 1–3
[142] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 167–168
[143] Vgl. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge (2009), S. 2302–2303
[144] Vgl. Signaturgesetz (vom 17.07.2009), § 16 Abs. 1
[145] Vgl. Fromm, Niels: Signatur und Zeitstempel zur Wahrung von Authentizität und Integrität (2009), S. 64

Das Signaturgesetz sieht weiterhin vor, dass nur natürliche Personen Inhaber eines Signaturschlüssels sein können.[146] Demnach ist die oben genannte Empfehlung im Nestor-Kriterienkatalog hinfällig, wonach Institutionen ein qualifiziertes Zertifikat beantragen sollten, um als juristische Person Signaturen vergeben zu können.

Dieser Umstand hat im Bankenwesen bereits dazu geführt, dass in einem Brief des Zentralen Kreditausschusses an den Vorsitzenden des Finanzausschusses des Deutschen Bundestags eine Alternative zur elektronischen Signatur gefordert wird, welche bei gleichbleibenden Sicherheitsstandards von einer juristischen Person, also z. B. einem Institut, vergeben werden kann. Hierbei könnte sich die Organisation beispielsweise durch einen Eintrag in einem entsprechenden Register identifizieren.[147]

Beim konkreten Signieren eines Dokuments wird folgendermaßen vorgegangen. Der Möglichkeit zur Vergabe von elektronischen Signaturen liegt das Prinzip einer asymmetrischen Verschlüsselung zugrunde. Dabei handelt es sich um ein Schlüsselpaar, welches aus einem privaten und einem zugehörigen öffentlichen Schlüssel besteht.[148] Ein Schlüssel, auch Key genannt, ist eine Abfolge von Bits, welche mithilfe eines bestimmten Algorithmus die Daten eines Dokuments verschlüsselt und dadurch eine eindeutige Kennzeichnung erzeugt, welche das Dokument identifiziert.[149] Eine elektronische Signatur ist das Ergebnis einer solchen Verschlüsselung.

In der Praxis wird meist nicht das Dokument selbst, sondern ein zuvor errechneter Hashwert verschlüsselt. Dies ist eine wirtschaftlichere Vorgehensweise, da es sich bei Dokumenten im Gegensatz zu Hashwerten in der Regel um größere Datenmengen mit unterschiedlicher Länge handelt. Diese müssten stets komplett verschlüsselt werden.[150] Durch die Kombination von Hashwerten und digitalen Signaturen können Authentizität und Integrität zugleich nachgewiesen werden. Die Vorgehensweise beim Erstellen von Hashwerten wird im Kapitel 4.3.2 erläutert.

Oft wird unter dem Begriff der Verschlüsselung eine Maßnahme für die Geheimhaltung von Nachrichten verstanden und es besteht durchaus die Möglichkeit den Schlüssel für diesen Zweck zu nutzen. Für den Fall der Abschlussarbeiten wäre eine solche Verschlüsselung jedoch äußerst ungünstig, da die Dokumente unter Umständen nicht mehr entschlüsselt und daraufhin auch nicht mehr gelesen werden könnten. Die folgenden Ausführungen beziehen sich deshalb ausschließlich auf die Funktion der Authentifikation durch asymmetrische Schlüsselpaare.

Zunächst erhält eine Person auf Antrag und nach ihrer Identifizierung von der CA ein Schlüsselpaar mit einem öffentlichen Schlüssel und einem privaten Schlüssel, auf welchen nur sie zugreifen kann.[151] Der Schlüsselinhaber, also der Unterzeichner, erstellt mit diesem privaten Schlüssel eine Signatur, um sein Dokument eindeutig als von ihm verfasst zu kennzeichnen. Ob diese digitale Signatur echt ist, kann von jeder beliebigen Person mithilfe des passenden öffentlichen Schlüssels desselben asymmetrischen Schlüsselpaares geprüft werden. Um sicherzustellen, dass der Prüfende den richtigen

---

[146] Vgl. Signaturgesetz (vom 17.07.2009), § 2 Nr. 9

[147] Vgl. Zentraler Kreditausschuss: Brief des Zentralen Kreditausschusses an den Vorsitzenden des Finanzausschusses des Deutschen Bundestages, Herrn Eduard Oswald, MdB (2008), S. 5/13–6/13

[148] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 2

[149] Vgl. Köhler, Thomas R.; Kirchmann, Walter: IT von A bis Z (2008), S. 230 und S. 206

[150] Vgl. Ertel, Wolfgang: Angewandte Kryptographie (2012), S. 98

[151] Vgl. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge (2009), S. 2302–2303

öffentlichen Schlüssel zur Verifizierung verwendet, werden die qualifizierten Zertifikate vergeben.[152]

Der komplette Vorgang der Erzeugung und Überprüfung der elektronischen Signaturen sowie die zuverlässige Aufbewahrung der privaten Schlüssel findet innerhalb der sogenannten Public Key Infrastruktur statt.[153] Dies ist wichtig, da das Erzeugen der Signatur mithilfe des privaten Schlüssels in einer gesicherten Umgebung erfolgen muss.[154]

Die ganz praktische Vorgehensweise bei der Vergabe von qualifizierten elektronischen Signaturen wird im Folgenden erläutert und in Abbildung 5 dargestellt.

Mit Erhalt des Zertifikats werden dem Antragsteller eine Signaturkarte, ein Lesegerät und eine persönliche Identifikationsnummer (PIN) übergeben.[155] Alle verwendeten technischen Komponenten müssen vom BSI zertifiziert sein.[156]

Zuerst wird der Hashwert # des Dokuments d nach der Hashfunktion h errechnet. Daraufhin wird # mittels des privaten Schlüssels verschlüsselt.[157] Hierfür wird die Chipkarte in das entsprechende Gerät eingesteckt und mit einer speziellen Software ausgelesen. Nachdem der Signierende die geforderte PIN korrekt eingegeben hat, wird anhand des Hashwerts # eine qualifizierte elektronische Signatur erstellt.[158] Bei diesem Vorgang wird der private Schlüssel niemals ausgegeben, sondern verbleibt stets auf der Signaturkarte, um dessen Geheimhaltung zu gewährleisten und dadurch einer eventuellen Manipulation vorzubeugen. In der Signaturkarte wird der private Schlüssel mit den zu signierenden Daten verknüpft und die fertige qualifizierte elektronische Signatur wird ausgegeben.[159]

Es gibt unterschiedliche Möglichkeiten, die digitale Signatur mit dem entsprechenden Dokument zu kombinieren. Bei PDF-Dokumenten wird die elektronische Signatur zumeist direkt in die Datei miteingebunden. Dieses Verfahren wird als enveloped bezeichnet. Außerdem besteht die Möglichkeit die Signaturdaten getrennt, auch detached genannt, von der Dokumentdatei in einer unabhängigen, binären Signaturdatei aufzubewahren. Hierbei muss über einen Link eine bleibende Verbindung zwischen den beiden Dateien hergestellt werden.[160]

Um auf der anderen Seite eine elektronische Signatur zu validieren, wird das entsprechende Zertifikat des Signierenden benötigt, denn darin ist der öffentliche Schlüssel des asymmetrischen Schlüsselpaars enthalten. Nur durch ihn kann die Echtheit der Signatur überprüft werden. Das Zertifikat kann öffentlich zugänglich an das Dokument

---

[152] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 28

[153] Vgl. Ertel, Wolfgang: Angewandte Kryptographie (2012), S. 117

[154] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 29

[155] Vgl. Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Abfallwirtschaft – Elektronisches Abfallnachweisverfahren – Fragen und Antworten – 4 (2010)

[156] Vgl. Fromm, Niels: Signatur und Zeitstempel zur Wahrung von Authentizität und Integrität (2009), S. 64

[157] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 30–31

[158] Vgl. Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Abfallwirtschaft – Elektronisches Abfallnachweisverfahren – Fragen und Antworten – 4 (2010))

