

HUMBOLDT-UNIVERSITÄT ZU BERLIN
INSTITUT FÜR BIBLIOTHEKS- UND INFORMATIONSWISSENSCHAFT



BERLINER HANDREICHUNGEN
ZUR BIBLIOTHEKS- UND
INFORMATIONSWISSENSCHAFT

HEFT 241

**ZUGANG ZU ELEKTRONISCHEN RESSOURCEN
FÜR EXTERNE BENUTZER IN
WISSENSCHAFTLICHEN BIBLIOTHEKEN**

KONZEPTION UND PRAKTISCHE ANWENDUNG

VON
JÖRG SIMANOWSKI

**ZUGANG ZU ELEKTRONISCHEN RESSOURCEN FÜR EXTERNE
BENUTZER IN
WISSENSCHAFTLICHEN BIBLIOTHEKEN**

KONZEPTION UND PRAKTISCHE ANWENDUNG

VON
JÖRG SIMANOWSKI

Berliner Handreichungen zur
Bibliotheks- und Informationswissenschaft

Begründet von Peter Zahn
Herausgegeben von
Konrad Umlauf
Humboldt-Universität zu Berlin

Heft 241

Simanowski, Jörg

Zugang zu elektronischen Ressourcen für externe Benutzer in wissenschaftlichen Bibliotheken : Konzeption und praktische Anwendung / von Jörg Simanowski. - Berlin : Institut für Bibliotheks- und Informationswissenschaft der Humboldt-Universität zu Berlin, 2008. – 87 S. : graph. Darst. - (Berliner Handreichungen zur Bibliotheks- und Informationswissenschaft ; 241)

ISSN 14 38-76 62

Abstract:

Ausgangspunkt der vorliegenden Arbeit sind Betrachtungen über die zunehmende Bedeutung elektronischer Ressourcen und die Auswirkung dieser Entwicklung auf eine serviceorientierte, wissenschaftliche Bibliothek.

Es folgt die Darstellung der bei der Nutzung elektronischer Ressourcen zu beachtenden rechtlichen Rahmenbedingungen. Im Ergebnis erweist es sich als notwendig, die vorhandenen Lokalen Bibliothekssysteme (LBS) um eine Komponente für einen rollenbasierten Zugang zu elektronischen Ressourcen zu erweitern. Dabei sind Kenntnis und Beachtung der in der Arbeit aufgeführten Rechtsnormen und Lizenzverträge nicht nur für Bibliotheken sondern generell für alle Einrichtungen der öffentlichen Hand relevant, die Dienstleistungen über einen Zugang zum Internet oder über die Bereitstellung lizenz- und kostenpflichtiger elektronischer Ressourcen für die Öffentlichkeit erbringen.

Im Rahmen der Arbeit wurde eine entsprechende Erweiterung eines LBS-PICA an der Universitätsbibliothek Rostock implementiert und unter Angabe der wesentlichen Abläufe und Einsatzszenarien sowie eines Aktionsplans für die Einführung dokumentiert. Diese wird neben anderen alternativen, ergänzenden und zukünftigen Lösungen betrachtet und soll einen Einstieg in die Thematik sowie eine Entscheidungshilfe für Planung und Einsatz entsprechender Funktionalitäten und Verfahren sein. Letztlich werden damit Forderungen der DFG umgesetzt, die in den aktuellen Empfehlungen für die Ausstattung von Hochschulbibliotheken mit Lokalen Bibliothekssystemen formuliert sind.

Diese Veröffentlichung geht zurück auf eine Master-Arbeit im postgradualen Fernstudiengang Master of Arts (Library and Information Science) an der Humboldt-Universität zu Berlin.

Online-Version: <http://www.ib.hu-berlin.de/~kumlau/handreichungen/h241/>

Inhaltsverzeichnis

1	Einleitung	7
1.1	Digitale Verfügbarkeit von Informationen	8
1.2	Nutzung standortunabhängiger Endgeräte.....	10
1.3	Bibliotheken auf dem globalen und vernetzten Informationsmarkt	11
1.4	Zugang zu elektronischen Ressourcen	14
1.5	Begriffsbestimmungen.....	17
2	Rechtliche Rahmenbedingungen	19
2.1	Authentifizierung versus „Walk-in“	20
2.2	Telekommunikationsüberwachung.....	22
2.2.1	Grundlagen	22
2.2.2	§ 110 TKG	22
2.2.3	§§ 113a, 113b TKG	25
2.2.4	Fazit Telekommunikationsüberwachung.....	27
2.3	Jugendschutz.....	28
2.3.1	Jugendmedienschutz.....	28
2.3.2	Fazit Jugendschutz.....	31
2.4	Lizenzverträge	32
2.4.1	Benutzergruppen in Lizenzverträgen.....	33
2.4.2	Beispiele für Lizenzverträge.....	33
2.4.3	Fazit Lizenzverträge	35
2.5	Benutzungsordnungen	36
2.5.1	Benutzungsordnung von Bibliothek und Rechenzentrum.....	36
2.5.2	Musterbenutzungsordnung DFN-Verein	38
2.5.3	Fazit Benutzungsordnungen	41
2.6	Rechtliche Rahmenbedingungen – Fazit und Konsequenzen.....	41
3	Umsetzung am Beispiel der UB Rostock	43
3.1	Organisatorische Grundlagen	43
3.2	Grundprinzipien der Implementierung	47
3.3	Technische Realisierung.....	47
3.3.1	Voraussetzungen.....	47
3.3.2	Abbildung der LBS-Benutzerverwaltung auf das Active Directory	48
3.3.3	Möglichkeiten der Zugangssteuerung	52

3.3.3.1	Booten, Softwareausführung (computer-based)	53
3.3.3.2	Sperren Benutzergruppen (role-based)	54
3.3.3.3	Ressourcen nicht beschränken (role-based)	54
3.3.3.4	Ressourcen beschränken mit Blacklist (role-based)	55
3.3.3.5	Ressourcen beschränken mit Black-/Whitelist (role-based)	56
3.3.3.6	Ressourcen beschränken (computer-based)	57
3.4	Organisatorische Realisierung	58
3.4.1	Planung (Aktionsplan) und Einführung.....	58
4	Alternativen und weitere Entwicklung	60
4.1	Lösung der UB Rostock.....	60
4.2	Alternative Lösungsansätze	62
4.2.1	Lösung der SUB Hamburg	62
4.2.2	H+H / Hidden Automatic Navigator (HAN)	63
4.2.3	OCLC / Identity Management Connector.....	64
4.2.4	OCLC / SISIS-SunRise webControl.....	65
4.3	AAI / Shibboleth.....	66
5	Schlussbemerkungen	69
Anhang		70
	Abkürzungsverzeichnis.....	70
	Literaturverzeichnis	73
	Anlage 1	84
	Anlage 2	87

1 Einleitung

„Wenn du und ich jeder einen Apfel haben und wir diese tauschen, dann hat danach immer noch jeder nur einen Apfel. Wenn du und ich jeder eine Idee haben und wir diese tauschen, dann hat danach jeder von uns zwei Ideen.“¹

Hans-Gert Gräbe

Mit Eintritt in die postmoderne Informationsgesellschaft Ende des 20. Jahrhunderts stehen die Bibliotheken als Einrichtungen der Informationsversorgung vor tiefgreifenden Veränderungen. Die gegenständliche Bibliothek mit ihren analogen Medien ist langsam aber sicher in Auflösung begriffen² und entwickelt sich zu einem „Service Bibliothek“³, der unter Nutzung aller technischen Möglichkeiten den Anforderungen der Benutzer gerecht werden muss. Dabei ist völlig offen, ob in Zukunft noch viele lokale oder nur wenige zentrale Einrichtungen diesen Service übernehmen werden.

Der „Service Bibliothek“ wird sich darauf einstellen müssen, dass zunehmend

- Informationen ausschließlich digital verfügbar sind,
- Benutzer über standortunabhängige Endgeräte verfügen und
- Dienstleistungen auf einem globalen und vernetzten Informationsmarkt zu erbringen sind.

Die in diesen drei Thesen formulierte Entwicklung ist vor allem bedingt durch das existierende globale Wirtschaftssystem und die technische Innovation in den Bereichen Informations- und Kommunikationstechnologie. Sie wird forciert durch das Internet und ist von enormer gesellschaftspolitischer Relevanz.

1 [\[Gräbe01\]](#)

2 Die Studien der letzten Jahre belegen, dass die Nutzung gedruckter Publikationen in wissenschaftlichen Bibliotheken nach wie vor von großer Bedeutung ist. Vgl. u. a. [\[HavemannKaufmann2006\]](#), S. 65-89.

3 Oder wie es Rainer Kuhlen formuliert: „Vom institutionellen zum funktionellen Bibliotheksverständnis“. In: [\[Kuhlen2008\]](#), S. 218.

Der Schwerpunkt der Aufgaben einer Bibliothek verschiebt sich aus dem Bereich der traditionellen und weitestgehend automatisierbaren Geschäftsprozesse in Richtung Vermittlung von Informationskompetenz und auf spezielle Bedürfnisse der Benutzer zugeschnittene Informationsvermittlung und Services⁴. Partizipierende Dienstleistungen, wie sie etwa von den auch in Bibliotheken vorhandenen Verfechtern des WEB 2.0 eingefordert werden, können zu einem mehr an Service und Qualität der angebotenen Dienstleistungen führen und sind als Chance zu verstehen, die Benutzer an den „Service Bibliothek“ zu binden⁵.

Sich nur auf die passive Bereitstellung von Informationen zu beschränken wird dazu führen, dass die Bibliothek als Einrichtung von den Benutzern nicht mehr wahrgenommen wird. Der Nutzer einer elektronischen Ressource, die von „seiner“ Bibliothek lizenziert wurde, ist nicht an die Benutzung eines Rechners in der Bibliothek gebunden. Er hat diese vielleicht in einer Verbunddatenbank, einem Portal oder einer Fachdatenbank recherchiert und kann so diesen Dienst nicht mehr mit einer Leistung „seiner“ Bibliothek in Verbindung bringen.

Diese Entwicklung, formuliert in den drei genannten Thesen, soll im Folgenden vor allem anhand von Beispielen aus dem Bereich der wissenschaftlichen Bibliotheken, unterlegt werden.

1.1 Digitale Verfügbarkeit von Informationen

Die Deutsche Forschungsgemeinschaft (DFG) finanziert seit 2004 mit etwa 15 Mio. Euro jährlich den Erwerb von Nationallizenzen, um die Versorgung mit elektronischer Fachinformation an deutschen Hochschulen, Forschungseinrichtungen und wissenschaftlichen Bibliotheken nachhaltig zu verbessern⁶. Die wissenschaftlichen Bibliotheken in Deutschland haben diese elektronischen Ressourcen selektiv in ihren Katalogen, in der Zeitschriftendatenbank (ZDB)⁷, im Datenbank-Infosystem (DBIS)⁸ und in der Elektronischen Zeitschriftenbibliothek (EZB)⁹ verzeichnet und zur Nutzung bereitgestellt.

4 Wie z.B. den Support für Autoren während des gesamten Lebenszyklus wissenschaftlicher Informationen/Publicationen, d.h. bei Recherche, Verfassen, Review, Publizieren und Archivieren.

5 So stand die Verbundkonferenz des Gemeinsamen Bibliotheksverbundes (GBV) 2007 in Bremen unter dem Motto „SUNRISE in Sicht - auf dem Weg zum Bibliothekssystem 2.0. Wohin entwickeln sich Bibliothekssysteme in Zeiten des Web 2.0?“. Internet: <http://www.suub.uni-bremen.de/verbundkonferenz/> [22.04.08]

6 Internet: <http://www.nationallizenzen.de/> [22.04.08]

7 Internet: <http://www.zeitschriftendatenbank.de/> [05.05.08]

8 Internet: <http://rzblx10.uni-regensburg.de/dbinfo/> [22.04.08]

9 Internet: <http://rzblx1.uni-regensburg.de/ezeit/> [22.04.08]

Mit der Digitalisierung großer Teile von Nationalbibliographien, wie z.B. die von Thomson Gale im Rahmen der Nationallizenzen angebotene Eighteenth Century Collections Online (ECCO)¹⁰, dem geplanten Digitalisierungsprojekt der Bayrischen Staatsbibliothek und Google¹¹ oder auch dem geplanten Aufbau des digitalen VD18¹² wird sich die Nutzung der Altbestände als eine der letzten Bastionen der analogen Bibliothek erheblich verringern.

Ein digitales Angebot von elektronischen Publikationen in Form von Hochschulschriften, Aufsätzen, Monographien, Nachschlagewerken usw. ist heute für jede wissenschaftliche Bibliothek, ihrem Aufgabenprofil entsprechend, selbstverständlich. Weitere Publikationsformen, wie etwa Protokolle und Forschungsprimärdaten, werden folgen. Umfangreiche elektronische Verlagsangebote, wie das der Springer Science+Business Media¹³ oder auch die im Rahmen der Nationallizenzen angebotene NetLibrary E-Book Collection¹⁴, haben längst Eingang in die Bibliothekskataloge gefunden. Während elektronischen Zeitschriften schon seit Jahren in wissenschaftlichen Bibliotheken genutzt werden, ist die Lizenzierung größerer Mengen an elektronischen Büchern seit etwa 2007 zu beobachten¹⁵. Die finanzielle Situation vieler wissenschaftlicher Bibliotheken sowie das sich verändernde Nutzungsverhalten hin zu elektronischen Medien führt zudem dazu, dass zunehmend auf die Print-Ausgaben zugunsten von „E-only“-Ausgaben verzichtet wird.

Publikations- und Dokumentenservices der Hochschulen bieten Dissertationen, Habilitationen, Diplom- und Magisterarbeiten, Schriftenreihen, Vorlesungsskripte, Lernmodule, digitalisierte Sammlungen u. a. m. ihren Benutzern an, arbeiten als

-
- 10 Die Eighteenth Century Collections Online (ECCO) von Thomson-Gale bietet Zugriff auf über 150.000 digitalisierte gedruckte Werke (E-Books), die zwischen 1701 und 1800 im Vereinigten Königreich veröffentlicht wurden. Internet: <http://gale.cengage.com/pdf/facts/ECCO.pdf> [22.04.08]
 - 11 Im Rahmen einer Public-Private-Partnership zwischen der BSB und Google ist die Digitalisierung des gesamten urheberrechtsfreien historischen Bestandes der BSB an Druckwerken geplant. Internet: http://www.bsb-muenchen.de/Massendigitalisierung_im_Rahme.1842+M567632dd262.0.html [22.04.08]
 - 12 Verzeichnis der im deutschen Sprachraum erschienenen Drucke des 18. Jahrhunderts (VD18). Die im Auftrag der DFG erstellte Machbarkeitsstudie wurde durch den Ausschuss für wissenschaftliche Bibliotheken und Informationssysteme der DFG Ende 2007 gebilligt. Siehe auch [Haller2007].
 - 13 SpringerLink ist ein fächerübergreifendes Portal, das eine Vielzahl von heterogenen Primärquellen unter einer Oberfläche anbietet: elektronische Zeitschriften, Bücher und Buchreihen, Nachschlagewerke sowie Protokolle. Internet: <http://springerlink.com/> [22.04.08]
 - 14 NetLibrary wurde als einer der größten E-Content Provider 2002 von OCLC erworben. Internet: <http://www.netlibrary.com/> [22.04.08]
 - 15 So weist die Nutzungsstatistik der Universitätsbibliothek Rostock für das Jahr 2007 ca. 155.000 Vollanzeigen von Zeitschriftenartikeln und ca. 92.000 Vollzugriffe auf E-Books aus, im Januar 2008 erfolgten bereits ca. 24.000 Vollzugriffe auf E-Books.

OAI-Data-Provider¹⁶, sammeln selbst via OAI-PMH¹⁷ ausgewählte Metadaten und verlinken die zugehörigen Volltexte¹⁸.