[159] Vgl. Fromm, Niels: Signatur und Zeitstempel zur Wahrung von Authentizität und Integrität (2009), S. 64

[160] Vgl. Neuroth, Heike; Oßwald, Achim; Scheffel, Regine; Strathmann, Stefan; Huth, Karsten: Nestor-Handbuch (2010), S. 5:16

angehängt[161] oder im öffentlichen Verzeichnis des jeweiligen Signaturkartenanbieters recherchiert werden.[162]

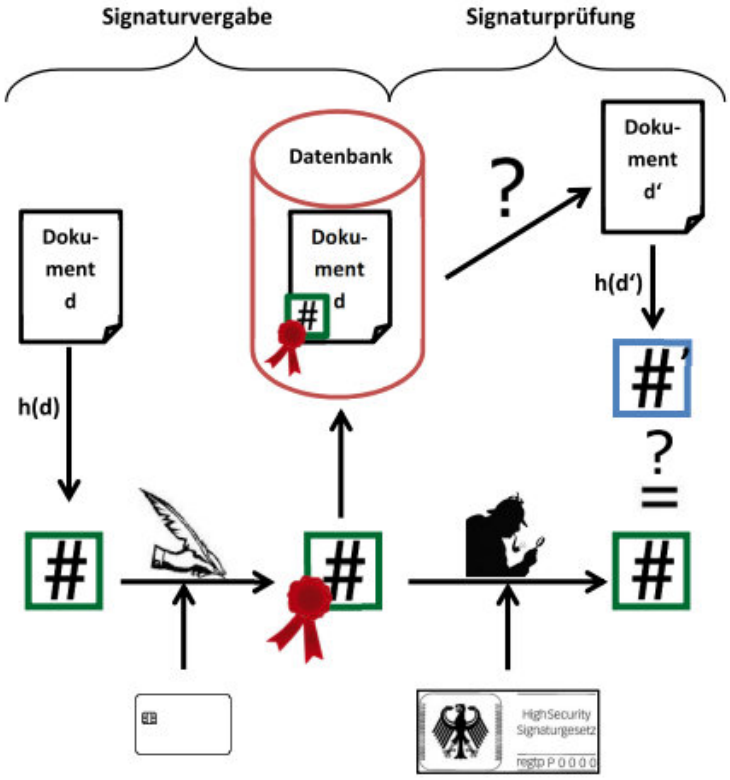

Abbildung 5:Vergabe und Prüfung von qualifizierten elektronischen Signaturen

Damit der Leser des Dokuments sicher sein kann, dass das Zertifikat vertrauenswürdig ist, wird dieses selbst mit einer Signatur der jeweiligen CA versehen. Hierfür muss sich die Zertifizierungsstelle von einer übergeordneten Behörde einen privaten Schlüssel zuordnen lassen. Der öffentliche Schlüssel zur Verifizierung des Zertifikats der CA muss aus einer öffentlich zugänglichen, verlässlichen Quelle stammen.[163]

Wenn festgestellt wurde, dass das Zertifikat gültig ist, so wird die digitale Signatur mit dem darin enthaltenen öffentlichen Schlüssel entschlüsselt, sodass wiederum der vom Verfasser erstellte Hashwert # zum Vorschein kommt. Um diesen zu überprüfen wird, wie bereits bei der Validierung von Hashwerten, ein neuer Hashwert #‘ mit der gleichen Hashfunktion h aus dem vorliegenden Dokument d‘ errechnet. Stimmen die Hashwerte # und #‘ überein, so ist damit bewiesen, dass das Dokument d‘ vom vorgegebenen Verfasser stammt und seit der Signaturvergabe nicht mehr verändert wurde.[164]

---

[161] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 169–170
[162] Vgl. Ertel, Wolfgang: Angewandte Kryptographie (2012), S. 119
[163] Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit (2011), S. 169–170
[164] Vgl. ebd., S. 30–31

Die Verifizierung einer qualifizierten elektronischen Signatur mithilfe des öffentlichen Schlüssels gleicht der Gegenüberstellung einer handschriftlichen Unterschrift und der Unterschrift auf dem Ausweis der Person. Denn ohne einen eindeutigen Vergleichswert, der von einer offiziellen Stelle stammt, kann keine Aussage über die Authentizität einer Signatur, egal ob handschriftlich oder digital, getroffen werden.

Somit bieten sich für das Institut für Informationswissenschaft folgende Handlungsmöglichkeiten, um die auf dem Dokumentenserver PubLIS Cologne abgelegten Abschlussarbeiten mithilfe einer qualifizierten digitalen Signatur zu sichern.

Grundsätzlich ist anzumerken, dass es für die Signierung der Hashwerte nötig ist, diese nach der Errechnung vom BSZ zu erhalten. Schließlich können diese am Institut für Informationswissenschaften weitergenutzt werden.

Zum einen könnte das Institut in der Prüfungsordnung festlegen, dass die digitale Abschlussarbeit bei der Abgabe vom Prüfling selbst mit einer qualifizierten elektronischen Signatur versehen sein muss. Hiermit wäre das Dokument eindeutig der Identität des Verfassers zugeordnet und im Falle eines Rechtsstreits für den Prüfling nicht abstreitbar, dass er die Arbeit selbst in dieser Form erstellt und signiert hat. Da es sich in diesem Fall um ein privates Dokument handelt, würden die Vorschriften der Zivilprozessordnung für private Urkunden gelten. Diese besagen, dass die Echtheit des signierten digitalen Dokuments „nur durch Tatsachen erschüttert werden, die ernstzunehmende Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.“[165] Bei der genannten Erklärung handelt es sich in diesem Fall um die Abschlussarbeit und beim Signaturschlüssel-Inhaber um den Prüfling.

Betrachtet man die Tatsache, dass die Preise für eine Signaturkarte mit qualifiziertem Zertifikat zwischen beispielsweise. 39 Euro[166] mit einer Gültigkeit von einem Jahr bei der Deutschen Post AG und 99 Euro[167] mit einer Gültigkeit von zwei Jahren bei der Bundesdruckerei schwanken[168] und eine solche für das Signieren von Dokumenten zwingend nötig ist, so kann das selbstständige Signieren durch die Studierenden eine finanzielle Belastung darstellen. Ob die Aufwendung dieser Kosten von den Prüflingen verlangt werden kann oder, ob es eventuell eine anderweitige, entsprechende Finanzierungsmöglichkeit gibt, ist vom Institut für Informationswissenschaft zu klären. Abgesehen von finanziellen Gesichtspunkten ist zusätzlich der Aufwand, der mit der Beantragung einer Signaturkarte, der dabei nötigen Identifizierung und der Signierung selbst verbunden ist, zu beachten. Es muss nämlich entweder vom Prüfling selbst ein Hashwert errechnet und dieser verschlüsselt oder das komplette Dokument signiert werden. Diese Aspekte würden bei einer Einführung der vorgestellten Vorgehensweise gewiss kritische Stimmen hervorrufen. Es ist jedoch zu beachten, dass sich die Bedeutung und die Verbreitung von digitalen Signaturen in Zukunft noch steigern können. Vor allem durch die Einführung des neuen Personalausweises am 1. November 2010 wurde ein wichtiger Schritt getan, um das elektronische Signieren in vielen Lebensbereichen zu etablieren. Durch diesen ist es nämlich jedem Ausweisinhaber möglich sich im Internet zu authentifizieren und nach Beantragung eines Zertifikats qualifizierte elektronische Signaturen zu vergeben.[169]

Abschließend ist anzumerken, dass es sich bei dieser Vorgehensweise um die korrekte Art der Durchführung handelt, da nur dadurch der Prüfling unabstreitbar als Verfasser

---

[165] Zivilprozessordnung (vom 05.12.2005), § 371a Satz 1
[166] Vgl. Deutsche Post AG: Dienstleistungen – Elektronische Signatur – Signtrust Card (2011)
[167] Vgl. Bundesdruckerei – D-Trust: Preisinformationen (2012), S. 1
[168] Beide Preise sind ohne gesetzliche Umsatz- bzw. Mehrwertsteuer angegeben.
[169] Vgl. Ertel, Wolfgang: Angewandte Kryptographie (2012), S. 134–135

des abgegebenen Dokuments identifiziert wird. In diesem Fall übernimmt die elektronische Signatur die oben erläuterte Funktion der Identifikation. Besonders im Hinblick auf die eidesstattliche Erklärung, welche der Arbeit angefügt werden muss (siehe Kapitel 4.1.3), scheint eine qualifizierte elektronische Signatur vom Studierenden selbst abgegeben sinnvoll.