Projekte wie LOCKSS¹⁹ ermöglichen es den Bibliotheken, lizenzierte Verlagsangebote vor Ort zu hosten und damit eine hohe Verfügbarkeit und Performance beim Zugriff auf die digitalen Publikationen zu gewährleisten. Verlage wie Annual Reviews, BioMed Central, Institute of Physics, Sage Publications, Taylor and Francis und Wiley-Blackwell, um nur einige zu nennen, stellen ihre Angebote für die Speicherung in LOCKSS-Boxen zur Verfügung.

Kaum ein Verlag, der seine Zeitschrift oder Zeitung nicht in einer Online-Version über das Internet anbietet. Verlage öffnen ihre Zeitschriften- und Zeitungsarchive für die kostenfreie Online-Nutzung²⁰ und Anbieter führender Enzyklopädien sind durch das Angebot preiswerter bzw. kostenloser Angebote gezwungen, Online-Versionen in ihren Geschäftsmodellen zu berücksichtigen²¹.

1.2 Nutzung standortunabhängiger Endgeräte

Die Universitäten bieten Ihren Angehörigen zunehmend einen Wireless-Zugang zum Wissenschaftsnetz an. In der Folge solcher Projekte wie der BMBF-geförderten Notebook-Universität²² wurden ganze Hochschulen mit der benötigten Wireless-Technik ausgestattet, so dass insbesondere Campus-Universitäten wie z.B. Bielefeld oder Bremen aber auch solche über die Stadtfläche verteilten Universitäten wie

16 Open Archives Initiative (OAI) - Data-Provider bieten die Daten ihrer Dokumentserver zur Abfrage über das Protocol for Metadata Harvesting (PMH) an. Internet: <http://www.openarchives.org/> [22.04.08]

17 Ebd.

18 Referenzen sind hier z.B. die Elektronische Bibliothek der Staats- und Universitätsbibliothek Bremen „E-LIB“ (Internet: <http://elib.suub.uni-bremen.de/> [15.05.08]) oder der Dokumenten- und Publikationsserver der Humboldt-Universität zu Berlin „edoc“ (Internet: <http://edoc.hu-berlin.de/> [15.05.08]). Die Elektronische Bibliothek der SUUB Bremen weist für den April 2008 ca. 18,5 Mio. Datensätze aus, darunter ca. 6,7 Mio. zu den lokalen Beständen der SUUB, ca. 8,5 Mio. zu Zeitschriftenaufsätzen und ca. 2,9 Mio. via OAI-PMH eingesammelte und zu Volltexten verlinkte Datensätze (Auskunft Martin Blenkle, 7.4.08).

19 An “Lots of Copies Keep Stuff Safe” (LOCKSS) sind nach Abfrage der LOCKSS-Site vom 30.07.08 derzeit 7 deutsche Einrichtungen beteiligt, aus dem angloamerikanischen Sprachraum (USA, Kanada, UK) 154. Internet: <http://www.lockss.org/lockss/> [30.07.08]

20 Namhafte Beispiele sind hier Der Spiegel (Internet: <http://wissen.spiegel.de/wissen/> [15.05.08]), Focus (Internet: <http://www.focus.de/service/archiv/> [15.05.08]), Die Zeit (Internet: <http://www.zeit.de/archiv/> [15.05.08]) oder auch die New York Times (Internet: <http://www.nytimes.com/ref/membercenter/nytarchive.html> [15.05.08]).

21 Hier sind vor allem die Microsoft Encarta Anfang der 90'er und Wikipedia ab 2001 zu nennen, die nicht unwesentlich zum Erscheinen von Online-Versionen der Encyclopedia Britannica (Internet: <http://www.britannica.com/> [15.05.08]) und der Brockhaus-Enzyklopädie (Internet: <http://www.brockhaus.de/> [15.05.08]) beigetragen haben.

22 Internet: http://www.medien-bildung.net/notebook/notebook_6.php/hochschule/notebook/ [22.04.08]

Rostock über eine nahezu flächendeckende Versorgung im Bereich der wichtigsten Universitätsgebäude verfügen²³.

Die fast zeitgleiche Einführung von Lern-Management-Systemen wie Stud.IP, ILIAS oder Moodle lässt die Anzahl der Notebookbesitzer und damit WLAN-Nutzer an den Universitäten rasant in die Höhe schnellen²⁴. Dienste wie DFNRoaming gestatten Wissenschaftlern und Studenten längst den Zugang zum Wissenschaftsnetz auch in anderen wissenschaftlichen Einrichtungen außerhalb der eigenen Hochschule.

Während die Installation von Access-Points für einen WLAN-Betrieb ohne Antrag und Genehmigung möglich ist und dadurch Überlagerungen und Störungen der Aktionsbereiche nicht ausgeschlossen sind²⁵, erfolgt für den Breitband Wireless Access (BWA) eine regulierte Zuweisung der Frequenzbereiche durch die Bundesnetzagentur. Diese Übertragungstechnik kann in Zukunft die Basis für einen sicheren und leistungsfähigen funkgestützten Breitband-Zugang zum Internet bilden.

Auch außerhalb des Campus können Studenten und Mitarbeiter die elektronischen Ressourcen der Universität nutzen. Studentenwohnheime sind verkabelt und gestatten den Zugang zum Campus-Netz via VPN oder Terminalserver. Tarife von unter 30 Euro für eine monatliche Flatrate inkl. Telefonie in das deutsche Festnetz mit einem DSL-Anschluss und einer Bandbreite von bis zu 16MBit/s ermöglichen einen ausreichend leistungsfähigen und bezahlbaren Zugang zum Internet und zum Campus-Netz. Preiswerte WLAN-Router bringen das drahtlose Netz auch in die entferntesten privaten Haushalte.

1.3 Bibliotheken auf dem globalen und vernetzten Informationsmarkt

Die Anforderungen an den „Service Bibliothek“ steigen bei sinkenden oder stagnierenden finanziellen und personellen Kapazitäten. Ohne nationale und internationale Kooperation bei strikter Anwendung der internationalen Standards werden die benö-

23 So sind an der Universität Rostock derzeit ca. 250 Access-Points installiert, über die im Normalbetrieb ca. 300 Notebooks zeitgleich auf das Campusnetz zugreifen. Die Universität Bremen betreibt mehr als 400 Access-Points für ihre Mitarbeiter und Studierenden.

Siehe [ZML2004] und im Internet: <http://www.suub.uni-bremen.de/benutzung/wlan/> [22.04.08]

24 So stehen z.B. an der Universität Rostock im Jahre 2008, 5 Jahre nach der Einführung des Projektes stud.IP, 11.727 aktive Accounts von Studierenden, 82 Administratoren für 794 Dozenten und 503 Tutoren, 284 Einrichtungen in 17 Fakultäten, 2.890 aktive und 1.607 archivierte Veranstaltungen zu Buche, kaum eine Lehrveranstaltung die das System nicht benutzt. (Angaben April 2008 bei ca. 14.000 Studierenden, 330 Professoren und 1.000 wissenschaftlichen Mitarbeitern)

25 Siehe Ausführungen der Bundesnetzagentur zu WLAN-Funkanwendungen (Wireless Local Area Network), Stand vom 11.06.2007. Internet: http://www.bundesnetzagentur.de/enid/24e93bcb3dd1884f5cc7d51820b20611.0/Allgemeinzuteilungen/WLAN_dv.html [22.04.08]

tigten Leistungen nicht erbracht werden können. Ein Thema wie die Langzeitarchivierung digitaler Objekte²⁶, mit dem nicht nur die Nationalbibliotheken konfrontiert sind, macht dieses sehr deutlich.

Dass Bibliotheken schon auf einem globalen und vernetzten Informationsmarkt agieren, lässt sich vor allem an der Entwicklung ihres Kernprodukts, der Erschließung und Bereitstellung von Medienwerken²⁷ jeglicher Art über Online-Kataloge veranschaulichen.

Die kooperative Erschließung in Verbunddatenbanken bei Einsatz einheitlicher Lokalsysteme in den angeschlossenen Bibliotheken²⁸, der Austausch von bibliographischen Daten zwischen Verbänden und Bibliotheken, Datenlieferungen wie die der Nationalbibliotheken DNB und LoC oder von Nielsen BookData und Casalini stellen bereits einen großen Anteil der Titeldaten für die Katalogisierung der lokalen Bestände der beteiligten Bibliotheken bereit²⁹. Im Rahmen von „Catalogue-Enrichment“-Projekten digitalisieren die Verbände kooperativ und abgestimmt große Mengen Inhaltverzeichnisse von Monographien und ermöglichen deren Nutzung über ihre Online-Kataloge. Hinzu kommt die Anreicherung mit weiteren Sacherschließungsdaten und „Publisher-descriptions“, wie etwa die der LoC. Die Einbindung von Volltextsuchmaschinen wie Lucene oder FAST schafft die Verbindung zur digitalen Bibliothek, Suche und Zugriff auf Volltexte können so direkt über den Online-Katalog erfolgen.

Die Internationalisierung der Regelwerke, insbesondere die Einführung von RDA in Verbindung mit FRBR, die Verwendung des einheitlichen Austauschformates MARC21 sowie die Implementierung einheitlicher Schnittstellen für den Austausch der Daten, wie etwa des OAI-PMH oder von Zing/SRU³⁰, wird diese Entwicklung noch beschleunigen, den Anteil der eingespielten bibliographischen Daten weiter erhöhen und den der manuellen Formal- und Sacherschließungsarbeiten weiter verringern.

26 Die Problematik Langzeitarchivierung wird im Rahmen von nestor, dem Kompetenznetzwerk zur Langzeitarchivierung digitaler Quellen in Deutschland, ausführlich dokumentiert.

Internet: <http://langzeitarchivierung.de/> [22.04.08]

27 Medienwerk in Anlehnung an [DNB2006].

28 Wie im Beispiel des GBV derzeit mit dem einheitlichen Einsatz von LBS-PICA als Lokalsystem für wissenschaftliche Bibliotheken. In anderen Verbänden, wie etwa dem SWB, sind auch heterogene lokale Systeme im Einsatz.

29 Siehe Protokoll der Facharbeitsgruppe Erschließung und Informationsvermittlung im GBV vom 2.9.2003, TOP1. Eine Ausnahme bei der Übernahme von Titeldaten bilden sicherlich noch die Spezial- und SSG-Bibliotheken.

Internet: https://www.gbv.de/cls-download/fag-erschliessung-und-informationsvermittlung/protokolle/ii-2003-2005/fagei_prot_030902.pdf [22.04.08]

30 ZING/SRU: Z39.50 International Next Generation. Internet: <http://www.loc.gov/standards/sru/> [22.04.08]

Hinzu kommt die Konzentration der Kataloge aus den Verbundsystemen, die aktuell mit dem Aufbau eines nationalen Katalogsystems im Rahmen des Projektes „Kooperative Neukatalogisierung“ fortgesetzt wird, in dem alle an der AG der Verbundsysteme beteiligten Verbände und Bibliotheken ihre Daten regelmäßig austauschen, so dass Nova in Zukunft nur einmal erfasst werden müssen und dann allen am Datenaustausch beteiligten Partnern zur Verfügung stehen.³¹

Selbst ein „Weltkatalog“ unter internationaler Beteiligung wissenschaftlicher Bibliotheken, wie der von OCLC betriebene WorldCat³², ist inzwischen eine denkbare Option für die Zukunft.

Damit gehen die Verbände über ihre Aufgaben der Anfangszeit, die im Wesentlichen im Aufbau der Struktur für eine kooperative Erschließung sowie der Organisation von Dokumentenlieferung und Fernleihe bestanden, weit hinaus und entwickeln sich zu Dienstleistungsverbänden, die in Zusammenarbeit von Verbundzentrale und Bibliotheken, organisiert in themenbezogenen Gremien und Arbeitsgruppen, inzwischen fast das gesamte Spektrum des „Service Bibliothek“ bearbeiten.³³

Für die Bibliotheken ist die kooperative Arbeit in einem Verbund existenziell. Kaum eine größere Bibliothek wird noch in der Lage sein, die vielfältigen Anforderungen aus eigener Kraft so zu bewältigen, dass sie eine „exzellente“ Informationsversorgung, wichtiger Faktor im globalen Wettbewerb der um Mittel und Studenten konkurrierenden Hochschulen, sicherstellen kann.

31 Dazu im Bericht der 53. Sitzung der AG Verbundsysteme: „Ziel des Projektes Kooperative Neukatalogisierung, an dem alle deutschsprachigen Verbände (BVB, GBV, hbz, HeBIS, KOBV, OBV, SWB und ZDB) sowie die Deutsche Nationalbibliothek (DNB) beteiligt sind, ist die Erarbeitung von Maßnahmen zur Verbesserung der Datenübernahme im Bereich Formal- und Sacherschließung der Verbände untereinander. Schwerpunkte hierbei sind die Senkung der Eigenkatalogisierungsquote, die Anreicherung von Katalogisaten mit zusätzlichen Informationen (Sacherschließung, TOCs usw.) und die Angleichung bzw. Vereinheitlichung von Regelwerksanwendung, Formatanwendung und Qualitätsstandards in den Verbänden.“

Internet: http://www.d-nb.de/standardisierung/pdf/ag_verbund_sitzungsbericht_53.pdf [22.04.08]

32 WorldCat ist die derzeit größte bibliographische Datenbank der Welt. Auch einige deutsche Bibliotheken spielen bereits ihre Metadaten in den WorldCat ein. Internet: <http://worldcat.org/> [22.04.08]

33 Vgl. Ziel- und Leistungsvereinbarung (ZLV) 2008 der Verbundleitung des GBV mit der Verbundzentrale (VZG). Die Dienstleistungen reichen inzwischen bis in die Arbeitsbereiche der Hochschulen hinein, wenn z.B. solche Komplexe wie Identity-Management, Universitätsbibliographie oder Dokumentenserver bearbeitet werden. Internet: http://www.gbv.de/vgm/info/biblio/02GBV/PDF/PDF_3404.pdf [22.04.08]

1.4 Zugang zu elektronischen Ressourcen

Die angeführten Beispiele sind ein Beleg dafür, dass sich die Bedingungen für die Nutzung elektronischer Ressourcen in den letzten 10 Jahren erheblich verändert haben. E-Campus und E-University und damit der „Service Bibliothek“ sind in Bereichen bereits Realität geworden und dennoch ist es ungewiss und aus heutiger Sicht nur schwer vorstellbar, dass das gedruckte Buch und mit ihm die gegenständliche Einrichtung Bibliothek jemals vollständig verschwinden wird.

Der „Service Bibliothek“ muss sich dabei mit gesellschaftspolitischen und zunehmend globalen Prozessen und Strukturen auseinandersetzen. Eine Gesellschaft, in welcher der Zugang zu den benötigten Informationen über das Leben und die Existenz ihrer Mitglieder maßgeblich bestimmt, die von allen „Informationskompetenz“ und „Lebenslanges Lernen“ fordert, sollte auch dafür Sorge tragen, dass alle ihre Mitglieder eine faire Chance haben, an die dafür benötigten Informationen zu gelangen.

Sowohl auf internationaler als auch auf nationaler Ebene ist das Recht eines jeden Menschen auf Meinungsfreiheit, welches ohne den ungehinderten Zugang zu den zur Meinungsbildung wichtigen und notwendigen Informationen, ohne die dazugehörige Informationsfreiheit, nicht gewährleistet werden kann, festgeschrieben. In Art. 19 der unter dem Eindruck der Ereignisse des 2. Weltkriegs durch die Vereinten Nationen 1948 verabschiedeten Allgemeinen Erklärung der Menschenrechte heißt es:

*„Jeder hat das Recht auf Meinungsfreiheit und freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, Meinungen ungehindert anzuhängen sowie über Medien jeder Art und ohne Rücksicht auf Grenzen Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten.“*³⁴

Für die Mitgliedstaaten des Europarats wird durch Art. 10 der Europäischen Menschenrechtskonvention ein Mindeststandard für die Meinungsfreiheit geschaffen, an den die Mitgliedsstaaten der Europäischen Union, mit Ausnahme von Großbritannien, in Artikel 11 der Charta der Grundrechte gebunden sind und der ab 2009 Bestandteil eines zukünftigen Europäischen Verfassungsvertrages werden soll³⁵. Das Grundgesetz für die Bundesrepublik Deutschland schreibt in Artikel 5 die Meinungs-

34 [\[AEMR\]](#)

35 Siehe Presseerklärung der Bundesregierung zu den Ergebnissen des Europäischen Rates vom 23.06.2007. Internet: http://www.bundesregierung.de/nn_1264/Content/DE/Artikel/2007/06/2007-06-23-ergebnisse-europaeischer-rat-bruessel.html [22.04.08]

und Informationsfreiheit sowie die Freiheit von Kunst, Wissenschaft, Forschung und Lehre fest³⁶.

Für die heute existierende, markt- und verwertungsorientierte Gesellschaft sind Wissen und Informationen zunehmend als Faktor im Reproduktionsprozess von Bedeutung. Humankapital wird als Grundlage für die Erschließung des „Rohstoffs Wissen“ kalkuliert und Verwertungsprozesse durchziehen alle Bereiche des öffentlichen und privaten Lebens. Die Tendenz, Informationen und Wissen wie gegenständliche Waren zu behandeln und durch deren Verknappung Gewinne zu realisieren, gerät dabei zunehmend in Widerspruch zu den deklarierten Rechten auf Meinungs- und Informationsfreiheit und den Erfordernissen zur Lösung globaler Menschheitsprobleme³⁷.

Die Entwicklung der Fachinformationspolitik in Deutschland ist dafür ein anschauliches Beispiel. Nach zunehmender Marktorientierung und Verfolgung des Subsidiaritätsprinzips Anfang der 80er Jahre im Rahmen der auf das IuD-Programm folgenden Fachinformationsprogramme, der Reduktion von Fachinformation auf wissenschaftlich-technische Fachinformation, der Entdeckung von „Information als Rohstoff“ und der Abwicklung wichtiger für eine umfassende und qualifizierte Entwicklung der Fachinformationspolitik erforderlicher Strukturen³⁸ sind das Aktionsprogramm der Bundesregierung „iD2010 – Informationsgesellschaft Deutschland 2010“ des BMWi³⁹ und das daraus resultierende Förderprogramm des BMBF „IKT2020 - Forschung für Innovation“⁴⁰ offene Subventionsprogramme für relevante Schlüsseltechnologien der Wirtschaft. Das propagierte „market pull [...] technology push“⁴¹ ist lediglich mit einer Schwerpunktförderung für „Anwendungsfelder/Branchen, in denen Innovationen in hohem Maße IKT-getrieben sind“⁴² verbunden, um „damit aus FuE-Ergebnissen auch wirtschaftliche Erfolge zu generieren“⁴³.

36 [\[GG\]](#)

37 „Die Weltgesundheitsorganisation WHO schätzt, dass weltweit bis zu 1,7 Mrd. Menschen von Krankheiten bedroht sind, die mit Hilfe existierender Medikamente relativ einfach geheilt werden könnten, dass aber der Zugang zu diesen Medikamenten durch bestehende Schutzrechte geistigen Eigentums und den damit verbundenen extrem hohen Monopolpreisen, nur wenigen vorbehalten ist.“ [\[SchiedchenSpennemann2007\]](#)

38 Vgl. [\[Broschard2001\]](#). Gedacht ist hierbei vor allem an die 1977 gegründete Gesellschaft für Information und Dokumentation (GID), die auf Basis des 1984 vom Wissenschaftsrat erstellten Gutachtens aufgelöst wurde und an das 1978 gegründete Deutsche Bibliotheksinstitut (DBI), dessen Finanzierung ebenfalls nach einem Gutachten des Wissenschaftsrates 1999 eingestellt wurde.

39 [\[BMW2006\]](#)

40 [\[BMBF2007\]](#)

41 Ebd., S. 65.

42 Ebd., S. 24.

43 Ebd., S. 4.

Auf internationaler Ebene finden diese Bestrebungen ihren Ausdruck im TRIPS-Abkommen, welches als Teil der WTO-Charta Fragen des Umgangs mit geistigen Eigentumsrechten regelt. Die Frage des Urheberrechts wurde im WIPO Copyright Treaty 1996 festgeschrieben, ist seitdem auf dem Weg in europäisches und bundesdeutsches Recht⁴⁴ und nicht erst seit der Verabschiedung des 2. Korbs der Urheberrechtsreform⁴⁵ im März 2006 auch ein Thema für deutsche Bibliotheken.

Die Wissenschaftsgemeinschaft wendet sich im Rahmen verschiedenster Initiativen gegen eine vollständige Vermarktung der Wissenschaft und setzt sich für einen freizügigen Zugang zu den für Bildung und Wissenschaft benötigten Wissensgütern ein.

So haben Vertreter von Forschungsorganisationen 2003 die „Berliner Erklärung über offenen Zugang zu wissenschaftlichem Wissen“ unterzeichnet und damit ein wichtiges Signal für den freien Zugang zu Informationen und gegen eine Privatisierung geistigen Eigentums gesetzt⁴⁶. Das Aktionsbündnis „Urheberrecht für Bildung und Wissenschaft“ setzt sich für einen 3. Korb der Urheberrechtsreform ein und wendet sich gegen die Abtretung von exklusiven Verwertungsrechten an kommerzielle Verlage im öffentlichen Bereich von Bildung und Wissenschaft⁴⁷.

Wenn sich die vorliegende Masterarbeit mit dem Thema „Zugang zu elektronischen Ressourcen für externe Benutzer in wissenschaftlichen Bibliotheken“ beschäftigt, dann mit der Intention, dass durch einen kontrollierten Zugang zu den elektronischen Ressourcen den geltenden Rechtsnormen Rechnung getragen werden muss, die Bibliothek dabei aber den Zugang im Rahmen ihrer Möglichkeiten nicht mehr als notwendig einschränkt und damit allen ihren Benutzern ein Maximum an elektronischen Fachinformationen und Dienstleistungen zur Verfügung stellt.

Die mit der Implementierung einer Erweiterung des Lokalen Bibliothekssystems (LBS) um einen rollenbasierten Zugang zu elektronischen Ressourcen verfolgten Ziele, wie im Rahmen dieser Arbeit an der Universitätsbibliothek Rostock erfolgt, sind somit auf die **Erfüllung des Auftrags der Bibliothek** und die **Beachtung der bestehenden Rechtsnormen** gerichtet.

44 Siehe auch [Gräbe2005Okt], S.297-313 sowie [Kuhlen2008].

45 „Zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft“ (Zweiter Korb) trat am 1. Januar 2008 in Kraft, (BGBl. I 2007. 2512 ff. vom 31. Oktober 2007).

46 Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities. Berlin, Oktober 2003. Internet: http://oa.mpg.de/openaccess-berlin/berlin_declaration.pdf [22.04.08]

47 Siehe „Göttinger Erklärung zum Urheberrecht für Bildung und Wissenschaft vom 5. Juli 2004“. Internet: <http://www.urheberrechtsbuendnis.de/> [22.04.08]

1.5 Begriffsbestimmungen

Elektronische Ressourcen

Elektronische Ressourcen sind alle netzgebundenen digitalen Objekte bzw. unkörperlichen Medienwerke, d.h. „*alle Darstellungen in Schrift, Bild und Ton, die [...] in unkörperlicher Form [...] zugänglich gemacht werden [können]*“⁴⁸, wobei die Art der Dienste oder Programme, die zu ihrer Darstellung genutzt werden und Medium und Ort ihrer Speicherung vollkommen unerheblich sind. Als elektronische Ressourcen werden netzgebundene Online-Werke betrachtet, die drahtlos oder drahtgebunden über ein im Internet oder Intranet befindliches Endgerät im Sinne des Urheberrechtsgesetzes „*Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich*“⁴⁹ sind.

Externe Benutzer

Externe Benutzer sind im Sinne des Telekommunikationsgesetzes (TKG) alle Benutzer einer Bibliothek, die der Öffentlichkeit zugerechnet werden können, d.h. die nicht „*in gesellschaftsrechtlichen oder schuldrechtlichen Dauerbeziehungen oder nichtvertraglichen, aber dauerhaften Verbindungen zur Verfolgung gemeinsamer beruflicher, wirtschaftlicher oder hoheitlicher Ziele stehen*“⁵⁰ und damit keine geschlossene Benutzergruppe bilden.

Geschlossene Benutzergruppen sind in diesem Sinne z.B. alle Angehörigen einer Hochschule oder Forschungseinrichtung, die die Bibliothek ihrer Einrichtung nutzen, alle Abgeordneten, die ihre Parlamentsbibliothek nutzen oder auch alle Angestellten einer Firma, die ihre Firmenbibliothek nutzen. Dass in den jeweiligen Bibliotheken nur solche Informationen bereitgestellt werden, die der Verfolgung der gemeinsamen beruflichen, wirtschaftlichen oder hoheitlichen Ziele der jeweiligen geschlossenen Benutzergruppe dienen, sei hier als selbstverständlich vorausgesetzt.

Externe Benutzer sind in diesem Sinne z.B. die Benutzer einer Stadtbibliothek, denen schwerlich eine dauerhafte Verbindung und ein gemeinsamer Zweck zugeordnet werden kann, die also im Sinne des TKG mit der Allgemeinheit (Öffentlichkeit) gleichgesetzt werden müssen.

Zugang und Öffentlichkeitsbegriff

Es ist zwischen dem Öffentlichkeitsbegriff im urheberrechtlichen Sinne der öffentlichen Zugänglichmachung eines Werkes und dem Öffentlichkeitsbegriff in Bezug auf das Erbringen von Telekommunikationsdienstleistungen zu unterscheiden.

48 Gesetz über die Deutsche Nationalbibliothek vom 22. Juni 2006 (BGBl. I S. 1338). [[DNB2006](#)]

49 UrhG § 19 a. [[UrhG](#)]

50 Schütz, In: Beck'scher TKG-Kommentar, 2. Auflage 2000, Rn. 29.

Während die Bereitstellung des Zugangs zum Internet für alle Angehörigen einer Hochschule keine Erbringung einer Telekommunikationsdienstleistung für die Öffentlichkeit ist, da diese eine geschlossene Benutzergruppe bilden, ist die Aufführung eines urheberrechtlich geschützten Werkes während einer Vorlesung mit Studenten und Mitarbeitern einer Universität eine öffentliche Zugänglichmachung und bedarf der Zustimmung des Urhebers bzw. Rechteinhabers, es sei denn, es handelt sich um eine nach § 52a UrhG⁵¹ erfolgte öffentliche Zugänglichmachung für Unterricht und Forschung, die aber mit Einschränkungen verbunden ist.

Wissenschaftliche Bibliotheken

Die Betrachtungen werden auf wissenschaftliche Bibliotheken beschränkt, die ein Teil von juristischen Personen des öffentlichen Rechts sind, wie z.B. Staats-, Landes- oder Universitätsbibliotheken⁵². Diese haben, im Gegensatz zu den meisten öffentlichen Bibliotheken, bereits größere Mengen an elektronischen Ressourcen lizenziert. Die beispielhafte Implementierung einer Erweiterung des Lokalen Bibliothekssystems (LBS) um einen rollenbasierten Zugang zu elektronischen Ressourcen im Rahmen dieser Arbeit erfolgte in einer Universitätsbibliothek, deren Access-Provider der DFN-Verein ist⁵³. Generell sind die behandelten Fragestellungen für alle Bibliotheken relevant, deren Benutzer keine geschlossene Benutzergruppe bilden, die also auch externen Benutzern den Zugang zu elektronischen Ressourcen gestatten.

51 [\[UrhG\]](#)

52 Die einzige Bibliothek in Deutschland, die für sich eine rechtsfähige juristische Person des öffentlichen Rechts darstellt, ist die Deutsche Nationalbibliothek. Ansonsten sind Bibliotheken ein nichtrechtsfähiger (unselbständiger) Teil von juristischen Personen des öffentlichen Rechts, die als Stiftungen oder Körperschaften fungieren, wie z.B. die Staatsbibliothek zu Berlin als Teil der Stiftung Preußischer Kulturbesitz oder die Universitätsbibliothek Rostock als Teil der Universität Rostock. Vgl. [\[Kirchner1991\]](#), S.33 ff.

53 Komponenten und Funktionalitäten eines Lokalen Bibliothekssystems können den Empfehlungen der DFG für die Ausstattung von Hochschulbibliotheken mit lokalen Bibliothekssystemen im HBBG-Verfahren (AHLB) entnommen werden. Danach sind Lokale Bibliothekssysteme „vernetzte Systeme aus Arbeitsplatzrechnern und Serverrechnern mit Anbindung an Hochschulnetze und externe Netze“ (S.7), die ein Funktionsmodul zur Bereitstellung digitaler Medien enthalten, welches „in diesem Kontext alle erforderlichen technischen Komponenten für Erfassung, Speicherung und Verwaltung, Erschließung und Nachweis, sowie für Zugriff und Nutzung digitaler Medien durch Bibliotheksbenutzer zur Verfügung [stellt]“ (S.17). Ebenso wird mehrfach auf die rechtlichen Rahmenbedingungen eingegangen, die vor allem durch Lizenzvereinbarungen oder allgemeine urheber- und verwertungsrechtliche Bestimmungen bedingt sind und es erfordern, dass „Lokale Bibliothekssysteme [...] daher technische Komponenten enthalten [müssen], die sicherstellen, dass die mit den einzelnen Informationsobjekten verknüpften Rechte bei Zugriff und Nutzung nicht verletzt werden können“ (S.12). So wird in Zusammenhang mit der Vertragsgestaltung zur Internetanbindung von Hochschulen über das Wissenschaftsnetz durch den DFN-Verein auch gefordert, dass „das lokale Bibliothekssystem zumindest zwischen internen und externen Benutzern unterscheiden können sowie – davon abhängig – den Zugang zu weiteren Informationsquellen steuern [muss]“ (S.13). [\[AHLB2003\]](#)

2 Rechtliche Rahmenbedingungen

Betrachtet werden die rechtlichen Rahmenbedingungen, die für den Zugang der Benutzer zu den durch die Bibliothek angebotenen elektronischen Ressourcen maßgeblich sind. Wenn im Folgenden von Normen die Rede ist, dann sind damit ausschließlich Rechtsnormen gemeint. Die vollständigen und zitierfähigen Bezeichnungen der Normen finden sich im Literaturverzeichnis. Folgende Normen bzw. Verträge sind wesentlich für den rechtlichen Rahmen und Gegenstand dieser Arbeit⁵⁴:

- Telekommunikationsüberwachung, insbesondere auf Grundlage:
 - o TKG⁵⁵ in Verbindung mit TKÜV⁵⁶, TR TKÜ⁵⁷ (, TVerleihV⁵⁸)
 - o GG⁵⁹, G 10⁶⁰
 - o StPO⁶¹
- Jugendschutz, insbesondere auf Grundlage:
 - o JuSchG⁶², JMStV⁶³
 - o TMG⁶⁴
- Lizenzverträge
- Benutzungsordnungen
 - o der Bibliothek
 - o des Rechenzentrums auf Grundlage der Musterordnung des DFN-Vereins

54 Nicht näher eingegangen wird auf Bestimmungen zum Datenschutz z.B. bzgl. der Speicherung von Verkehrsdaten oder auch der Einführung von Identitätsmanagement-Systemen (vgl. auch [Köcher2006] und [Dierking2005]). Geltende Normen sind vor allem das Bundesdatenschutzgesetz (BDSG) sowie die jeweiligen Landesdatenschutzgesetze. Die Speicherung der Benutzerdaten im hier beschriebenen Projekt erfolgt ausschließlich innerhalb des Lokalen Bibliothekssystems unter Einhaltung der datenschutzrechtlichen Grundsätze (Erforderlichkeit, Zweckbindung, Datensparsamkeit) und wird durch die schriftliche Einwilligung der Benutzer (§ 4a BDSG, § 7 Abs. 1 DSGVO M-V) bei Anmeldung durch die Anerkennung der Benutzungsordnung (§ 4 Abs. 10) bestätigt. Unterrichtung und ggf. schriftliche Freigabe durch den Datenschutzbeauftragten (§ 4g BDSG, § 19 DSGVO M-V) sollten erfolgen.