Als Alternative könnte ein verantwortlicher Institutsmitarbeiter ein qualifiziertes Zertifikat bei einer Zertifizierungsstelle beantragen, sodass dieser qualifizierte elektronische Signaturen im Namen des Instituts für Informationswissenschaft bzw. der Fachhochschule Köln vergeben kann. Besonders in Unternehmen tritt oft der Fall auf, dass ein Mitarbeiter im Namen des Unternehmens ein Schriftstück erstellt. Die in diesem Dokument vorhandenen Aussagen sollen nicht explizit der natürlichen Person zugeordnet werden, sondern als Willenserklärung des Unternehmens veröffentlicht oder versendet werden.

Für solche Fälle regelt das Signaturgesetz in § 5 Abs. 2 die Möglichkeit einer Person das Recht zu übertragen, qualifizierte elektronische Signaturen im Namen einer dritten Person zu erstellen. Der Schlüsselinhaber besitzt damit die Vertretungsmacht für die entsprechende Person. Ob das Hinzufügen dieser zusätzlichen Angaben, welche als Attribute bezeichnet werden, rechtens ist, muss von der in diesem Fall zuständigen Stelle geprüft werden.[170]

Auf der Website des Bundesumweltministeriums werden Fakten zur Vergabe einer Vertretungsmacht erklärt. Da sich diese FAQs allgemein auf die Verwendung qualifizierter elektronischer Signaturen beziehen, können einige Sachverhalte auch auf die Lage des Instituts für Informationswissenschaft übertragen werden. Demnach kann die Gestaltung der Vertretungsmacht des jeweiligen Mitarbeiters im qualifizierten Zertifikat genau geregelt werden, um so die Signiermöglichkeiten auf bestimmte Bereiche zu beschränken. In diesen Aufgabenkreisen, welche durch die Attribute des Zertifikats festgelegt sind, erhält der Mitarbeiter eine Vollmacht zur Signierung von Dokumenten. Auch sollte die Art der Bevollmächtigung des jeweiligen Mitarbeiters genau festgelegt werden. Seine Befugnisse sollten im Arbeitsvertrag oder in sonstigen schriftlichen Vereinbarungen, z. B. einer Unterschriftenregelung, festgehalten werden. Dadurch wird genau geklärt, in welchen Bereichen er seine Unterschrift in Vertretung für das Unternehmen abgeben kann. Dies gilt sowohl für die Vergabe einer qualifizierten elektronischen Signatur, als auch für die eigenhändige Unterschrift.[171] Hierbei spielt der Aspekt der eindeutigen und verbindlichen Festlegung von Zuständigkeiten und Verantwortlichkeiten eine Rolle (siehe Kapitel 4.1.1).

Im Anwendungsfall des Instituts für Informationswissenschaft tritt jedoch die Problematik auf, dass die zu unterzeichnenden Dokumente nicht vom Institut selbst, sondern von den Prüflingen stammen. Somit kann die qualifizierte elektronische Signatur, wenn sie von einem Mitarbeiter in Vertretung für das Institut vergeben wird, nicht die Zuordnung zum studentischen Verfasser gewährleisten.

Dennoch kann sie für Erhalt und Nachweis der Authentizität der Abschlussarbeit während deren Speicherung auf dem Dokumentenserver PubLIS Cologne eingesetzt werden. Da die Dokumente, wie oben erwähnt, mit Abgabe beim Prüfungsamt in den Besitz der Prüfungsbehörde übergehen und als amtliche Urkunden gelten, könnte von der besitzenden Behörde eine qualifizierte elektronische Signatur vergeben werden. Durch diese Unterzeichnung würde der Funktion nach die Echtheit des vorliegenden

---

[170] Vgl. Signaturgesetz (vom 17.07.2009), § 5 Abs. 2

[171] Vgl. Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit: Abfallwirtschaft – Elektronisches Abfallnachweisverfahren – Fragen und Antworten – 6 (2010)

Dokuments bestätigt werden. Zum Zeitpunkt der Einreichung erstellt, würde die qualifizierte elektronische Signatur so den Zustand der eingereichten Abschlussarbeit dokumentieren.

Als weiterer Lösungsansatz besteht grundsätzlich die Möglichkeit der eingereichten Abschlussarbeit ein Dokument anzufügen, in welchem der Originalzustand der abgelegten Datei von der Prüfungsbehörde bestätigt wird. Schließlich wird anstelle der Abschlussarbeit direkt diese offizielle Bestätigung vom verantwortlichen Mitarbeiter mit einer qualifizierten elektronischen Signatur versehen. Dies bietet den zusätzlichen Vorteil, dass die Bewertung der Arbeit und die entsprechende Begründung direkt signiert und mitabgespeichert werden könnten. Wie diese Dokumente über ein Hashbaum-Verfahren miteinander verknüpft werden können, wird im Kapitel 4.3.2 näher erläutert. In diesem Fall werden die Dokumente nicht einzeln digital signiert, sondern es wird lediglich eine qualifizierte elektronische Signatur für den gesamten Hashbaum erzeugt. Dieses Verfahren bestätigt zwar die Echtheit der Abschlussarbeit, es wird jedoch wiederum keine verbindliche Aussage über den Verfasser getroffen.

Wichtig ist zudem die Vergabe eines Zeitstempels, da dadurch belegt werden kann, dass das Dokument zu einem bestimmten Zeitpunkt in genau dieser Form eingereicht und abgespeichert wurde. Ein Zeitstempel ist ebenso wie eine Signatur nur dann gültig, wenn er mit einem gültigen qualifizierten Zertifikat erstellt worden ist.[172]

Wie ein solcher Zeitstempel, der stets von der Zertifizierungsstelle selbst vergeben wird, aufgebaut ist, wird im Folgenden erklärt. Die CA hängt das Datum und die Uhrzeit in codierter Form an das Dokument bzw. den Hashwert an. Zusätzlich wird die Datei mit einer Signatur versehen, welche mit dem privaten Schlüssel der Zertifizierungsstelle erzeugt wird. Diese Einheit aus Zeitpunkt und qualifizierter elektronischer Signatur ist der Zeitstempel.[173]

Gerade, wenn es um die fristgerechte Einreichung von Abschlussarbeiten geht, spielt der zeitliche Aspekt eine zentrale Rolle. Dies setzt natürlich voraus, dass die Arbeiten zeitnah, am besten am Tag der Einreichung, signiert werden, wobei der entsprechende Zeitstempel angefügt wird. Des Weiteren dient der Zeitstempel als Beweis dafür, dass das qualifizierte Zertifikat zum Zeitpunkt der Signaturvergabe gültig war.[174]

Als Beispiel für die bereits praktizierte Vergabe von Zeitstempeln für Dokumente eines Repositoriums ist die Humboldt-Universität zu Berlin zu nennen. Deren Vorgehensweise lässt sich durchaus auf die Lage des Instituts für Informationswissenschaft übertragen. Der errechnete Hashwert für ein Dokument wird an die zuständige Zertifizierungsstelle gesendet, wo er mit einem Zeitstempel versehen wird. Dieser Zeitstempel wird zusammen mit den Dokumenten, den zugehörigen Hashwerten und digitalen Signaturen zusätzlich auf einem separaten Server gespeichert. Dieser ist unabhängig vom eigentlichen Repositorium und nur für die zuständigen Mitarbeiter zugänglich.[175]

Eine gesonderte Sicherung dieser erzeugten Komponenten ist notwendig, denn der Hashwert, die elektronische Signatur und der Zeitstempel bilden die Grundlage um Integrität und Authentizität der Abschlussarbeiten auf dem Dokumentenserver PubLIS Cologne zu beweisen.

---

[172] Vgl. Bundesamt für Sicherheit in der Informationstechnik: Grundlagen der elektronischen Signatur (2006), S. 85

[173] Vgl. Ertel, Wolfgang: Angewandte Kryptographie (2012), S. 119

[174] Vgl. Signature Perfect KG: Leitfaden Elektronische Signatur (2008), S. 15

[175] Vgl. Fromm, Niels: Signatur und Zeitstempel zur Wahrung von Authentizität und Integrität (2009), S. 66

Ferner ist bei der Signaturvergabe durch den Vertreter einer Institution dem Thema der sicheren Verwahrung von Signaturschlüsseln eine besondere Beachtung zu schenken. Ein speziell geregeltes Verfahren, sollte den privaten Schlüssel des Signaturschlüsselinhabers, also des Bevollmächtigten, vor Manipulation und unsachgemäßer Nutzung schützen.[176] Hierzu sollten entsprechende organisatorische Voraussetzungen geschaffen werden. So sollte nur der Schlüsselinhaber und eventuell ein Stellvertreter Kenntnis über die PIN haben und die Signaturkarte und das entsprechende Lesegerät sollten getrennt voneinander und sicher verwahrt werden, z. B. in einem Tresor.

Im Kostenbeispiel oben ist bereits deutlich geworden, dass die Gültigkeit eines qualifizierten Zertifikats auf einen bestimmten Zeitraum beschränkt ist. Seitens der Institution ist auf die Gültigkeit der verwendeten qualifizierten Zertifikate zu achten, denn im Allgemeinen endet mit der Gültigkeitsdauer eines Zertifikats auch die Beweiskraft bezüglich der Verbindlichkeit der mit diesem Signaturschlüssel signierten Dokumente. Odenthal verweist in seiner Abhandlung jedoch auf die revisionssichere Speicherung der Dokumente. Da diese während der Speicherung auf dem Dokumentenserver vor Veränderungen geschützt sind, ist eine Nachzertifizierung der einzelnen Dokumente solange sie am Speicherort verbleiben nicht nötig.[177]

Die Kosten für das Institut würden sich beim Erwerb einer Signaturkarte z. B. von D-Trust, einem Dienstleister der Bundesdruckerei, auf 213,01 Euro für vier Jahre belaufen. Der Preis für weitere vier Jahr beträgt im Moment 207,06 Euro. Die angegebenen Preise beziehen sich auf eine einfache Signaturkarte mit welcher qualifizierte elektronische Signaturen vergeben werden können.[178] Zudem besteht die Möglichkeit eine Massensignaturkarte zu erwerben. Mit dieser können mehrere Dokumente auf einmal signiert werden.[179] Im Hinblick auf die momentan eher geringe Anzahl von Abschlussarbeiten, die zu signieren und hochzuladen wären, erscheint die Anschaffung einer solchen Massensignaturkarte jedoch nicht nötig (siehe Kapitel 3.2).

Des Weiteren muss ohnehin jedes einzelne Dokument vom abgegebenen Datenträger des Prüflings übernommen und vor dem Upload geprüft werden. Die digitale Unterzeichnung durch den verantwortlichen Mitarbeiter und die Vergabe des Zeitstempels sollten in diese Prozessabfolge integriert werden.

4.3.4 Maßnahmen zur Sicherung der Vertraulichkeit der Dokumente

Neben den Aspekten Authentizität und Integrität spielt zudem Vertraulichkeit eine Rolle. Da der Dokumentenserver PubLIS Cologne nicht, wie für Repositorien üblich, in erster Linie für die Veröffentlichung von Dokumenten, sondern ebenso zur Speicherung von Arbeiten dient, welche nicht publiziert werden dürfen, müssen zur Sicherung der Vertraulichkeit entsprechende Maßnahmen getroffen werden.

Von besonderer Bedeutung ist Vertraulichkeit, wenn die Arbeit mit einem Sperrvermerk versehen ist, da sie firmeninterne Informationen enthält. Ein solcher Sperrvermerk ist der Arbeit voranzustellen und muss Informationen darüber enthalten, welche Abschnitte der Arbeit und wie lange diese der Geheimhaltung unterliegen.[180] Als Beispiel einer schriftlichen Vereinbarung bezüglich eines Sperrvermerks kann ein Vertragsmus-

---

[176] Vgl. Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge (2009), S. 2302
[177] Vgl. Odenthal, Roger: Digitale Archivierung (2007), S. 39
[178] Vgl. Bundesdruckerei – D-Trust: Preisinformationen (2012), S. 1
[179] Vgl. ebd., S. 2
[180] Vgl. Fachhochschule Köln / Fakultät für Informations- und Kommunikationswissenschaften: Informationen zur Bachelorarbeit (2013), S. 10

ter im Merkblatt für Studienabschlussarbeiten der Hochschule für Technik und Wirtschaft Dresden herangezogen werden. Für die Fachhochschule Köln findet sich keine vergleichbare Ausführung. In diesem Vertrag, der zwischen dem Prüfling, dem beteiligten Unternehmen und der durch den Erstgutachter vertretenen Hochschule abgeschlossen wird, wird festgeschrieben, dass der Studierende als Urheber von seinem Verbreitungsrecht nur nach Zustimmung des Unternehmens Gebrauch macht. Die Hochschule selbst verpflichtet sich die Abschlussarbeit nach den Vorschriften der Geheimhaltung aufzubewahren und das Dokument nur den Gutachtern und dem Prüfungsausschuss zur Bewertung zugänglich zu machen. Wichtig ist an dieser Stelle auch der Vermerk, dass die Hochschule keinerlei Haftung für ein Zuwiderhandeln seitens des Studierenden oder des Unternehmens übernimmt.[181] Nach Abschluss eines solchen schriftlichen Vertrages würde sich die Hochschule bei einer beabsichtigten oder unbeabsichtigten Veröffentlichung der betroffenen Abschlussarbeit des Vertragsbruches schuldig machen. Um die Rechte und Pflichten der beteiligten Parteien zu klären, ist eine solche Vereinbarung dringend zu empfehlen. Des Weiteren wird das betroffene Unternehmen gewiss auf diese Absicherung bestehen.

Wenn der Prüfling mit der Veröffentlichung seiner Abschlussarbeit nicht einverstanden ist und das auf dem entsprechenden Formular vermerkt, ist ebenfalls die Vertraulichkeit des Dokuments zu wahren. In diesem Fall würde die Fachhochschule bei einer Publikation gegen die schriftliche Vereinbarung mit dem Urheber der Arbeit verstoßen.

Wie bereits in Kapitel 4.1.2 erläutert, ist deshalb eine reibungslose Organisation und deren regelmäßige Kontrolle nötig. Darum muss der Festlegung der Zugriffsebene vor dem Hochladen des Dokuments besondere Aufmerksamkeit gewidmet werden. Die Überprüfung, ob das Aufrufen des Volltextes nur vom vorgesehenen Standpunkt aus möglich ist, ist unbedingt nötig und sollte von einem Mitarbeiter übernommen werden, der nicht am Prozess des Hochladens beteiligt war.

Für die technischen Aspekte der Vertraulichkeitserhaltung muss das BSZ als Host des Dokumentenservers Sorge tragen. Dies sollte in einer schriftlichen Vereinbarung eindeutig geregelt werden.