55 Telekommunikationsgesetz (TKG). [TKG]

56 Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TKÜV). [TKÜV]

57 Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜ). [TRTKÜ]

58 Telekommunikations-Verleihungsverordnung (TVerleihV): wird neben § 3 Nr. 19 TKG vom 25. Juni 1996 zur näheren Bestimmung des Begriffs „geschlossene Benutzergruppe“ herangezogen. [DBV2006], S. 1043.

59 Grundgesetz für die Bundesrepublik Deutschland (GG). [GG]

60 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10). [G10]

61 Strafprozeßordnung (StPO). [StPO]

62 Jugenschutzgesetz (JuSchG). [JuSchG]

63 Jugenschutzgesetz und Jugendmedienschutz-Staatsvertrag der Länder (JMStV). [JuSchG_JMStV]

64 Telemediengesetz (TMG). [TMG]

2.1 Authentifizierung versus „Walk-in“

Bibliotheken gestatten Ihren Benutzern auf verschiedene Art und Weise den Zugang zu elektronischen Ressourcen. Neben Bibliotheken, die generell nur registrierten Bibliotheksbenutzern oder Hochschulangehörigen via Authentifizierung Zugang gewähren, gibt es auch Bibliotheken, die den Zugang für nicht registrierte Bibliotheksbenutzer, sogenannte „Walk-in-User“, an einzelnen drahtgebundenen Arbeitsplätzen oder vielleicht auch drahtlos über WLAN erlauben. Aus verschiedenen Gründen gestaltet sich die Zulassung von „Walk-in-Usern“ problematisch. Die Einhaltung der hier zu betrachtenden Normen ist eng mit der Authentifizierung der Benutzer verbunden und für „Walk-in-User“ überhaupt nur dann möglich, wenn für die entsprechenden Arbeitsplätze erhebliche Einschränkungen an Funktionalität in Kauf genommen werden. Folgende Argumente sprechen gegen die Bereitstellung von Arbeitsplätzen für „Walk-in-User“:

Anzahl der Benutzer

Mit der Zulassung von „Walk-in-Usern“ kann keine genaue Aussage über die Anzahl der potentiellen Benutzer getroffen werden, was aber bei einer Anwendung der Ausnahmevorschrift § 3 Abs. 2 Nr. 5 TKÜV in Zusammenhang mit einer möglichen Verpflichtung nach § 110 TKG von Bedeutung ist.

Verpflichtung zur Benutzungsordnung

„Walk-in-User“ haben nicht zwingend die Benutzungsordnung der Bibliothek anerkannt und sind damit auch nicht dem dort deklarierten Zweck der wissenschaftlichen, nichtkommerziellen Nutzung verpflichtet. Die Bildung einer geschlossenen Benutzergruppe ist bei Zulassung von „Walk-in-Usern“ nicht zu realisieren.

Gruppen- oder rollenbasierte Dienstleistungen und Ressourcen

Bibliothekssysteme fassen ihre registrierten Benutzer in Gruppen zusammen und können dementsprechend bei Kopplung an einen Verzeichnisdienst gruppen- oder rollenbasierte Ressourcen und Dienstleistungen nach Authentifizierung des Benutzers automatisch zuweisen. Beispiele hierfür wären ein Druckservice mit Bezahlungsfunktion, der nur mit authentifizierten Benutzern umzusetzen ist, die Gestaltung des Zugangs zu den elektronischen Ressourcen, deren Nutzung durch Lizenzverträge oft auf bestimmte Benutzergruppen festgelegt ist, oder die notwendige Einschränkung des Internetzugangs für Jugendliche. Für einen „Walk-in-User“ würde das bedeuten, dass an dem betreffenden Arbeitsplatz alle entsprechenden elektronischen Ressourcen gesperrt werden müssten, was in der Realität wohl heißen mag, dass es sich um einen Katalogarbeitsplatz handelt, der den Zugang auf wenige ausgewählte

und für die Öffentlichkeit bestimmte Ressourcen reduziert und damit den Arbeitsplatz in seiner Funktionalität erheblich einschränkt.

Sicherheit

Wenn Benutzer ohne Authentifizierung Zugang zu Arbeitsplätzen in der Bibliothek haben, besteht eine wesentlich höhere Gefahr, dass

- Unbefugte auf IT-Systeme oder Daten Zugriff nehmen können,
- die Verursacher von Problemen nicht identifiziert werden können
oder
- die Herkunft von Daten nicht bestimmt werden kann⁶⁵.

Das setzt natürlich voraus, dass bei einer Authentifizierung die entsprechenden Informationen (Verkehrsdaten) auch gespeichert werden⁶⁶. Wenn § 113a TKG wegen der derzeitigen Rechtsunsicherheit und einer möglichen Verpflichtung erst ab dem 1. Januar 2009 momentan noch außer Acht gelassen werden kann, ergibt sich z.B. auf Grundlage von § 100 Abs. 1 TKG (zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen) oder § 100 Abs. 3 TKG (zum Aufdecken sowie Unterbinden von Leistungerschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste) unter bestimmten Bedingungen eine begrenzte Möglichkeit der Speicherung von Bestands- und Verkehrsdaten⁶⁷. Eine andere Option ist eine Dienstvereinbarung mit der Personalvertretung, die eine längere Speicherung der Verkehrsdaten der **Mitarbeiter** einer Einrichtung ermöglicht und genaue Festlegungen zu deren Auswertung enthält. Eine weitergehende Speicherung von Verkehrsdaten der **externen Benutzer** ist nur mit deren Zustimmung möglich. Die Auswertung der Daten kann im Falle von Störattacken auf das Datennetz für den „Schutz der Netzinfrastrukturen, aber auch [...] [für] den Schutz der Nutzer vor Schadsoftware und betrügerischer Inanspruchnahme ihrer Zugangsberechtigungen“⁶⁸ erfolgen oder auch im Fall eines rechtswidrigen Verhaltens Dritter von Bedeutung sein, so dass eine Einrichtung wegen Verletzung von Prüfungs- und Kontrollpflichten nicht in Haftung genommen werden kann, bzw. ihrerseits Schadensersatzansprüche geltend machen kann, wenn Benutzer an den von ihr bereitgestellten Endgeräten mit Zugang zum Internet gegen geltende Normen, wie z. B. Straf-, Jugendschutz- und Urheberrechtsgesetz verstoßen oder beispielsweise rechtswidrig kostenpflichtige Internetangebote nutzen.

65 Siehe auch Informationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).
Internet: <http://www.bsi.bund.de/gshb/> [22.04.08]

66 Vgl. auch [Hoeren2008], S. 407 ff.

67 Siehe Köcher, Jan K.: Speicherfristen von Verkehrsdaten an Hochschulen. [Köcher2006]. Aktuell LG Darmstadt: Urteil v. 06.06.2007 Az. 10 O 562/03 und AG Bonn: Urteil v. 5.7.2007 Az. 9 C 177/07 mit einer maximalen Speicherfrist von 7 Tagen.

68 [Schaar2007]

2.2 Telekommunikationsüberwachung

2.2.1 Grundlagen

Die folgenden Ausführungen folgen der 2006 erstellten Stellungnahme der DBV-Rechtskommission⁶⁹, dem Protokoll der Beratung von Vertretern des DFN-Vereins und der bayrischen Bibliotheken 2006 in Würzburg⁷⁰ und den aktuellen Unterlagen auf der Website des DFN-Vereins zum Thema „Recht im DFN“⁷¹.

Nach Art. 10 Abs. 1 des Grundgesetzes (GG) ist das Fernmeldegeheimnis als Grundrecht garantiert. Art. 10 Abs. 2 GG schränkt dieses Grundrecht jedoch ein und erlaubt Eingriffe in das Fernmeldegeheimnis, wenn dafür eine gesetzliche Ermächtigungsgrundlage vorhanden ist. Ermächtigungsgrundlagen hierfür ergeben sich aus § 100a StPO, dem G 10, dem Zollfahndungsdienstgesetz und den Polizeigesetzen der Länder und stehen in der Regel unter Richtervorbehalt oder wie im Beispiel des G 10 auch unter parlamentarische Kontrolle. Berechtigte Stellen für die Durchführung der Überwachungsmaßnahmen sind dem entsprechend Ermittlungsbeamte der zuständigen staatlichen Behörden.

2.2.2 § 110 TKG⁷²

Das Telekommunikationsgesetz (TKG) ist eine Norm mit dem Ziel der Regulierung des Wettbewerbs auf dem Telekommunikationsmarkt und dient der Umsetzung diverser europäischer Richtlinien. Die zuständige Regulierungsbehörde ist die Bundesnetzagentur⁷³. Unter bestimmten Voraussetzungen sind die Betreiber von Telekommunikationsanlagen (TK-Anlagen), die einen Zugang zum Internet bereitstellen, nach § 110 TKG in Verbindung mit TKÜV und TR TKÜ zur Errichtung von Überwachungseinrichtungen verpflichtet.

Eine Verpflichtung nach § 110 TKG würde bedeuten, dass:

- diverse Benachrichtigungs-, Berichts- und Prüfungspflichten gegenüber der Bundesnetzagentur bestehen (§§ 5 ff. TKÜV),
- Überwachungseinrichtungen vorgehalten werden müssen⁷⁴,
- und die Umsetzung auf eigene Kosten zu erfolgen hat (§ 110 Abs. 9 TKG).

69 [DBV2006], S. 1040-1049.

70 [DFNBIB2006], Anlage 1.

71 DFN-Verein: Recht im DFN. Internet: <http://www.dfn.de/de/beratung/rechtimdfn/> [22.04.08]

72 § 110 TKG - Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften.

73 Internet: <http://www.bundesnetzagentur.de/> [22.04.08]

74 Die technischen Spezifikationen der Überwachungstechnik werden durch die Bundesnetzagentur in der TR TKÜ festgelegt. [TRTKÜ]

Verpflichteter ist nach § 110 TKG Abs. 1 derjenige, der **Betreiber einer TK-Anlage** ist, mit der **Telekommunikationsdienstleistungen für die Öffentlichkeit** erbracht werden und der **nicht unter den Tatbestand einer Ausnahmvorschrift nach § 3 Abs. 2 TKÜV** fällt, die für ihn die Anwendbarkeit des § 110 TKG ausschließt.

Betreiber einer Telekommunikationsanlage

Nach § 3 Nr. 23 TKG sowie nach § 2 Nr. 4 TKÜV sind Universitäten und der DFN-Verein als Access-Provider Betreiber von TK-Anlagen. Sie üben die tatsächliche Kontrolle über die Funktionen der TK-Anlagen aus und haben so die Möglichkeit des Zugriffs auf Informationen über die Telekommunikation der Benutzer.

Erbringen von Telekommunikationsdienstleistungen für die Öffentlichkeit

Der Öffentlichkeitsbegriff im Sinne des TKG sowie der Begriff des externen Benutzers wurden in Kapitel 1.5 unter Verwendung des Begriffs „geschlossene Benutzergruppe“ erläutert. Danach erbringen Bibliotheken, die jedermann den Zugang zum Internet gewähren, ob mit oder ohne Authentifizierung, Telekommunikationsdienstleistungen für die Öffentlichkeit und wären nach § 110 TKG verpflichtet. Im Gegensatz dazu erbringen Bibliotheken, die den Internetzugang lediglich für eine geschlossene Benutzergruppe gestatten, keine Telekommunikationsdienstleistungen für die Öffentlichkeit.

Ausnahmvorschriften nach § 3 Abs. 2 TKÜV

Für Bibliotheken, die jedermann Zugang zum Internet gewähren, ist die Anwendung einer Ausnahmvorschrift nach § 3 Abs. 2 TKÜV zu prüfen. Dabei ist zu berücksichtigen, dass nach § 3 Abs. 1 S. 2 TKÜV die Verpflichtung nach § 110 TKG und damit auch die Anwendung der Ausnahmvorschriften sich nur auf den Teil der TK-Anlage bezieht, der zur Erbringung von Telekommunikationsdiensten für die Öffentlichkeit genutzt wird, so dass bei einer Nutzung durch Hochschulangehörige (geschlossene Benutzergruppe) und externe Benutzer hier nur die Letzteren zu betrachten sind. Von Interesse sind die beiden Ausnahmvorschriften § 3 Abs. 2 Nr. 4 und Nr. 5 TKÜV:

„(2) Für Telekommunikationsanlagen im Sinne von Absatz 1 müssen keine Vorkehrungen getroffen werden, soweit [...]

4. sie ausschließlich der Verteilung von [...] für die Öffentlichkeit bestimmten Diensten, dem Abruf von allgemein zugänglichen Informationen oder der Übermittlung von [...] nicht individualisierten Daten [...] dienen, oder

5. an sie nicht mehr als 10.000 Teilnehmer oder sonstige Nutzungsberechtigte angeschlossen sind.“⁷⁵

75 [\[TKÜV\]](#)

§ 3 Abs. 2 Nr. 4 TKÜV

Da die Benutzung einer Bibliothek i.d.R. auch immer mit der Benutzung des Online-Katalogs verbunden ist und der Zugang zu den Daten des Benutzerkontos nur über eine Authentifizierung möglich ist, scheidet die Anwendung der Ausnahmegvorschrift § 3 Abs. 2 Nr. 4 TKÜV aus. Es kann auch nicht im Sinn der Bibliotheken sein, externe Benutzer von dieser Funktionalität auszunehmen, ist doch die Verbesserung des Angebots personalisierter Dienstleistungen grundlegend für die weitere Entwicklung und Nutzung der Online-Kataloge.

§ 3 Abs. 2 Nr. 5 TKÜV

Nach § 3 Nr. 20 TKG sind externe Benutzer keine Teilnehmer im Sinne des TKG, solange mit ihnen keine vertragliche Vereinbarung über die Erbringung derartiger Dienste abgeschlossen wird. In der Regel werden sich Bibliotheken ihren externen Benutzern gegenüber dazu weder schriftlich noch mündlich verpflichten. Bleibt die Frage, ob es sich bei den externen Benutzern um „sonstige Nutzungsberechtigte“ handelt. Zum Verständnis dieser Formulierung kann die Begründung des Verordnungsentwurfs für die Neufassung der TKÜV 2005 herangezogen werden. Dort heißt es auf Seite 25:

*„Die Ergänzung in Absatz 2 Satz 1 Nr. 5 um die Worte „oder sonstige Nutzungsberechtigte“ trägt neueren Entwicklungen Rechnung, die es ermöglichen, dass eine Telekommunikationsanlage auch Nutzer versorgen kann, die nicht zwingend als „Teilnehmer“ an sie angeschlossen sind, bei denen aber dennoch eine ggf. nur kurzfristige Nutzungsberechtigung vergeben wird (z. B. WLAN). Die Vorschrift wird ausdrücklich nicht auf „Nutzer“ bezogen, weil damit die Interpretation möglich wäre, dass hier auf die Zahl der gleichzeitig nutzenden Nutzer abgestellt würde; eine solche Interpretation würde aber nicht dem Ziel der Vorschrift entsprechen. **Ziel der Vorschrift ist vielmehr, auf die Größe einer TK-Anlage im Hinblick auf die Zahl der mit der Anlage potentiell zu versorgenden Nutzer abzustellen.**“⁷⁶*

Die Stellungnahme der DBV-Rechtskommission [[DBV2006](#)] kommt zu dem Schluss, dass „Wenn die Bibliothek für die externen [Be]Nutzer Zugang zum Internet über fest installierte PC's gewährt, an denen sie sich nicht registrieren müssen und externen [Be]Nutzern keinen Netzzugang über WLAN gestattet, [...] sie nach § 3 Abs. 2 Nr. 5 TKÜV von den Pflichten nach § 110 TKG zur Bereithaltung von Überwachungseinrichtungen ausgenommen [ist]“⁷⁷ und dass externe Benutzer, die lediglich fest installierte Internet-Arbeitsplätze nutzen, nicht an die TK-Anlage „angeschlossen“ sind, da ihnen kein eindeutiger Zugang im Sinne eines Telekommunikationsanschlusses zuzuordnen ist.

⁷⁶ Bundesrats-Dr. 631/05, S.25, Zu § 3 Abs. 1 und Abs. 2 Satz 1. [[BR63105](#)]

⁷⁷ Ebd., S. 1047.