4.3.5 Vorkehrungen für einen Krisenfall

Um einen sicheren Erhalt der Dokumente zu erreichen, müssen neben technischen Vorkehrungen auch Maßnahmen für einen eventuellen Krisenfall ausgearbeitet werden. Ein Notfall kann in unterschiedlichsten Formen auftreten. So können durch technisches Versagen, z. B. einen Stromausfall oder einen Serverabsturz, Daten verloren gehen. Da sich im Fall von PubLIS Cologne das BSZ als externer Dienstleister für die technischen Aspekte der Speicherung der Dokumente verantwortlich zeigt, beziehen sich die folgenden Empfehlungen auf organisatorische Vorsorgemaßnahmen, welche das Institut für Informationswissenschaft selbst durchführen kann. Die Vorkehrungen, die das BSZ für einen solchen Fall trifft, werden in Kapitel 3.3.2 vorgestellt.
Im Allgemeinen sollte der Erhalt der Dokumente für mindestens zehn Jahre garantiert werden, da dies aus juristischer Sicht die nötige Aufbewahrungsfrist ist (siehe Kapitel 3.4).

Auch fehlende oder nicht weitergeführte Finanzierung und dadurch entstehender Mangel an Fachpersonal kann eine Notsituation für den Dokumentenserver bedeuten. Um das langfristige Bestehen des Repositoriums zu gewährleisten, müssen schriftliche

[181] Vgl. Hochschule für Technik und Wirtschaft Dresden / Fakultät Wirtschaftswissenschaften: Merkblatt für die Erstellung der Studienabschlussarbeit (2009), S. 21–22

Garantien für die Zukunft gegeben werden. Diese sollen vor allem eine ausreichende Finanzierung für einen unbefristeten Zeitraum garantieren. Die Schaffung einer eigenen Kostenstelle und eine schriftliche Zusicherung von Geldern durch das Institut, wie sie in Kapitel 4.1.1 empfohlen werden, wären ein erster wichtiger Schritt in diese Richtung.

Zudem wird bei den vorgestellten Kriterien in Kapitel 2.3 die Regelung einer Nachfolge gefordert. Eine festgelegte, am besten übergeordnete, Instanz verpflichtet sich dabei die Daten zu übernehmen, falls der Träger das Repositorium nicht mehr unterhalten kann. Zu diesem Zweck sollte ein genauer Ablaufplan für die Übergabe der Daten feststehen und die Informationsobjekte in einem für den Export geeigneten Datenformat vorgehalten werden.

Da es sich beim Institut für Informationswissenschaft als Teil der Fachhochschule Köln jedoch um eine staatlich finanzierte, öffentliche Institution handelt, ist eine finanzielle Krise, wie sie ein Unternehmen z. B. in Form einer Insolvenz treffen kann, auszuschließen. Dennoch sollte durch schriftliche Zusicherungen seitens der Fachhochschule eine langfristige Finanzierung des Dokumentenservers PubLIS Cologne gesichert werden. Zusätzlich sollte garantiert werden, dass das Repositorium auch im Falle von Umstrukturierungen, die das Institut für Informationswissenschaft betreffen könnten, weitergeführt wird und die Verantwortung von der nachfolgenden Organisationseinheit bzw. von der Fachhochschule selbst übernommen wird. Um zukünftige Potentiale voll ausschöpfen zu können, sollte eine mögliche Erweiterung des Datenbestandes, z. B. durch die Übernahme von Veröffentlichungen aus anderen Instituten, mit einem gesteigerten Budget, mehr Personalstellen und erweiterten Verantwortungsbereichen einhergehen.

Diese Kriterien bezüglich einer Notlage lassen sich nicht nur auf das Institut als Träger des Dokumentenservers, sondern auch auf den Host, also das BSZ, beziehen. Besonders in diesem Fall sollten Regelungen zur Vorgehensweise im Krisenfall und zur eventuellen Datenübernahme durch einen Nachfolger bestehen. Diese Vorkehrungen sollten schriftlich festgelegt und dem Institut für Informationswissenschaft bekannt sein.

5 AUSBLICK

Nach Betrachtung und Beurteilung der Möglichkeiten für die ausschließlich digitale Archivierung von Abschlussarbeiten, kann zusammenfassend festgestellt werden, dass es durchaus vielversprechende Potentiale und Chancen zur sicheren Umsetzung gibt. Denn Wege zur Erhaltung von Integrität und Authentizität, den beiden Kernpunkten der revisionssicheren Archivierung, existieren. Diese wurden umfassend vorgestellt und bewertet.

Dennoch bleiben einige Problemstellungen, vor allem was die konkrete Handhabung betrifft, ungelöst. Es handelt es sich bei der elektronischen Aufbewahrung von Abschlussarbeiten und Prüfungsunterlagen im Allgemeinen, wie bereits erwähnt, um eine rechtliche Grauzone. Zwar gibt es bereits konkrete Gesetze, die die Beweiskraft digitaler Dokumente, gerade in Verbindung mit qualifizierten elektronischen Signaturen, sichern. So findet die digitale Archivierung im Unternehmensbereich bereits vielfältige Anwendung. Nun liegt es an den Hochschulen nachzuziehen und die elektronische Aufbewahrung der Abschlussarbeiten hochschulrechtlich zu klären. Zugleich würden eine Neuinterpretation der Rechtsprechung in einem konkreten Fall oder die Erweiterung der entsprechenden Gesetze selbst juristische Sicherheit mit sich bringen.

In jedem Fall ist es nötig, das Bewusstsein für die Notwendigkeit der digitalen Archivierung zu wecken. Denn die zunehmende Bedeutung digitaler Dokumente und deren rechtssichere Verwaltung ist längst in Deutschlands Alltag angekommen und macht auch vor Hochschulen und Prüfungsämtern nicht halt. Durch die Einführung elektronischer Semesterapparate und Online-Prüfungsservices sind bereits deutliche Schritte in diese Richtung unternommen worden. Ergänzend ist anzumerken, dass in der Lebenswelt der Studierenden IT-Lösungen eine immer größere Rolle spielen und die Affinität dazu mit jeder neuen Generation an Absolventen steigt. Zudem werden durch die e-Card-Strategie der Bundesregierung immer mehr Bereiche des öffentlichen Lebens in die Digitalisierung einbezogen. Hierzu gehören z. B. der bereits erwähnte elektronische Personalausweis sowie die elektronische Steuererklärung und die elektronische Gesundheitskarte.[182]

Der Bedarf für gesetzliche Regelungen bezüglich der digitalen Abwicklung von Abschlussarbeiten im Speziellen ist also durchaus gegeben. Dies würde eine verlässliche Grundlage für die Weiterführung von PubLIS Cologne in der gewünschten Form bieten. Auch über die Kölner Fachhochschule hinaus werden sich gewiss Befürworter des Verfahrens finden. Gerade da viele Hochschulen über ein eigenes Repositorium verfügen, bietet sich diese Vorgehensweise zur Nachahmung an. Hierbei kann die Vergabe der unterschiedlichen Zugriffsebenen als besonders innovativ angesehen werden.

Zudem ist für die Abschlussarbeiten lediglich eine Speicherung für zehn Jahre nötig, wodurch die Problematiken der Langzeitarchivierung zum größten Teil außer Acht gelassen werden können. Dieser Zeitraum orientiert sich jedoch an den rechtlichen Mindestanforderungen. Bereits im Moment wird für den Dokumentenserver PubLIS Cologne das Ziel, die Dokumente auf unbestimmte Zeit verfügbar zu halten, ausgesprochen. Dieser Aspekt wurde in den Betrachtungen der vorliegenden Arbeit jedoch nicht behandelt und muss weitergehende Überlegungen nach sich ziehen. In diesem Fall kann auf die Erfahrung des BSZ zurückgegriffen werden.

Die Entscheidung, ob eine Umstellung auf die ausschließlich elektronische Speicherung der Abschlussarbeiten erfolgen und wie die konkrete Umsetzung aussehen soll,

---

[182] Vgl. Eckert, Claudia: IT-Sicherheit (2012), S. 406–408

muss schließlich vom Institut für Informationswissenschaft in Abstimmung mit dem Prüfungsamt getroffen werden. Jedoch müssen im Vorfeld noch diverse Punkte geklärt und gewiss viel Überzeugungsarbeit geleistet werden, um diese Idee durchzusetzen.

Abschließend kann jedoch festgehalten werden, dass es sich bei der digitalen Archivierung von Abschlussarbeiten um ein wichtiges und vor allem zukunftsfähiges Thema handelt. Es hat das Potenzial, die Abgabe von Abschlussarbeiten in den digitalen Fortschritt miteinzubeziehen und eine Bereicherung für die Hochschullandschaft darzustellen.

6 QUELLEN- UND LITERATURVERZEICHNIS

3rd international PDF/A Conference (2009): PDF/A up to date: Long-Term Archiving with PDF. Berlin: Association for Digital Document Standards ADDS / PDF/A Competence Center.

Abgabenordnung (AO) vom 01.10.2002 (16.03.1976).
http://www.gesetze-im-internet.de/ao_1977/index.html [abgerufen am: 03.08.2013].

Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (2013): Fachinformationen: Aktueller Entwurf der GoBIT.
http://www.awv-net.de/cms/index-b-267-848.html [abgerufen am: 02.08.2013].

Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (2012): Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz (GoBIT): Entwurf. Version: 5.1.
http://www.awv-net.de/cms/upload/pdf/GoBIT_Entwurf_V_5_0_2012_10_13_final.pdf [abgerufen am: 02.08.2013].

Association for Digital Document Standards e.V. (2013): PDF/A kompakt 2.0: PDF für die Langzeitarchivierung; Der ISO-Standard - von PDF/A-1 bis PDF/A-3.
http://www.pdfa.org/wp-content/uploads/2013/05/PDFA-kompakt-20.pdf [abgerufen am: 02.08.2013].

Bibliotheksservice-Zentrum Baden-Württemberg: Entgeltordnung des Bibliotheksservice-Zentrums Baden-Württemberg vom 27.04.2011.
http://swop.bsz-bw.de/volltexte/2011/928/pdf/entgeltordnung_bsz_2011.pdf [abgerufen am: 02.08.2013].

Bibliotheksservice-Zentrum Baden-Württemberg: Museen, Archive und Repositorien im Bibliotheksservice-Zentrum Baden-Württemberg.
http://www.bsz-bw.de/mare/index.html [abgerufen am: 02.08.2013].

Bibliotheksservice-Zentrum Baden-Württemberg: Willkommen beim Bibliotheksservice-Zentrum Baden-Württemberg!
http://www.bsz-bw.de/index.html [abgerufen am: 02.08.2013].

Borghoff, Uwe M.; Rödig, Peter; Scheffczyk, Jan; Schmitz, Lothar (2003): Langzeitarchivierung: Methoden zur Erhaltung digitaler Dokumente. 1. Aufl. Heidelberg: dpunkt-Verlag.

Brand, Thorsten (2012): An Geschäftsdokumente stellen Gesetze hohe Anforderungen: Ein effizienter Zugriff auf Informationen ist für Unternehmen unerlässlich. Bei elektronischen Ablagen regeln Gesetze die Ausgestaltung. Eventuelle Compliance-Defizite deckt eine Analyse auf. In: is report (07-08), S. 36–39.
http://www.wiso-net.de/webcgi?START=A60&DOKV_DB=ZECO&DOKV_NO=ISRBD7C5ED2074A16CEF5A19D50F2BD7344&DOKV_HS=0&PP=1 [abgerufen am: 08.08.2013].

Bürgerliches Gesetzbuch (BGB) vom 02.01.2002 (18.08.1896).
http://www.gesetze-im-internet.de/bgb/__126a.html [abgerufen am: 03.08.2013].

Bundesamt für Sicherheit in der Informationstechnik (2006): Grundlagen der elektronischen Signatur: Recht, Technik, Anwendung.
https://www.bsi.bund.de/cae/servlet/contentblob/487196/publicationFile/31407 [abgerufen am: 02.08.2013].

Bundesamt für Sicherheit in der Informationstechnik (2009): IT-Grundschutz-Kataloge. 11. Ergänzungslieferung, November 2009.
https://www.bsi.bund.de/cae/servlet/contentblob/478418/publicationFile/54741/it-grundschutz-kataloge_2009_EL11_de.pdf, zuletzt aktualisiert am 09.10.2009 [abgerufen am: 02.08.2013].

Bundesdruckerei - D-Trust (2012): Preisinformationen : Qualifizierte Signaturkarten. Version 2.94
http://www.bundesdruckerei.de/sites/default/files/2.preisinformationen_2.pdf [abgerufen am: 02.08.2013].

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (2010): Abfallwirtschaft – Elektronisches Abfallnachweisverfahren – Fragen und Antworten – 4.
http://www.bmu.de/themen/wasser-abfall-boden/abfallwirtschaft/abfallrecht/national/elektronisches-abfallnachweisverfahren-fragen-und-antworten-4/ [abgerufen am: 02.08.2013].

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (2010): Abfallwirtschaft – Elektronisches Abfallnachweisverfahren – Fragen und Antworten – 6.
http://www.bmu.de/themen/wasser-abfall-boden/abfallwirtschaft/abfallrecht/national/elektronisches-abfallnachweisverfahren-fragen-und-antworten-6/ [abgerufen am: 02.08.2013].

Callas Software GmbH (2013): pdfaPilot – PDF/A-Unterstützung für Einsteiger, als Standalone oder in Acrobat.
http://www.callassoftware.com/callas/doku.php/de:products:pdfapilot [abgerufen am: 02.08.2013].

Deutsche Initiative für Netzwerkinformation e.V.: DINI: DINI-Zertifikat 2010 für Dokumenten- und Publikationsservices.
http://www.dini.de/dini-zertifikat/ [abgerufen am: 02.08.2013].

Deutsche Initiative für Netzwerkinformation e.V. / Arbeitsgruppe Elektronisches Publizieren: DINI-Zertifikat: Dokumenten- und Publikationsservice 2010, 2011 (DINI Schriften, 3-de).
http://edoc.hu-berlin.de/series/dini-schriften/2010-3/PDF/dini-zertifikat-3.1.pdf [abgerufen am: 02.08.2013].

Deutsche Nationalbibliothek: Nestor – Home: Willkommen bei Nestor.
http://www.langzeitarchivierung.de/Subsites/nestor/DE/Home/home_node.html;jsessionid=C5445ED53BF6B859EE0DFBC8F716A64A.prod-worker2 [abgerufen am: 02.08.2013].

Deutsche Nationalbibliothek: Persistent Identifier: Beschreibung des Algorithmus zur Berechnung der URN-Prüfziffer.
http://www.persistent-identifier.de/?link=316 [abgerufen am: 05.08.2013].

Deutsche Nationalbibliothek (2008): Persistent Identifier: FAQs.
http://www.persistent-identifier.de/?link=400 [abgerufen am: 02.08.2013].

Deutsche Nationalbibliothek (2012): Policy für die Vergabe von URNs im Namensraum urn:nbn:de: Version 1.0.
http://d-nb.info/1029114455/34 [abgerufen am: 02.08.2013].

Deutsche Nationalbibliothek (2013): Projects – NESTOR – Network of Expertise in Long-term Storage of Digital Resources.
http://www.dnb.de/EN/Wir/Projekte/Abgeschlossen/nestor.html [abgerufen am: 02.08.2013].

Deutsche Post AG (2011): Dienstleistungen – Elektronische Signatur – Signtrust Card.
http://www.deutschepost.de/dpag?xmlFile=link1015459_49577 [abgerufen am: 02.08.2013].

Drümmer, Olaf; Oettler, Alexandra; von Seggern, Dietrich (2007): PDF/A kompakt: Digitale Langzeitarchivierung mit PDF. Berlin : callas software GmbH.