„Da deren Anzahl in Bibliotheken in aller Regel nicht über 1.000 liegen dürfte, sind also schon keine 1.000 Anschlüsse vorhanden, und schon gar nicht sind die externen Benutzer selbst hier angeschlossen. Der eindeutig bezeichnete Zugang identifiziert hier einzig die Bibliothek bzw. Universität. Nur diese Einrichtungen sind also „angeschlossen“⁷⁸ so dass letztlich „wenn externen Benutzern der Zugriff auf das jeweils eigene Online-Benutzerkonto der Bibliothek oder auf E-Mail-Accounts bei anderen Diensteanbietern gestattet wird“⁷⁹ keine Verpflichtung nach § 110 TKG besteht. Im Interesse der Rechtssicherheit der Bibliotheken empfiehlt [DBV2006] aber, diese Interpretation der Ausnahmenvorschriften mit der Bundesnetzagentur zu beraten.

Denkbar wäre auch eine Interpretation dahingehend, dass externe Benutzer, ob mit oder ohne Authentifizierung, ob mit oder ohne WLAN-Zugang zum Internet, als „sonstige Nutzungsberechtigte“ im Sinne des § 3 Abs. 2 Nr. 5 TKÜV anzusehen sind. Eine solche Interpretation sollte dazu führen, einen Zugang ohne Authentifizierung auszuschließen, weil nur so die Anzahl der „potentiell zu versorgenden Nutzer“ genau bestimmt werden kann. Bibliotheken registrieren ihre Benutzer in Gruppen in ihren Bibliothekssystemen und haben dort die Hochschulangehörigen und die externen Benutzer klar getrennt. Wird das Bibliothekssystem an einen Verzeichnisdienst angebunden und eine rollenbasierte Authentifizierung ermöglicht, so kann jederzeit über die genaue Anzahl der „sonstigen Nutzungsberechtigten“ Auskunft gegeben werden. Bibliotheken mit weniger als 10.000 externen Benutzern würden demnach unter die Ausnahmenvorschrift § 3 Abs. 2 Nr. 5 TKÜV fallen. Für die anderen Bibliotheken, wenn es sich um wissenschaftliche Bibliotheken handelt, die lt. ihrer Benutzungsordnung auf eine wissenschaftliche Nutzung festgelegt sind, wäre die Möglichkeit der Erweiterung der geschlossenen Benutzergruppe zu prüfen. Dieses ist ein Weg, den Bibliotheken und DFN-Verein derzeit empfehlen⁸⁰ und der im Fazit zum Thema Telekommunikationsüberwachung unter Kap. 2.2.4 dargestellt wird.

2.2.3 §§ 113a, 113b TKG⁸¹

Diffizil ist die Betrachtung des § 113a zu Speicherungspflichten für Daten (Vorratsdatenspeicherung) und des § 113b zur Verwendung der nach § 113a gespeicherten Daten, da diesbezüglich noch diverse Klagen anhängig sind, denen durchaus Aussicht auf Erfolg zu bescheinigen ist. So hat das Bundesverfassungsgericht in seinem Beschluss zur Sache 1 BvR 256/08⁸² am 11. März 2008, einer Verfassungsbeschwer-

78 Ebd., S. 1048. Die Anhebung der Anzahl der sonstigen Nutzungsberechtigten von 1.000 auf 10.000 in § 3 Abs. 2 Nr. 5 TKÜV trat am 01.01.2008 in Kraft (BGBl I 2007, 3198).

79 Ebd., S. 1048.

80 [DFNBIB2006], Anlage 1.

81 § 113 a TKG - Speicherungspflichten für Daten.
§ 113 b TKG - Verwendung der nach § 113a gespeicherten Daten.

82 BVerfG, 1 BvR 256/08 vom 11.3.2008, Absatz-Nr. (1 - 188). [BVerfG25608]

de zum Erlass einer einstweiligen Anordnung zur Aussetzung von §§ 113a, 113b TKG, teilweise Recht gegeben. Die Ermächtigung zum Abruf der gespeicherten Verbindungsdaten wurde bis zur Entscheidung in der Hauptsache eingeschränkt und auf schwere Straftaten beschränkt, die alle Voraussetzungen nach § 100a Abs. 1 StPO erfüllen und einen Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG rechtfertigen. In den übrigen Fällen des § 100g Absatz 1 StPO sind die Verkehrsdaten zwar nach § 113a TKG zu speichern, aber von einer Übermittlung der Daten ist einstweilen abzusehen. Zudem hat die Bundesregierung dem Bundesverfassungsgericht zum 1. September 2008 nach Maßgabe der Gründe über die praktischen Auswirkungen der in § 113a des Telekommunikationsgesetzes vorgesehenen Datenspeicherungen und der vorliegenden einstweiligen Anordnung zu berichten.

Der Beschluss des BVerfG stellt zudem fest, dass *„Die Richtlinie 2006/24/EG [...] formell gemeinschaftswidrig und mit den von dem Europäischen Gerichtshof anerkannten Gemeinschaftsgrundrechten nicht vereinbar [sei]“*⁸³ und verweist auf die noch anhängige Klage der Republik Irland vor dem Europäischen Gerichtshof⁸⁴: *„Die Republik Irland hat am 6. Juli 2006 eine Klage vor dem Europäischen Gerichtshof erhoben, um gemäß Art. 230 EG die Richtlinie 2006/24/EG für nichtig erklären zu lassen (Rs. C-301/06). Zur Begründung hat sie ausgeführt, die Richtlinie sei kompetenzwidrig zustande gekommen. Sie ziele nicht auf Errichtung und Funktionsfähigkeit des europäischen Binnenmarktes ab, sondern diene in erster Linie Belangen der Strafverfolgung, hätte daher eine andere Kompetenzgrundlage erfordert und in der Folge nicht als Richtlinie, sondern nur als Rahmenbeschluss ergehen können, der gemäß Art. 34 Abs. 2 Satz 2 Buchstabe b EU Einstimmigkeit verlangt hätte. [...] Zudem kann derzeit nicht ausgeschlossen werden, dass der Europäische Gerichtshof die Richtlinie 2006/24/EG aufgrund der anhängigen Nichtigkeitsklage der Republik Irland (Rs. C-301/06) wegen der Inanspruchnahme eines nicht tragfähigen Kompetenztitels für nichtig erklären wird. Diese Klage erscheint angesichts der Erwägungen, mit denen die Klägerin die Kompetenzwidrigkeit der Richtlinie begründet, zumindest nicht von vornherein aussichtslos [...]“*⁸⁵

83 Ebd.

84 Vgl. [[RsC30106](#)].

85 Ebd.

Anzumerken ist noch, dass nach § 150 Abs. 12b TKG die „Anbieter von Internetzugangsdiensten, Diensten der elektronischen Post oder Internettelefondiensten [...] die sie treffenden Anforderungen aus § 111 Abs. 1 Satz 3 und § 113a spätestens ab dem 1. Januar 2009 zu erfüllen.“ haben.

Unabhängig von der derzeitigen Rechtsunsicherheit bzgl. §§ 113a, 113b TKG kann aber von der Intention des Gesetzgebers ausgegangen werden, für die Speicherung der Verkehrsdaten den Öffentlichkeitsbegriff analog zu § 110 TKG anzuwenden, d.h. dass für geschlossene Benutzergruppen keine Pflicht zur Speicherung besteht. Im Gesetzentwurf der Bundesregierung wird als Erläuterung zu § 113a Abs. 1 Satz 1 dazu ausgeführt, „dass für den nicht öffentlichen Bereich (z. B. unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten ausschließlich für dort immatrikulierte Studierende oder Bedienstete sowie die Telematikinfrastruktur im Gesundheitswesen) eine Speicherungspflicht nicht besteht.“⁸⁶

2.2.4 Fazit Telekommunikationsüberwachung

Geschlossene Benutzergruppe

Gestattet die Bibliothek lediglich einer geschlossenen Benutzergruppe den Zugang zum Internet, so ist sie von einer Verpflichtung nach § 110 TKG entbunden. Auch bei einer möglichen Entscheidung für die Vorratsdatenspeicherung nach § 113a TKG sollte kein Handlungsbedarf entstehen.

Externe Benutzer

Im Oktober 2006 trafen sich Vertreter der bayrischen wissenschaftlichen Bibliotheken und des DFN-Vereins in Würzburg und berieten zum Thema § 110 TKG. Das Protokoll der Sitzung⁸⁷ wurde anschließend über den DFN-Verein an die Rechenzentren der deutschen Universitäten verteilt. Im Ergebnis der Sitzung wird auf die Option der Bildung einer geschlossenen Benutzergruppe unter Einbeziehung der „sonstigen Bibliotheksbenutzer“, d.h. der nicht Hochschulangehörigen, fokussiert, was über die Benutzungsordnung (ABOB⁸⁸), entsprechende Hinweise bei der Nutzung der Endgeräte und eine zusätzliche schriftliche Erklärung des Benutzers, mit der er sich zur ausschließlich wissenschaftlichen Nutzung des Internet verpflichtet, realisiert werden soll. Im Ergebnis werden 2 Lösungsansätze offeriert:

86 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG1. S. 161. [TKÜ2007]

87 [DFNBIB2006], Anlage 1.

88 Allgemeine Benutzungsbedingungen der Bayrischen staatlichen Bibliotheken (ABOB) vom 18. August 1993. Internet: http://www.bsb-muenchen.de/Allgemeine_Benutzungsordnung.1438.0.html [22.04.08]

Lösungsansatz 1 – Authentifizierung und schriftliche Erklärung

- a) Alle Benutzer müssen sich authentifizieren, um Zugang zum Internet zu erhalten. Nur Benutzer der geschlossenen Benutzergruppe erhalten so Zugang zum Internet, außerdem werden die Sicherheitsrisiken minimiert.
- b) Voraussetzung für die Erteilung von Zugangsdaten und damit für die Aufnahme in die geschlossene Benutzergruppe ist die Prüfung des wissenschaftlichen Zwecks der Nutzung bei der Zulassung „nicht-hochschulangehöriger Benutzer“. Aus Nachweisgründen sollte eine schriftliche Erklärung verlangt werden.

Lösungsansatz 2 – unterschiedliche Provider für externe Benutzer und Hochschulangehörige

Für externe Benutzer wird ein privater Provider herangezogen, der Überwachungs-einrichtungen im Sinne des § 110 TKG bereits vorhält. Bestimmte Subnetze werden dann über den privaten Provider versorgt.

Der Lösungsansatz 1 wurde von den Beteiligten der Beratung als die bevorzugte Lösung dargestellt und ist auch die Grundlage für das in dieser Arbeit vorgestellte Konzept, welches an der Universitätsbibliothek Rostock umgesetzt wurde. Dabei sei noch einmal darauf verwiesen, dass unabhängig von der Interpretation zur Ausnahmenvorschrift § 3 Abs. 2 Nr. 5 TKÜV diese Maßnahmen zur Bildung einer geschlossenen Benutzergruppe, d.h. die Authentifizierung und die schriftliche Verpflichtung zur wissenschaftlichen Arbeit in der Bibliothek, als Grundlagen zur Umsetzung aller rechtlicher Rahmenbedingungen und damit als notwendig angesehen werden müssen.

2.3 Jugendschutz

Entsprechend der Gesetzgebungskompetenz von Bund und Ländern regelt der Bund im JuSchG den Schutz der Jugend in der Öffentlichkeit sowie die Verbreitung jugendgefährdender Schriften und Medieninhalte während die Länder im JMStV eine einheitliche Rechtsgrundlage für den Jugendschutz in den elektronischen Medien (Internet, Fernsehen, Rundfunk) geschaffen haben. Beide Normen stellen in der Sache ein einheitliches Gesetzeswerk dar, welches es ermöglicht, auf allen Ebenen nach einheitlichen Standards zu entscheiden.⁸⁹

2.3.1 Jugendmedienschutz

§ 3 Abs. 1 JMStV bestimmt Kinder und Jugendliche wie folgt: „*Kind im Sinne dieses Staatsvertrages ist, wer noch nicht 14 Jahre, Jugendlicher, wer 14 Jahre, aber noch nicht 18*

89 Jugendmedienschutz-Staatsvertrag (JMStV). [[JuSchG_JMStV](#)]

Jahre alt ist.“ Ein Blick in die Benutzungsordnung einiger wissenschaftlicher Bibliotheken zeigt, dass die Altersgrenze für die Zulassung zur Nutzung verschieden gehandhabt wird.

Die Staatsbibliothek zu Berlin differenziert in ihrer Benutzungsordnung unter § 4 (Zulassung zur Benutzung) verschiedene Nutzungsbereiche mit Altersgrenzen zwischen 16 und 18 Jahren und legt für die Benutzung der Internetarbeitsplätze fest: *„Benutzerinnen und Benutzern unter 18 Jahren ist die Benutzung der Internetarbeitsplätze nicht gestattet.“*⁹⁰

Die Universitätsbibliothek Rostock lässt neben den Mitgliedern und Angehörigen der Hochschulen des Landes zur Benutzung *„alle weiteren Personen, die im Land Mecklenburg-Vorpommern ihren amtlich gemeldeten Wohnsitz haben und das 16. Lebensjahr vollendet haben“*⁹¹ zu.

Die Staats- und Universitätsbibliothek Bremen bestimmt in ihrer Benutzungsordnung § 4 (Zulassung zur Benutzung) unter Abs. 3 : *„[...] Zusätzlich ist vorzulegen: [...] von Kindern und Jugendlichen bis zum vollendeten sechzehnten Lebensjahr eine schriftliche Einwilligung eines Erziehungsberechtigten, in der dieser sein Einverständnis zur Benutzung der Einrichtungen der Bibliothek erklärt und für die Forderungen aus diesem Nutzungsverhältnis eintritt.“*⁹²

Kinder oder Jugendliche sind also durchaus auch in Übereinstimmung mit den jeweiligen Benutzungsordnungen Benutzer wissenschaftlicher Bibliotheken.

§ 4 JMStV⁹³ legt die unzulässigen Angebote für die genannte Personengruppe fest, wobei Abs. 1 auf die Medien mit absolutem Verbreitungsverbot durch Rundfunk und Telemedien, Abs. 2 auf die Medien mit absolutem Verbot der Verbreitung durch Rundfunk und mit Verbot der Verbreitung an Kinder und Jugendliche durch Telemedien und Abs. 3 auf die Angebote, die geeignet sind, die Entwicklung von Kindern und Jugendlichen schwer zu gefährden, eingeht.

In § 5 JMStV wird auf entwicklungsbeeinträchtigende Angebote für Kinder und Jugendliche eingegangen und dem Anbieter solcher Angebote die Schaffung von Barrieren mittels technischer oder sonstiger Mittel auferlegt, die einen Zugang zu diesen Angeboten unmöglich machen oder wesentlich erschweren.

90 [\[SBB2007\]](#), S. 9.

91 [\[UNIRO2008\]](#), S. 4.

92 [\[SUUB2000\]](#), S. 4.

93 [\[JuSchG_JMStV\]](#), S. 69-74.

Bibliotheken sind keine Anbieter entwicklungsbeeinträchtigender Angebote im Sinne des JMStV. Mit dem Zugang zum Internet können sie bzw. ihr Access-Provider aber solche Angebote zugänglich machen, was für den Zweck von Forschung und Lehre durchaus auch notwendig sein kann. Klar ist auch, dass eine wirkliche Verhinderung des Zugriffs auf unzulässige Angebote im Ausland, die nicht mit den nationalen Normen zu greifen sind, durch technische Schutzmaßnahmen derzeit nur durch die Bibliothek bzw. das Rechenzentrum oder den Access-Provider ermöglicht werden kann.

Bibliotheken die Internet-Arbeitsplätze anbieten, sind Diensteanbieter im Sinne des § 2 Nr. 1 TMG und damit nach § 7 Abs. 1 TMG für eigene Informationen, die sie zur Nutzung im Internet bereitstellen, verantwortlich. Nach § 7 Abs. 2 TMG und §§ 8 bis 10 TMG sind sie für fremde Inhalte, die sie lediglich durchleiten, zwischenspeichern oder speichern, nur unter besonderen Voraussetzungen verantwortlich. Es gibt keine allgemeine Überwachungspflicht dahingehend, fremde Inhalte auf ihre Rechtmäßigkeit hin zu überprüfen. Allerdings können sie zur Sperrung oder Beseitigung erkannter rechtswidriger Inhalte aufgefordert werden und müssen im Einzelfall Inhalte prüfen, um einer Unterlassungsverpflichtung nachzukommen. So ergibt sich aus der Aufsichtspflicht und der Verfügungsgewalt über die Räumlichkeiten der Bibliothek, die in direktem Kontakt mit den Benutzern realisiert werden, eine Rechtspflicht zum Handeln, d.h. zur Sperrung entsprechender Angebote für Kinder und Jugendliche⁹⁴.

Auch durch eine Einwilligung der Erziehungsberechtigten in den möglichen Kontakt ihrer Schützlinge mit jugendgefährdenden Inhalten des Internet kann sich die Bibliothek ihrer bestehenden Verantwortlichkeit nicht entziehen, wie z.B. die Herausnahme des Erziehungsprivilegs aus § 184 StGB, der die Verbreitung pornographischer Schriften unter Strafe stellt, zeigt.⁹⁵

Derzeit geltende Rechtsauffassung im Sinne des Jugendschutzes ist es, Kindern und Jugendlichen in öffentlich zugänglichen Einrichtungen keinen Zugang zu Angeboten entspr. §§ 4, 5 JMStV in Bibliotheken zu gewähren, dieses entsprechend in der Benutzungsordnung zu verankern und durch technische oder sonstige Mittel sicherzustellen.

Dazu liegen die Rechtsauffassung der Obersten Landesjugendbehörden (OLJB)⁹⁶ sowie rechtliche Hinweise der Kultusministerkonferenz (KMK) zur Nutzung des

94 [\[LieschingGünter2000\]](#)

95 Ebd., S. 266.

96 [\[OLJB2005\]](#)

Internet an Schulen⁹⁷ vor. Auch von Seiten der Bibliotheken wurde sich bereits mit dem Thema auseinandergesetzt⁹⁸.

So wird in [OLJB2005] ausgeführt, dass:

„(1) Die Aufstellung von Computern [...] in öffentlich zugänglichen Einrichtungen wie Schulen, Einrichtungen der Kinder- und Jugendhilfe, Bibliotheken [...] sowie deren Vernetzung bzw. deren Anschluss an das Internet [...] grundsätzlich den Beschränkungen des JuSchG sowie des JMStV [unterliegen]. Die einschlägigen Regelungen (§§ 4, 6, 7, 8, 9, 10, 12, 13, 14, 15 JuSchG sowie §§ 4, 5 JMStV) sind zu beachten.“

„(6) Online verfügbare Inhalte dürfen nur zugänglich gemacht werden, wenn unter Berücksichtigung der §§ 4 und 5 JMStV sichergestellt ist, dass eine Jugendbeeinträchtigung oder -gefährdung ausgeschlossen ist. Dies ist sicherzustellen über:

- die Installierung einer geeigneten Filtersoftware*
- gelegentliche, stichprobenartige Kontrolle der aufgerufenen Seiten*
- durch Kontroll- oder Servicepersonal*
- gelegentliche Kontrolle des Internetprotokolls*
- einsehbare Aufstellung der Bildschirme.“*

2.3.2 Fazit Jugendschutz

Der Schutz von Kindern und Jugendlichen, so diese zur Benutzung der Bibliothek und ihrer Internet-Arbeitsplätze zugelassen sind, erfordert durch die Bibliothek die Beschränkung der abrufbaren Inhalte nicht nur über Festlegungen in der Benutzungsordnung sondern auch durch technische und organisatorische Maßnahmen. Kinder und Jugendliche können nicht in „geschlossenen Benutzergruppen“ der Verpflichtung zur Umsetzung dieser Normen entzogen werden, d.h. auch für Angehörige einer Einrichtung, etwa Studenten, die das 18. Lebensjahr noch nicht vollendet haben oder Schüler, die an Projekten an einer Universität mitarbeiten, sind die entsprechenden Regelungen zu beachten, wenn ihnen Zugang zum Internet gewährt wird. Auch die Einwilligung eines Erziehungsberechtigten entbindet die Bibliothek nicht von ihrer Verantwortung.

Online verfügbare Inhalte dürfen für Kinder oder Jugendliche nur dann zugänglich gemacht werden, wenn unter Berücksichtigung der §§ 4 und 5 JMStV durch techni-

97 Kultusministerkonferenz (KMK): Rechtliche Hinweise zur Nutzung des Internets an Schulen. Internet: <http://www.datenschutz.hessen.de/ds007a1.htm> [22.04.08]

98 Siehe z.B. im Internet: <http://www.bibliothekerverband.de/ko-recht/jugendschutz.html> [05.05.08]

sche und organisatorische Maßnahmen sichergestellt ist, dass eine Jugendbeeinträchtigung oder -gefährdung ausgeschlossen ist. So kann für Kinder und Jugendliche eine durch die Kommission für Jugendmedienschutz (KJM) zugelassene Filtersoftware eingesetzt werden. Dabei ist zu beachten, dass auch Filtersoftware ihre Grenzen hat und manuelle oder automatische Verfahren zur Generierung von Negativlisten derzeit keinen absoluten Schutz gewähren können.⁹⁹ Lediglich durch die Bereitstellung einer Positivliste (Whitelist) mit ausgewählten elektronischen Ressourcen kann die Nutzung von jugendgefährdenden Angeboten aus dem Internet praktisch ausgeschlossen werden. Die durch die OLJB vorgeschlagenen Überwachungsmaßnahmen, so diese in einer wissenschaftlichen Bibliothek überhaupt sinnvoll durchführbar sind, unterliegen den geltenden Normen zum Datenschutz. Ein genereller Ausschluss von der Nutzung des Internets ist nicht zu empfehlen, da gerade die Heranführung von Jugendlichen als potentiellen Studenten der Universitäten und Benutzer der wissenschaftlichen Bibliotheken gewünscht sein sollte. Online-Katalog und öffentliche Seiten der Einrichtung sollten auch für alle Kinder und Jugendlichen an Internet-Arbeitsplätzen in der Bibliothek zugänglich sein. Eine Option zur Erweiterung der Positivliste wären z.B. nach Sachthemen gegliederte und durch Bibliotheken aufbereitete Linksammlungen wie etwa die der Zentral- und Landesbibliothek Berlin¹⁰⁰ oder die der Deutschen Internetbibliothek (DIB)¹⁰¹.

2.4 Lizenzverträge

Wissenschaftliche Bibliotheken haben in der Regel bereits erhebliche Mengen an elektronischen Ressourcen für ihre Benutzer lizenziert. Dabei kann die Lizenzierung indirekt, wie im Falle der Nationallizenzen über die Deutsche Forschungsgemeinschaft (DFG), oder auch direkt durch Erwerb einzelner Ressourcen oder ganzer Pakete durch die einzelne Bibliothek oder im Rahmen verschiedener Konsortien¹⁰² erfolgen. Typische Publikationsformen für lizenzierte elektronische Ressourcen sind z.B. elektronische Zeitschriften (E-Journals) und Bücher (E-Books), Datenbanken und Nachschlagewerke (Reference Works). Lizenzverträge, die Bibliotheken mit den Anbietern elektronischer Ressourcen abschließen, sind letztlich Nutzungsvereinbarungen, zu deren Abschluss die Anbieter aufgrund der ihnen von den Urhebern übertragenen Verwertungsrechte berechtigt sind. Damit sind sie letztlich Ausdruck des geltenden Urheberrechts.

99 Vgl. [Schindler2000] und [GünterSchindler2006].

100 Linksammlung der Zentral- und Landesbibliothek Berlin (ZLB). Internet: <http://linksammlungen.zlb.de/> [15.05.08]

101 Deutsche Internetbibliothek (DIB). Internet: <http://www.internetbibliothek.de/> [22.04.08]

102 Konsortien, die sich wiederum in der German, Austrian and Swiss Consortia Organisation (GASCO) als überregionales Forum für Konsortien in Deutschland, Österreich und der Schweiz organisiert haben. Internet: http://www.hbz-nrw.de/angebote/digitale_inhalte/gasco/ [22.04.08]

2.4.1 Benutzergruppen in Lizenzverträgen

Wissenschaftliche Bibliotheken schließen Lizenzverträge zur Nutzung elektronischer Ressourcen in der Regel zu speziellen Konditionen für Forschung und Lehre ab, die sie gegenüber kommerziellen Nutzern bevorzugen, so es für die betreffenden Ressourcen einen gewinnträchtigen Markt gibt. Als Beispiel, auch ohne dass dem Autor vergleichbare Verträge dazu vorliegen, seien hier das „Juristische Informationssystem für die Bundesrepublik Deutschland“ (Juris-Online) der juris GmbH und „beck-online : die Datenbank“ des Verlags C. H. Beck oHG angeführt, deren Nutzung auch für Anwaltskanzleien nicht ganz unbedeutend sein dürfte. Die von den Bibliotheken abgeschlossenen Lizenzverträge enthalten genaue Angaben zur Art der Nutzung und den zur Nutzung zugelassenen Benutzergruppen.

2.4.2 Beispiele für Lizenzverträge

Im Folgenden werden mit Zustimmung des jeweiligen Verlages Auszüge aus einigen Lizenzverträgen aufgeführt. Verschiedene Bestimmungen bzgl. Art der Nutzung und zugelassenen Benutzungsgruppen können nicht gegeneinander gewertet werden, da keine Aussagen zu Preis oder Umfang der Nutzung gemacht werden. Die Auflistung der Beispiele erfolgt lediglich, um die Notwendigkeit eines rollenbasierten Zugriffs auch im Hinblick auf eine mögliche Nutzung durch externe Benutzer aufzuzeigen. Die aufgeführten Beispiele wurden als repräsentativ aus einer größeren Menge an Lizenzverträgen¹⁰³ herausgesucht.

- Produkt: CrossFire for Academic In-House-Licensees (CrossFire Beilstein)
 - “**PERMITTED USES**
 - [...] license is granted for internal research and educational purposes only.”*
 - “**NON-PERMITTED USES**
 - [...] allow any person(s) other than its faculty members, employees and students taking part in "not-for-profit" research [...]"*

- Produkt: Nature Archive License, Academic License
 - “**DELIVERY AND GRANT OF RIGHTS**
 - [...] for research, teaching, and private study purposes [...]*
 - USAGE RESTRICTIONS**
 - [...] for any commercial purpose;*
 - [...] other than Authorised Users;”*

103 Analysiert wurden ca. 30 Lizenzverträge, die die Universitätsbibliothek Rostock als eigenständige Lizenzverträge abgeschlossen hat oder denen sie im Rahmen von Konsortialverträgen beigetreten ist.

- Produkt: Thieme Connect, Standort-Lizenzvertrag
„LIZENZ
[...] zur ausschließlichen Nutzung im Rahmen ihrer Lehre, Forschung, Aus- und Weiterbildung und für persönliche Zwecke gemäß den Bestimmungen des vorliegenden Vertrages.
BERECHTIGTE BENUTZER
[...] alle derzeitigen Mitarbeiter, fest angestellten Lehrkräfte und Gastwissenschaftler sowie Studenten der Universität Rostock.“

- Produkt: RÖMPP-Lexika, Lizenzvertrag
„VERTRAGSGEGENSTAND
[...] ausschließlich solche Personen, welche in einem Dienst-, Arbeits-, Lehr-, Studien- oder Schulverhältnis zum Lizenznehmer stehen (z.B. Professoren, Lehrbeauftragte, wissenschaftliche Mitarbeiter, Doktoranden, eingeschriebene Studenten, Praktikanten, Arbeitnehmer der Universität oder ihrer Fakultäten, Lehrer, Referendare, Schüler).“

- Produkt: wiso, Konsortial-Nutzungsvertrag
„NUTZUNGSRECHTE
[...] das örtlich, auf die Räume der Hochschule, begrenzte (Campuslizenz), nicht ausschließliche Recht ein, die Datenbanken zu wissenschaftlichen Forschungs- und Ausbildungszwecken für ihre Hochschulangehörigen bereitzuhalten [...]
GESCHÄFTSBEDINGUNGEN
[...] dieses Angebot im Rahmen seiner Organisation einem hierfür berechtigten Nutzerkreis zur Verfügung zu stellen.“

- Produkt: SpringerLink Plattform, Lizenzvertrag
„BERECHTIGTE NUTZER
[...] sind Wissenschaftler, Angestellte und Mitarbeiter der Lizenznehmer sowie Privatpersonen, die die Bibliotheken besuchen und diese zu persönlichen wissenschaftlichen Zwecken nutzen. Nutzungsberechtigt sind auch Personen an Zweig- bzw. Außenstellen, nicht aber Organisationen, Firmen oder Einrichtungen, es sei denn sie sind in Anlage B genannt. Die Präsenznutzung durch Besucher bzw. Nutzer einer Bibliothek erfüllt nicht den Tatbestand der "öffentlichen Wiedergabe" gem. § 4 AOB.“ (AOB = Allgemeine Online-Vertragsbedingungen).

2.4.3 Fazit Lizenzverträge

Aus der Analyse der vorliegenden Lizenzverträge ergibt sich:

- Der Zugang zu den elektronischen Ressourcen erfolgt derzeit zu fast 100% IP-basiert, d.h. auf der Grundlage der Angabe einzelner oder mehrerer Netz-adressen, aber auch unter möglicher Angabe der Adressen von Proxy-Servern. Einzelne Verträge enthalten bereits eine Option zur Nutzung von Shibboleth, einem System in einer verteilten Authentifizierungs- und Autorisierungs-Infrastruktur (AAI).
- In der Regel handelt es sich um Verträge mit speziellen Konditionen für Forschung, Studium und Lehre.
- Die Gruppe der Nutzungsberechtigten unterscheidet sich je nach Produkt oder Verlag, manchmal auch für verschiedene Produkte eines Verlages.
- Die Verträge sind hinsichtlich der erlaubten Benutzergruppen heterogen. Verträgen zur ausschließlichen Nutzung durch Universitätsangehörige stehen Verträge gegenüber, die durchaus externen Benutzern und „Walk-in-Usern“ die Nutzung in den Räumen der Bibliothek gestatten.
- Einheitlich festgeschrieben ist in der Regel in allen Verträgen der wissenschaftliche und nichtkommerzielle Verwendungszweck der lizenzierten elektronischen Ressourcen.

Im Ergebnis der Analyse der Lizenzverträge ergibt sich die Aussage, dass aufgrund der festgelegten heterogenen Benutzergruppen zur Einhaltung der vertraglich vereinbarten Nutzung ein System benötigt wird, welches:

- nur Benutzern Zugang zu den elektronischen Ressourcen gestattet, die dem vertraglich vereinbarten wissenschaftlichen und nichtkommerziellen Zweck verpflichtet sind und
- den Zugang rollenbasiert entsprechend dem vertraglich vereinbarten Benutzerkreis gestaltet.

Beide Anforderungen lassen sich in einer Bibliothek, die externen Benutzern den Zugang zu ihren lizenzierten elektronischen Ressourcen gestattet, nur über eine Authentifizierung an den Endgeräten sicherstellen.

2.5 **Benutzungsordnungen**

Wie in Kap. 1.5 ausgeführt, beschränken sich die Betrachtungen auf wissenschaftliche Bibliotheken, die Teil von juristischen Personen des öffentlichen Rechts sind, wie z.B. Staats-, Landes- oder Universitätsbibliotheken. Im Zusammenhang mit der Betrachtung von Benutzungsordnungen der Bibliotheken müssen auch die Benutzungsordnungen der Rechenzentren berücksichtigt werden¹⁰⁴, die eine sinnvolle und notwendige Ergänzung darstellen. In Benutzungsordnungen legen Bibliotheken und Rechenzentren die Grundsätze ihrer Verwaltungstätigkeit in Bezug auf die Erbringung von Dienstleistungen für ihre Benutzer fest. Benutzungsordnungen sind Rechtsverordnungen, die von den tragenden Einrichtungen aufgrund der ihnen zugestanden Selbstverwaltung im Rahmen der Gesetze erlassen werden¹⁰⁵. Benutzungsordnungen können als Rechtsnorm in Form einer Satzung oder Verwaltungsnorm in Form einer Verfügung erlassen werden. Die Benutzungsordnung einer Bibliothek kann die Benutzungsordnung eines Rechenzentrums mit einschließen, welches durch Betrieb und Bereitstellung des Datennetzes mit Anschluss an das Wissenschaftsnetz mit dem DFN-Verein als Access-Provider wesentliche Basisdienste für die Bibliothek erbringt.