Eckert, Claudia (2012): IT-Sicherheit: Konzepte, Verfahren, Protokolle. 7., überarbeitete und erweiterte Auflage. München: Oldenbourg Wissenschaftsverlag.

Ertel, Wolfgang (2012): Angewandte Kryptographie. 4., überarbeitete und ergänzte Auflage. München: Hanser.

European Telecommunications Standards Institute: ETSI – PDF Advanced Electronic Signature (PAdES) FAQ.
http://www.padesfaq.net/ [abgerufen am: 02.08.2013].

Fachhochschule Köln: Einschreibungsordnung der Fachhochschule Köln, Stand: 11.07.2007.
http://www.presse.fh-koeln.de/imperia/md/content/verwaltung/dezernat5/amtliche/2007_25.pdf [abgerufen am: 08.08.2013].

Fachhochschule Köln (22.01.2009): Prüfungsordnung für den Studiengang Bibliothekswesen mit dem Abschlussgrad „Bachelor of Arts“ der Fakultät für Informations- und Kommunikationswissenschaften der Fachhochschule Köln: BPO Bibliothekswesen, Stand: 16.10.2008.
http://www.fbi.fh-koeln.de/studium/pruefungen/BPO_Bibliothekswesen_Endfassung_Beginn_2008-2009.pdf [abgerufen am: 03.08.2013].

Fachhochschule Köln (06.02.2009): Prüfungsordnung für den Studiengang Informationswirtschaft mit dem Abschlussgrad „Bachelor of Science“ der Fakultät für Informations- und Kommunikationswissenschaften der Fachhochschule Köln: BPO Informationswirtschaft, Stand: 01.09.2008.
http://www.fbi.fh-koeln.de/studium/pruefungen/BPO_Informationswirtschaft_Endfassung_Beginn_2008-2009.pdf [abgerufen am: 03.08.2013].

Fachhochschule Köln / Fakultät für Informations- und Kommunikationswissenschaften: OPUS 4 – Übersicht der Dokumenttypen.
http://publiscologne.fh-koeln.de/solrsearch/browse/doctypes [abgerufen am: 02.08.2013].

Fachhochschule Köln / Fakultät für Informations- und Kommunikationswissenschaften (2013): Informationen zur Bachelorarbeit: Bachelorstudiengänge Bibliothekswesen und Informationswirtschaft.
http://www.fbi.fh-koeln.de/studium/pruefungen/InfoBachelorarbeitBIB+IW.pdf [abgerufen am: 03.08.2013].

Ferle, Christoph H. (2012): Marktstudie digitale Langzeitarchivierung: im Spannungsfeld zwischen Digital Preservation und Enterprise Information Archiving. Unter Mitarbeit von Dieter Spath und Anette Weisbecker. Stuttgart : Fraunhofer Verlag.

Fromm, Niels (2009): Signatur und Zeitstempel zur Wahrung von Authentizität und Integrität. In: CMS-Journal (32), S. 63–66.
http://edoc.hu-berlin.de/cmsj/32/fromm-niels-63/PDF/fromm.pdf [abgerufen am: 05.08.2013].

Gerland, Friederike, 29.05.2013. E-Mail an Autorin.

Handelsgesetzbuch (HGB) vom 20.04.2013 (10.05.1897).
http://www.gesetze-im-internet.de/hgb/index.html [abgerufen am: 03.08.2013].

Heinrich, Gert; Horstschäfer, Anna (2013): Das interne Kontrollsystem beim Einsatz elektronischer Archivierungsverfahren. In: *HMD* – Praxis der Wirtschaftsinformatik (289), S. 70–78.
http://www.wiso-net.de/webcgi?START=A60&DOKV_DB=ZECO&DOKV_NO=HMD78B945BA46D98400AB4E5548DB6459C2&DOKV_HS=0&PP=1 [abgerufen am: 08.08.2013].

Hochschule für Technik und Wirtschaft Dresden / Fakultät Wirtschaftswissenschaften (2009): Merkblatt für die Erstellung der Studienabschlussarbeit.
http://www.htw-dresden.de/fileadmin/userfiles/wiwi/Downloads/allgemein/Merkblatt09_end.pdf [abgerufen am: 02.08.2013].

Hofferberth, Dorothee, 12.04.2013. Mündliche Auskunft an Autorin.

Hofferberth, Dorothee, 05.06.2013. E-Mail an Autorin.

Hofferberth, Dorothee, 26.07.2013. E-Mail an Autorin.

Industrie- und Handelskammer Frankfurt am Main (2008): Gesellschafts- und kapitalmarktrechtliche Grundlagen von Compliance: Vortrag im Rahmen des Seminars „Prävention und Management aktueller Unternehmensrisiken: Compliance in Unternehmen“ des Deutschen Aktieninstituts am 22.04.2008 in der Industrie und Handelskammer Frankfurt am Main.
http://www.frankfurt-main.ihk.de/recht/themen/unternehmensrecht/compliance/ [abgerufen am: 02.08.2013].

Institut für Informationswissenschaft der Fachhochschule Köln: Kölner Arbeitspapiere zur Bibliotheks- und Informationswissenschaft.
http://www.fbi.fh-koeln.de/institut/papers/arbeitspapiere.php [abgerufen am: 02.08.2013].

Institut für Informationswissenschaft der Fachhochschule Köln: PubLIS Cologne – Institutionelles Repositorium (ab Mitte 2012).
http://www.fbi.fh-koeln.de/institut/papers/abschlussarbeiten/publis.php [abgerufen am: 02.08.2013].

IT-Wissen – Das große Online-Lexikon für Informationstechnologie (2013): USV (Unterbrechungsfreie Stromversorgung).
http://www.itwissen.info/definition/lexikon/Unterbrechungsfreie-Stromversorgung-UPS-uninterruptable-power-supply-USV.html [abgerufen am: 02.08.2013].

Keens, Walter, 08.05.2013. E-Mail an Autorin.

Keens, Walter, 24.05.2013. E-Mail an Autorin.

Keens, Walter, 23.07.2013. E-Mail an Autorin.

Köhler, Thomas R.; Kirchmann, Walter (2008): IT von A bis Z: Das schnelle und kompakte Nachschlagewerk. Frankfurt am Main: Frankfurter Allgemeine Buch.

Konrad-Zuse-Zentrum für Informationstechnik Berlin (2012): OPUS 4: Überblick. http://www.kobv.de/opus4/ueberblick/ [abgerufen am: 02.08.2013].

Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe OAIS-Übersetzung/Terminologie (2012): Referenzmodell für ein Offenes Archiv-Informations-System. Deutsche Übersetzung (Nestor-Materialien, 16).
http://files.d-nb.de/nestor/materialien/nestor_mat_16.pdf [abgerufen am: 02.08.2013].

Nestor – Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung (2008): Nestor-Kriterien: Kriterienkatalog vertrauenswürdige digitale Langzeitarchive; Version 2 (Nestor-Materialien, 8).
http://files.d-nb.de/nestor/materialien/nestor_mat_08.pdf [abgerufen am: 02.08.2013].

Neuroth, Heike; Oßwald, Achim; Scheffel, Regine; Strathmann, Stefan; Huth, Karsten (Hg.) (2010): Nestor-Handbuch: Eine kleine Enzyklopädie der digitalen Langzeitarchivierung. Version 2.3. Nestor – Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit Digitaler Ressourcen für Deutschland.
http://nestor.sub.uni-goettingen.de/handbuch/nestor-handbuch_23.pdf [abgerufen am: 02.08.2013].

Norm DIN 31644 (2012): Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive.

Odenthal, Roger (2007): Digitale Archivierung: Leitfaden. Frechen: Datakontext.

PDF/A Competence Center (2011): Validierung von PDF/A.
http://www.pdfa.org/2011/09/validierung-von-pdfa/?lang=de#pdf_a-validierungprodukte [abgerufen am: 02.08.2013].