Das Benutzungsverhältnis kann als ein öffentlich-rechtliches oder als ein privatrechtliches gestaltet werden. Auch eine Option, die für Sondernutzungsfälle eine privatrechtliche Regelung zulässt, ist möglich. Unterschiede zwischen beiden bestehen z.B. bezüglich der Verfahrensweise bei der Durchsetzung von Rechtsansprüchen gegenüber Benutzern.

In Bezug auf das Thema der Arbeit interessieren die in der Benutzungsordnung zugelassenen Benutzer und der zugelassene Zweck der Nutzung. Unter welchen Bedingungen lassen wissenschaftliche Bibliotheken (und Rechenzentren) in ihren Benutzungsordnungen externe Benutzer zur Nutzung elektronischer Ressourcen zu?

2.5.1 **Benutzungsordnung von Bibliothek und Rechenzentrum**

Als Beispiel seien hier die maßgeblichen Benutzungsordnungen der Universität Rostock aufgeführt, die Benutzungsordnung für die Universitätsbibliothek¹⁰⁶ sowie

104 Vgl. Informationen des DFN-Vereins zum Thema Benutzungsverhältnis.

Internet: <http://www.dfn.de/de/beratung/rechtimdfn/rgwb/rechtsguide/rg-kapitel1/> [05.05.08]

105 Auf Grundlage des Hochschulrahmengesetzes (HRG) [HRG], § 58 Rechtsform und Selbstverwaltungsrecht, bzw. der Landeshochschulgesetze, z.B. des Gesetzes über die Hochschulen des Landes Mecklenburg-Vorpommern (LHG M-V) [LHG MV], § 81 Senat, sind die Hochschulen ermächtigt, selbständig Rechtsnormen in Form von Satzungen zur Regelung ihrer Verwaltungstätigkeit zu erlassen.

106 [UNIRO2008]

die Betriebsregelung und Benutzungsordnung für das Datenkommunikationsnetz der Universität Rostock RUN¹⁰⁷.

Die Benutzungsordnung für die Universitätsbibliothek¹⁰⁸ trifft bezüglich der Aufgaben der Bibliothek und der Zulassung zur Benutzung folgende Festlegungen:

§ 2 Abs. 1 (Aufgaben der Bibliothek):

„(1) Die Universitätsbibliothek [...] dient als öffentliche wissenschaftliche Bibliothek der universitären Literatur- und Informationsversorgung. Sie erfüllt darüber hinaus Aufgaben in der wissenschaftlichen Ausbildung, der beruflichen Arbeit und der Fortbildung von regionaler und überregionaler Bedeutung.“

§ 4 Abs. 3 (Zulassung zur Benutzung):

„(3) Zur Benutzung der Universitätsbibliothek im Rahmen der in § 2 genannten Aufgabenstellung können alle nachfolgenden natürlichen Personen zugelassen werden:

- a. Mitglieder und Angehörige der Hochschulen des Landes Mecklenburg-Vorpommern,*
- b. alle weiteren Personen, die im Land Mecklenburg-Vorpommern ihren amtlich gemeldeten Wohnsitz haben und das 16. Lebensjahr vollendet haben,*
- c. andere Personen nach Einzelentscheidung durch die Bibliotheksleitung.“*

Die Universitätsbibliothek beschränkt ihre Aufgabe nicht auf die Versorgung der Hochschulangehörigen, sondern nimmt darüber hinaus noch Aufgaben von regionaler und überregionaler Bedeutung wahr. Externe Benutzer sind zur Benutzung zugelassen, der Zweck der Nutzung ist auf die wissenschaftliche Informationsversorgung bzw. Unterstützung der beruflichen Arbeit und Fortbildung festgelegt.

§ 17 Abs. 1 und Abs. 2 (Nutzung von EDV-Arbeitsplätzen)¹⁰⁹:

„(1) [...] Die Benutzer oder Benutzerinnen erkennen die Betriebsregelung und Benutzungsordnung für das Datenkommunikationsnetz (RUN) sowie die WWW-Ordnung der Universität Rostock an.

(2) Die Nutzung steht unter dem Vorbehalt des dienstlichen, wissenschaftlichen bzw. studienbezogenen Zwecks. Sie kann im Bedarfsfall reguliert werden. Jede bibliotheksfremde oder kommerzielle Nutzung der EDV-Einrichtungen, einschließlich der Internet-Zugänge, ist unzulässig. Bibliotheksfremde Nutzung ist jegliche Nutzung, die Arbeit und Auftrag der Universitätsbibliothek behindert, gegen gesetzliche Vorschriften oder die guten Sitten verstößt.“

107 [\[UNIRO1995\]](#)

108 [\[UNIRO2008\]](#)

109 Ebd.

Während § 17 Abs. 2 den Zweck der Nutzung auf die EDV-Arbeitsplätze überträgt und auf eine mögliche Regulierung der Nutzung hinweist, wird der Benutzer in § 17 Abs. 1 zur Betriebsregelung und Benutzungsordnung für das Datenkommunikationsnetz (RUN)¹¹⁰ und zur WWW-Ordnung der Universität Rostock¹¹¹ verpflichtet.

Die WWW-Ordnung enthält Regelungen zum Anbieten eigener Inhalte im WWW durch die Universität, eine Funktionalität, die nur Hochschulangehörigen vorbehalten ist. Die Präambel zur Betriebsregelung und Benutzungsordnung für das Datenkommunikationsnetz (RUN) legt fest:

„Das Rostocker Universitäts Netz (RUN) [...] ist für Forschung, Lehre und Studium sowie zur Erledigung von Verwaltungsaufgaben an der Universität Rostock vorgesehen.“¹¹²

und enthält damit keine explizite Zulassung externer Benutzer.

Die Benutzungsordnung der Bibliothek regelt ferner unter § 19 Abs. 2 (Zugang zu elektronischen Ressourcen):

“(2) Der Datenbankzugang richtet sich nach den Bedingungen der Lizenzgeber. Freinutzbare Datenbanken werden entsprechend markiert, eingeschränkt nutzbare elektronische Informationsquellen (z.B. nur für Universitätsangehörige oder Nutzung nur in den Räumen der Universitätsbibliothek oder über dedizierte IP-Adressen der Universität Rostock) werden besonders gekennzeichnet. Die Zugangsberechtigung wird durch ein Authentifizierungs/Autorisierungsprogramm überprüft.“¹¹³

Auf mögliche Beschränkungen, die sich aus den für die Nutzung der elektronischen Ressourcen abgeschlossenen Lizenzverträgen ergeben, und die in diesem Zusammenhang notwendige Authentifizierung und Autorisierung wird hingewiesen.

2.5.2 Musterbenutzungsordnung DFN-Verein

Die Konsequenz aus den aufgeführten Benutzungsordnungen wäre, dass externe Benutzer nach der Benutzungsordnung der Bibliothek wohl für die Nutzung der Bibliothek, nach der Benutzungsordnung des Rechenzentrums aber nicht für die Nutzung des dafür erforderlichen Datennetzes zugelassen sind. Auch ohne explizite Nennung der externen Benutzer wird aber im Sinne der Benutzungsordnung der Bibliothek von einer Zulassung auch für das Datennetz der Universität und damit letztlich der Zulassung für den Zugang zum Wissenschaftsnetz ausgegangen.

110 [\[UNIRO1995\]](#)

111 [\[UNIRO1999\]](#)

112 Und ebenso [\[UNIRO1995\]](#), Nr. 5 (a): „Das RUN darf nur für Forschung, Lehre und Studium und zur Erledigung von Verwaltungsaufgaben an der Universität Rostock genutzt werden.“

113 Ebd.

Die Benutzungsordnung des Rechenzentrums wurde auf Basis der DFN-Musterbenutzungsordnung¹¹⁴ erstellt. Diese soll hier betrachtet werden, weil sich daraus Schlüsse über die Rechtsauffassung des DFN-Vereins als Access-Provider bezüglich der Zulassung externer Benutzer ziehen lassen.

Für Bibliotheken stellt sich daher auch die Frage, ob sie bestimmte Aspekte der Musterbenutzungsordnung des DFN-Vereins in ihre Benutzungsordnung übernehmen sollten. Die Musterbenutzungsordnung des DFN-Vereins ist primär auf „die möglichst störungsfreie, ungehinderte und sichere Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur des Hochschulrechenzentrums der Hochschule“¹¹⁵ gerichtet, eine wichtige Voraussetzung für den Betrieb der Bibliothek. Eine genauere Betrachtung ergibt, dass inhaltliche Überschneidungen bei fast allen Paragraphen (§§ 4 ff.) der Musterbenutzungsordnung möglich sind. Der beste Weg ist sicher der, dass Bibliothek und Rechenzentrum sich hier abstimmen und alle Aspekte, die die Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur betreffen, weitestgehend in die Ordnung des Rechenzentrums aufnehmen, um dann aus der Benutzungsordnung der Bibliothek auf diese zu verweisen. Eine andere Möglichkeit ist die Festlegung von Benutzungsregeln für Internet-Arbeitsplätze in einer Anlage zur Benutzungsordnung, die dann durch die Bibliothek ohne Änderung der Satzung an ggf. geänderte technische Bedingungen angepasst werden kann.¹¹⁶

Wie sieht der DFN-Verein die Zulassung externer Benutzer? In § 4 Abs. 1 (Nutzungsberechtigung und Zulassung zur Nutzung) werden als mögliche Benutzer der Dienste des Hochschulrechenzentrums aufgeführt:

1. Mitglieder, Angehörige und Einrichtungen einschließlich der Verwaltung der XY Universität sowie der Fachhochschule XY;
2. Beauftragte der Hochschule zur Erfüllung ihrer Dienstaufgaben;
3. Mitglieder und Angehörige anderer Hochschulen des Landes XX oder staatlichen Hochschulen außerhalb des Landes XX aufgrund besonderer Vereinbarungen;
4. sonstige staatliche Forschungs- und Bildungseinrichtungen und Behörden des Landes XX aufgrund besonderer Vereinbarungen;
5. Studentenwerke im Land XX;¹¹⁷

114 [\[DFN2006\]](#)

115 Ebd.

116 Benutzungsordnungen, die ergänzende Regelungen in einer Anlage zur Benutzungsordnung getroffen haben sind z.B. die Universitätsbibliothek Greifswald oder die TIB Hannover, Bibliotheken die auf eine Benutzungsordnung des Rechenzentrums verweisen sind z.B. die Universitätsbibliothek Rostock oder die Johann Wolfgang Goethe-Universität Frankfurt.

117 Ebd.

Es folgt als Kommentar:

Aufgrund der in § 110 TKG geregelten Verpflichtung zur Ermöglichung von Überwachungsmaßnahmen durch Betreiber von Telekommunikationsanlagen, mit denen Telekommunikationsdienste für die Öffentlichkeit erbracht werden, sollte der Nutzerkreis nach Möglichkeit nicht auf Personen außerhalb der Hochschulen (Privatpersonen, private Unternehmen ohne direkten Bezug zu einem Forschungsvorhaben) ausgeweitet werden. Wenn grundsätzlich jede Person unabhängig von der Hochschulzugehörigkeit zur Nutzung zugelassen werden kann, besteht die Gefahr einer Verpflichtung nach § 110 TKG i.V.m. der TKÜV.

~~*Sonstige juristische oder natürliche Personen, sofern hierdurch die Belange der unter 1. bis 5. genannten Nutzer nicht beeinträchtigt werden.*~~¹¹⁸

Und § 4 Abs. 2 lautet:

*„(2) Die Zulassung erfolgt ausschließlich zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, zu Zwecken der Bibliothek und der universitären Verwaltung, zur Aus- und Weiterbildung sowie zur Erfüllung sonstiger Aufgaben der XY Hochschule. Eine hiervon abweichende Nutzung kann zugelassen werden, wenn sie geringfügig ist und die Zweckbestimmung des Hochschulrechenzentrums sowie die Belange der anderen Nutzer nicht beeinträchtigt werden.“*¹¹⁹

Danach entspricht es durchaus der Rechtsauffassung des DFN-Vereins, auch in geringem Umfang externe Benutzer, solange nicht die Belange der primären Benutzerklientel beeinträchtigt werden, zur Nutzung zuzulassen. Der Kommentar zu einer möglichen Verpflichtung nach § 110 TKG und die folgende Streichung der „sonstige[n] juristische[n] oder natürliche[n] Personen“ zeigen dies recht deutlich. In § 4 Abs. 2 wird ein „Zweck Bibliothek“ aufgeführt, der für die Bibliothek primär dem Betrieb des Lokalen Bibliothekssystems, d.h. Erwerbung, Ausleihe und Katalogisierung, der Dokumentenlieferung und Fernleihe, aber auch der Bereitstellung des Online-Katalogs und dem Zugang zu elektronischer Ressourcen entspricht.

118 Ebd.

119 Ebd.

2.5.3 Fazit Benutzungsordnungen

Wissenschaftliche Bibliotheken erlassen ihre Benutzungsordnungen in der Regel als Satzungen. Diese sind damit verbindliche Rechtsvorschriften und gelten für alle Benutzer der Bibliothek. Viele wissenschaftliche Bibliotheken, die sich in Trägerschaft der öffentlichen Hand befinden, beschränken ihren Auftrag nicht auf eine geschlossene Benutzergruppe, z.B. der Angehörigen einer Hochschule, sondern haben darüber hinaus einen Auftrag zur regionalen und überregionalen wissenschaftlichen Informationsversorgung. So werden externe Benutzer nicht von der Nutzung der Internet-Arbeitsplätze ausgeschlossen, solange die Versorgung der primären Benutzerklientel dadurch nicht beeinträchtigt wird. In Benutzungsordnungen oder als Anlage aufgeführte ergänzende Ausführungsbestimmungen können aber Klauseln enthalten, die den Zugang für externe Benutzer einzuschränken. Denkbare Optionen für Einschränkungen wären z.B. die Anzahl der Internet-Arbeitsplätze, die zugelassene Arbeitszeit oder die angebotenen elektronischen Ressourcen. Abstimmung und Verbindung der Benutzungsordnungen von Bibliothek und Rechenzentrum sind sinnvoll, um die Regelungen zur Nutzung des Datennetzes auch auf alle Bibliotheksbenutzer zu übertragen. Der Zweck der Nutzung ist, unabhängig von der Art der Medien, in allen Benutzungsordnungen wissenschaftlicher Bibliotheken auf eine wissenschaftliche Nutzung ausgerichtet.

2.6 Rechtliche Rahmenbedingungen – Fazit und Konsequenzen

Als Ergebnis der Betrachtung der rechtlichen Rahmenbedingungen (Telekommunikationsüberwachung, Jugendmedienschutz, Lizenzverträge, Benutzungsordnungen) erweist sich die Einführung einer Erweiterung des Lokalen Bibliothekssystems (LBS) um einen rollenbasierten Zugang zu elektronischen Ressourcen als notwendig, vor allem wenn externe Benutzer für die Nutzung der Internet-Arbeitsplätze in der Bibliothek zugelassen werden. Nur so ist es der Bibliothek möglich, die rechtlichen Rahmenbedingungen zu beachten und den Zugang zu den elektronischen Ressourcen im Interesse der Erfüllung der Aufgaben der Bibliothek zu gestalten.

Aus den genannten Gründen: Bestimmung der Anzahl der externen Benutzer, Verpflichtung zur Benutzungsordnung, Bereitstellen rollenbasierter Dienstleistungen und Ressourcen sowie der Sicherheit des Betriebs der Informationstechnik sollten generell nur registrierte Benutzer zugelassen werden, die sich an den Internet-Arbeitsplätzen der Bibliothek authentifizieren müssen.