PDF-Association: FAQ zu PDF/A.
http://www.pdfa.org/competence-center/pdfa-competence-center/antworten-auf-haufig-gestellte-fragen-zu-pdfa/?lang=de [abgerufen am: 03.08.2013].

Q-Perior AG (2012): Optimierung und Prüfung des Internen Kontrollsystems (IKS): Die Q-Perior AG und ihre Leistungen.
http://www.revisionswelt.de/media/qp/Download/qperior-praesentation-optimierung-und-pruefung-des-internen-kontrollsystems-iks.pdf [abgerufen am: 03.08.2013].

Rösch, Hermann, 09.04.2013. Mündliche Auskunft an Autorin.

Signature Perfect KG (2008): Leitfaden Elektronische Signatur: Elektronische Signatur mit und ohne Zertifikat; Elektronische Signatur mit eigenhändiger Unterschrift. In Zusammenarbeit mit SigLab; Version 5.
http://www.signature-perfect.de/docs/Leitfaden_Elektronische_Signatur.pdf [abgerufen am: 03.08.2013].

Signaturgesetz (SigG) vom 17.07.2009 (16.05.2001).
http://www.gesetze-im-internet.de/sigg_2001/ [abgerufen am: 03.08.2013].

Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim (2011): Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen. 2., überarbeitete Auflage. Wiesbaden: Vieweg + Teubner.

Technische Universität Kaiserslautern: Glossar zu Begriffen der Informationskompetenz: Persistent Identifier.
http://glossar.ub.uni-kl.de/begriff550 [abgerufen am: 03.08.2013].

ZDB-OPAC – Sigelsuche: PubLIS Cologne.
http://dispatch.opac.ddb.de/DB=1.2/SET=5/TTL=1/CMD?ACT=SRCHA&IKT=8549&SRT=LST_os&TRM=k%F6ln+fachhochschule+publis [abgerufen am: 07.08.2013].

Zentraler Kreditausschuss (2008): Brief des Zentralen Kreditausschusses an den Vorsitzenden des Finanzausschusses des Deutschen Bundestages, Herrn Eduard Oswald, MdB: Regierungsentwurf für ein Gesetz zur Modernisierung und Entbürokratisierung des Steuerverfahrens (Steuerbürokratieabbaugesetz).
http://bankenverband.de/downloads/102008/sp0810-st-buerokratie-zka.pdf, [abgerufen am: 03.08.2013].

Zivilprozessordnung (ZPO) vom 05.12.2005 (12.09.1950).
http://www.gesetze-im-internet.de/zpo/__371a.html [abgerufen am: 03.08.2013].

Empfehlung einer Abschlussarbeit des IWS zur Veröffentlichung im institutseigenen Repositorium PubLIS Cologne

(**Bitte zusammen mit der Kopie des Anmeldeformulars an Frau Hofferberth weitergeben)**

☐ Bachelorarbeit

☐ Masterarbeit

von Frau/Herrn

Thema der Arbeit:

☐ Einzelarbeit ☐ Gruppenarbeit

Der Volltext der Abschlussarbeit soll im Repositorium auf folgender Ebene sichtbar sein:

☐ Weltweit (gute bis sehr gute Abschlussarbeit)

☐ FH-weit (gute bis noch gute Arbeit)

☐ Nur für admin (befriedigende und ausreichende Abschlussarbeit)

Die Abschlussarbeit

☐ hat einen Sperrvermerk (s. Bemerkungen)

☐ ist nicht bestanden

☐ ist aus anderen Gründen nicht zur Veröffentlichung geeignet (s. Bemerkungen)

Bemerkungen:

Erstgutachter:

Unterschrift

_____

Fachhochschule Köln
Cologne University of Applied Sciences

Fakultät für
Informations- und Kommunikationswissenschaften

Antrag auf Zulassung zur Bachelorarbeit ☐ Bibliothekswesen ☐ Informationswirtschaft

Bitte 3-fach einreichen, eine Kopie verbleibt beim Erstgutachter

Fachhochschule Köln . Claudiusstraße1 . 50678 Köln

Name und Anschrift:

Frau/Herrn

_____

_____

_____

Matrikel-Nr.:_____
(die ersten 8 Ziffern)

Telefon-Nr.:_____

Email-Adresse:_____

☐ 1. Versuch ☐ 2. Versuch

Thema der Bachelorarbeit (bitte in Druckbuchstaben einsetzen):

_____

_____

_____

Gruppenarbeit mit: _____

Vorbehaltlich der Zustimmung des Erstgutachters bin ich mit der Veröffentlichung der Arbeit auf einem Repositorium der Fachhochschule Köln einverstanden ☐ nicht einverstanden ☐ *

Betreuer/in:	Unterschrift _____ (bitte vor Abgabe einholen)
2. Gutacher/in:	Unterschrift _____ (bitte vor Abgabe einholen)

Köln, den _____
(Datum / Unterschrift Antragsteller/in)

Die Zulassungsvoraussetzungen
Lt. § 35 BPO sind erfüllt: _____
(Datum / Unterschrift Studienbüro)

Zur Bachelorarbeit zugelassen: _____
(Datum / Unterschrift Prüfungsausschuss)

Noch fehlende Prüfungen: _____

Mitteilung des Studienbüros

Die Bachelorarbeit mit o.g. Thema muss gem. § 35 BPO bis zum _____ im Studienbüro der FH Köln gedruckt in 3-facher Ausfertigung sowie im Format PDF/A ebenda auf CD eingereicht werden.
Bei Postzustellung ist das Datum des Poststempels maßgebend. Im Übrigen gelten die Regelungen der BPO.

Köln, den _____ _____
(Fristbeginn) (Unterschrift Studienbüro)

Bachelorarbeit abgegeben am: _____ _____
(Unterschrift Studienbüro)

* Informationen zum Repositorium s. nächste Seite

Informationen zum Hochschulschriftenserver des Instituts für Informationswissenschaft

Der Dokumentenserver PubLIS Cologne des Instituts für Informationswissenschaft der Fachhochschule Köln besteht seit 2012 und bietet Metadaten und Volltexte digitaler Publikationen und Qualifizierungsarbeiten von Mitgliedern und Absolventen des Instituts (http://publiscologne.fh-koeln.de/home). Die neuen Abschlussarbeiten werden zeitnah, die Arbeiten der zurückliegenden Jahre sukzessiv aufgenommen.

Die/der Autor/in einer Abschussarbeit wird gebeten, sich direkt bei Anmeldung der Arbeit zu entscheiden, ob er/sie einverstanden ist, dass der Volltext – vorbehaltlich der Zustimmung des Erstgutachters – auf diesem Server veröffentlicht werden kann. Das dritte Exemplar des Anmeldeformulars mit dem entsprechenden Votum verbleibt daher beim Gutachter.

Der Erstgutachter spricht nach der Notenvergabe eine Empfehlung zur Veröffentlichung aus, nach der die Abschlussarbeiten je nach Qualität in unterschiedlichem Umfang zugänglich gemacht werden:

- Volltexte und Metadaten weltweit, in Bibliothekskatalogen und Internetsuchmaschinen recherchierbar
- Volltexte und Metadaten nur hochschulweit
- Metadaten hochschulweit, Volltexte nur für den Admin aufrufbar

Metadaten und Dokumente werden gemäß dem aktuellen Erkenntnisstand zur digitalen Langzeitarchivierung dauerhaft archiviert und stehen unter Bezugnahme auf die Creative Commons-Lizenzen der Öffentlichkeit entgeltfrei zur Verfügung. Das Institut für Informationswissenschaft verwendet grundsätzlich die Creative Commons Lizenz "Namensnennung-Nicht Kommerziell-Keine Bearbeitung".

Bei weiteren Fragen wenden Sie sich bitte an Herrn Prof. Dr. Hermann Rösch (hermann.roesch@fh-koeln.de).