Einer Verpflichtung nach § 110 TKG (und evt. § 113a TKG) kann sich die Bibliothek entziehen, wenn die Zahl der externen Benutzer (sonstigen Nutzungsberechtigten) 10.000 nicht übersteigt (§ 3 Abs. 2 Nr. 5 TKÜV). Ist die Zahl der externen Benutzer größer als 10.000, so ist die Bildung bzw. der Erhalt einer geschlossenen Benutzergruppe durch schriftliche Verpflichtung der Benutzer zur wissenschaftlichen Nutzung zu prüfen. Kann auch dadurch die Anzahl der externen Benutzer nicht ausreichend verringert werden, sollte sich die Bibliothek auf das Gutachten der DBV-Rechtskommission [[DBV2006](#)] berufen, welches generell eine Verpflichtung nach § 110 TKG bei Bereitstellung fest installierter Internet-Arbeitsplätze verneint.

Der Schutz von Kindern und Jugendlichen, so diese zur Nutzung von Internet-Arbeitsplätzen in der Bibliothek zugelassen sind, macht technische und organisatorische Maßnahmen erforderlich, unabhängig davon, ob diese etwa zur geschlossenen Gruppe der Hochschulangehörigen gehören oder ob eine Einwilligung eines Erziehungsberechtigten vorliegt. Die sicherste Option ist hier die Umsetzung einer Positivliste (Whitelist), die nur ausgewählte elektronische Ressourcen zugänglich macht.

Von wissenschaftlichen Bibliotheken abgeschlossene Lizenzverträge sind in der Regel immer an eine wissenschaftliche und nichtkommerzielle Nutzung der lizenzierten elektronischen Ressourcen gebunden. Bezüglich der zugelassenen Benutzergruppen sind sie heterogen gestaltet und schließen in nicht wenigen Fällen die Nutzung durch externe Benutzer aus. Hier ist der Einsatz eines rollenbasierten Zugangssystems unbedingt erforderlich.

Viele wissenschaftliche Bibliotheken, die sich in Trägerschaft der öffentlichen Hand befinden, haben auch einen Auftrag zur regionalen und überregionalen wissenschaftlichen Informationsversorgung. Sie lassen externe Benutzer für die Nutzung von Internet-Arbeitsplätzen zu, solange die Versorgung der primären Benutzerklientel dadurch nicht beeinträchtigt wird. Dieses entspricht auch der Rechtsauffassung des DFN-Vereins als Access-Provider der meisten deutschen Hochschulen und Forschungseinrichtungen.

3 Umsetzung am Beispiel der UB Rostock

Die Betrachtungen aus Kap. 2 zu den rechtlichen Rahmenbedingungen der Nutzung elektronischer Ressourcen insbesondere durch externe Benutzer haben die Universitätsbibliothek Rostock veranlasst, das im Einsatz befindliche Lokale Bibliothekssystem LBS-PICA um eine Komponente zum rollenbasierten Zugang zu elektronischen Ressourcen zu erweitern.

3.1 Organisatorische Grundlagen

Als eine von über 400 Bibliotheken im Gemeinsamen Bibliotheksverbund (GBV) nutzt auch die UB Rostock das Lokale Bibliothekssystem LBS-PICA von OCLC, aktuell in der Version LBS3-Port¹²⁰. Die Daten der Benutzer werden für die Ortsleihe ausschließlich lokal im LBS gespeichert und dort mit den Titeldaten für Ausleihvorgänge verbunden. Die Titeldaten können dabei lokaler Herkunft sein, wie etwa im Fall der nehmenden Fernleihe, oder per Online-Update-Prozess aus dem zentralen Katalogisierungssystem (CBS) in das LBS überspielt worden sein.

Die Erstaufnahme oder Freischaltung¹²¹ eines Benutzerkontos erfolgt an einer Theke in der UB. Die Benutzer erhalten dabei einen Bibliotheksausweis mit einer 11-stelligen Benutzernummer. Diese Benutzernummer ermöglicht ihnen die Authentifizierung zur Nutzung der personalisierten Funktionen des Ausleihmoduls über den Online-Katalog, das automatisch zugewiesene Erstkennwort kann jederzeit geändert werden. Die Bearbeitung der Benutzerkonten an der Theke erfolgt mit der WINIBW¹²² im Ausleihmodul des LBS und die Daten werden in den entsprechenden Tabellen der zum LBS-PICA gehörigen Sybase-Datenbank gespeichert. Dabei werden die Benutzer in vordefinierten Benutzergruppen zusammengefasst, so dass eine Trennung von Hochschulangehörigen und externen Benutzern möglich ist.

120 LBS-PICA wird nach der Übernahme durch OCLC unter dem Namen „LBS“ weiter entwickelt. Internet: <http://www.oclc.org/de/de/services/management/> [15.05.08]

121 Freischaltung nach Einspielung der Daten aus dem Hochschul-Informationssystem (HIS).

122 WINIBW (Windows Intelligent Bibliographic Workstation) ist eine Client-Komponente des LBS, mit der ausschließlich die Mitarbeiter der Bibliothek zu Zwecken der Erwerbung, Ausleihe und Katalogisierung arbeiten.

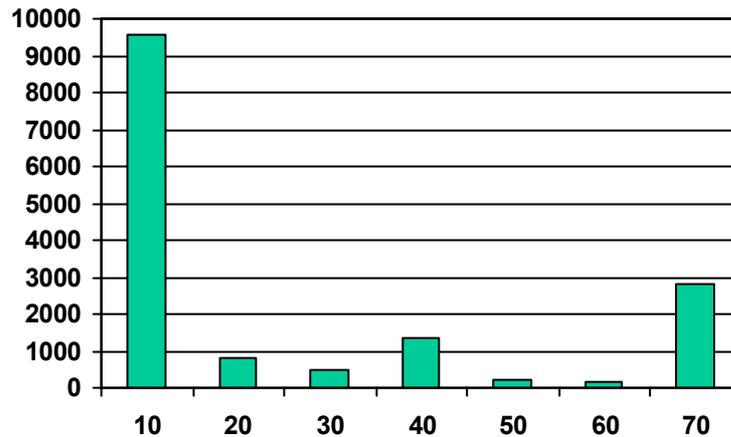


Abb. 1: Anzahl der Benutzer je Benutzergruppe, UB Rostock, Stand: 21.05.2008.

LBS-Benutzergruppen:

- | | |
|----|--|
| 10 | Student der Universität Rostock |
| 20 | Student einer Hochschule in M/V |
| 30 | Professor der Universität Rostock |
| 40 | Mitarbeiter der Universität Rostock |
| 50 | Mitarbeiter kooperierender Einrichtungen (An-Institute, HMT ...) |
| 60 | Mitarbeiter Bibliothek |
| 70 | Stadtbenutzer, Privatperson M/V (externe Benutzer) |

Es ergibt sich, dass die Anzahl der externen Benutzer (Benutzergruppe 70) mit 2.800 die Zahl der sonstigen Nutzungsberechtigten aus § 3 Abs. 2 Nr. 5 TKÜV von 10.000 nicht erreicht¹²³, aber im Verhältnis zur Gesamtanzahl der Benutzer nicht als sehr gering gesehen werden kann. Studenten anderer Hochschulen des Landes sowie die Mitarbeiter kooperierender Einrichtungen werden als wissenschaftliche, nichtkommerzielle Benutzer, im Folgenden kurz **wnk-Benutzer**, der geschlossenen Benutzergruppe der Hochschulangehörigen zugerechnet.

Die Notwendigkeit zur Erweiterung des LBS um einen rollenbasierten Zugang zu elektronischen Ressourcen ist in Kap. 2 ausführlich und in Kap. 2.5 zusammengefasst dargelegt worden, letztlich geht es um die Beachtung der rechtlichen Rahmenbedingungen sowie um die Erfüllung der Aufgabe der Bibliothek.

¹²³ Die Anhebung der Anzahl der sonstigen Nutzungsberechtigten von 1.000 auf 10.000 in § 3 Abs. 2 Nr. 5 TKÜV trat am 01.01.2008 in Kraft (BGBl I 2007, 3198).

Drei Aufgabenschwerpunkte können zusammenfassend wie folgt formuliert werden:

- a) Sicherung des Zugangs zu elektronischen Ressourcen für die primäre Benutzerklientel der Universitätsbibliothek entsprechend den geltenden Benutzungsordnungen durch Einschränkungen für externe Benutzer (Anzahl der Arbeitsplätze, Einschränkung der Ressourcen),
- b) Sicherung des Zugangs zum Online-Katalog durch Bereitstellung von Arbeitsplätzen mit ausgewählten Ressourcen (Katalog-Arbeitsplätze),
- c) Umsetzung der bestehenden rechtlichen Regelungen für den Zugriff auf elektronische Ressourcen durch Sperrung ausgewählter Ressourcen für Benutzer, die keine Hochschulangehörigen sind (rollenbasierter Zugang).

Für externe Benutzer besteht die Möglichkeit, durch einen Antrag auf wissenschaftliche Nutzung des Datennetzes¹²⁴ einer neuen Benutzergruppe 71 (externe wnk-Benutzer) zugeordnet zu werden und damit Zugang zu allen elektronischen Ressourcen zu erhalten, sofern diesem nicht Jugendschutz oder Lizenzverträge entgegenstehen. Ansonsten unterliegt die Benutzergruppe 71 demselben Ausleihreglement wie die Benutzergruppe 70. Die Mitgliedschaft in der Benutzergruppe 71 ist auf ein Jahr befristet und kann auf Antrag erneuert werden. Erfolgt keine Verlängerung, so wird der Benutzer nach Ablauf des Jahres automatisch der Benutzergruppe 70 zugeordnet.

Die Benutzergruppen werden in drei Rollen zusammengefasst:

Rolle A: Benutzergruppen, die an allen Rechnern der UB ohne Einschränkungen arbeiten können:

10	Student der Universität Rostock
30	Professor der Universität Rostock
40	Mitarbeiter der Universität Rostock
60	Mitarbeiter Bibliothek

Rolle B: Benutzergruppen mit externen wnk-Benutzern, die an allen Rechnern arbeiten können, deren Zugang zu elektronischen Ressourcen aber durch eine Negativliste (Blacklist), resultierend aus den Vorgaben der Lizenzverträge, eingeschränkt ist:

20	Student einer Hochschule in M/V
50	Mitarbeiter kooperierender Einrichtungen (An-Institute, HMT ...)
71	Externer wissenschaftlich, nichtkommerzieller Benutzer

¹²⁴ Anlage 2: Antrag auf wissenschaftliche Nutzung des Datennetzes der Universität Rostock.

Rolle C: Benutzergruppen mit externen und U18-Benutzern, die nur an ausgewählten Arbeitsplätzen arbeiten können und deren Zugang zu elektronischen Ressourcen durch eine Negativliste (Blacklist) und eine Positivliste (Whitelist) eingeschränkt ist:

- 70 Stadtbenutzer, Privatperson M/V (externe Benutzer)
- 118 virtuelle Gruppe der Benutzer, die das 18. Lebensjahr noch nicht vollendet haben (U18-Benutzer)

Zudem werden die Arbeitsplätze in drei Typen unterteilt:

- AP1:** Arbeitsplatz für Hochschulangehörige und wnk-Benutzer (Rollen A, B),
- AP2:** Arbeitsplatz für alle Benutzer (Rollen A,B,C),
- AP3:** Katalog-Arbeitsplatz für alle Benutzer (Rollen A,B,C) mit Einschränkung des Zugangs auf ausgewählte elektronische Ressourcen.

Die verschiedenen Arbeitsplatztypen werden am Bildschirmrand gekennzeichnet, z.B. durch die Aufschrift „Katalog Arbeitsplatz“, und außerdem über die Website der Universitätsbibliothek nach Standort ausgewiesen. Letzteres erfolgt über eine Abfrage der Datenbank des in der UB eingesetzten Managementsystems Altiris¹²⁵ und ermöglicht die Anzeige von Standort, Arbeitsplatztyp und Status (in Benutzung, eingeschaltet, ausgeschaltet) für jeden Rechner im öffentlichen Bereich der Bibliothek¹²⁶.

Authentifizierung: Der Zugang zu den fest installierten Internet-Arbeitsplätzen in der Bibliothek ist generell nur über eine Authentifizierung des Benutzers möglich. „Walk-in-User“ sind nicht zur Benutzung zugelassen.

WLAN-Nutzung: Allen Benutzern der Bibliothek steht ein WLAN-Zugang zu den öffentlich zugänglichen Seiten der Universität Rostock¹²⁷ zur Verfügung. Eine weitergehende Nutzung, so auch des Online-Katalogs der UB, ist nur mit einer Authentifizierung für Hochschulangehörige möglich.

VPN/Terminalserver: Ein Zugang zum Campusnetz via VPN oder Terminalserver ist nur mit einer Authentifizierung für Hochschulangehörige möglich.

125 Altiris ist eine Tochter der Symantec Corporation. Internet: <http://www.altiris.com/> [05.05.08]

126 Anzeige z.B. über die Seite Öffnungszeiten der einzelnen Bereichs- und Fachbibliotheken unter dem Link Rechnernutzung. Internet: http://www.uni-rostock.de/ub/xLibraries/hours_xde.shtml [05.05.08]

127 Internet: <http://www.uni-rostock.de/> [05.05.08]

3.2 Grundprinzipien der Implementierung

Bei begrenzten personellen und finanziellen Ressourcen soll mit minimalem Aufwand und geringen Kosten eine möglichst einfache Lösung realisiert werden. Der Einsatz neuer Produkte oder Lösungen, deren Anschaffung und Betrieb große personelle und finanzielle Kapazitäten bindet, ist in absehbarer Zeit nicht möglich.

Folgende Anforderungen an die Implementierung werden gestellt:

- Ankopplung an die Benutzerverwaltung des LBS (Verwaltung von Benutzergruppen; Anlegen, Aktualisieren und Löschen von Benutzerkonten),
- praktisch wartungsfreier (fehlerfreier und vollautomatischer) Betrieb,
- für alle Belange einfach parametrisierbar,
- Nutzung von vorhandenem Verzeichnisdienst (Active Directory (AD)¹²⁸) und Schnittstellen (SQL, LDAP) und damit mögliche Portierung auf andere LBS mit SQL-Datenbanken.

Neben dem bestehenden Verzeichnisdienst des Rechenzentrums, der allen Hochschulangehörigen den Zugang zum Wissenschaftsnetz gestattet, wurde auf Grundlage der bestehenden Windows-Domäne der UB (W2K3) ein separater Verzeichnisdienst aufgebaut, der eine Abbildung (Snapshot) der LBS-Benutzerverwaltung ist und auch externen Benutzern die Authentifizierung an den Rechnern der UB gestattet. Für die Hochschulangehörigen ist damit ein redundantes System vorhanden, welches auch die Arbeit an den Rechnern der UB mit Zugriff auf die elektronischen Ressourcen ermöglicht, wenn der Verzeichnisdienst des Rechenzentrums nicht verfügbar ist.

3.3 Technische Realisierung

3.3.1 Voraussetzungen

Rechenzentrum und UB betreiben zwei eigenständige Windows Forest-Root-Domänen, die über eine externe Vertrauensstellung verbunden sind. Die Domäne der UB (ub.uni-rostock.de) vertraut der Domäne des Rechenzentrums (uni-rostock.de) und ermöglicht somit Hochschulangehörigen an Rechnern der UB die Authentifizierung für beide Domänen. Der Abgleich der Benutzerkonten zwischen der relationalen LBS-Datenbank als Primärquelle und der Verzeichnisdatenbank der UB-

128 Active Directory (AD, auch Active Directory Service - ADS) ist der in Anlehnung an X.500 entwickelte und auf LDAP basierende Verzeichnisdienst von Microsoft. AD verwendet Domain Name System (DNS) für die Adressenspeicherung und Kerberos für die Authentifizierung. Im AD werden als administrative Einheiten „Organisation Units“ (OUs) erstellt, die Objekte nach vordefinierten Schemata wie z.B. Benutzer und Rechner mit ihren relevanten Daten (Attributen) enthalten. Ab Windows Server 2008 werden die AD-Dienste unter Active Directory Domain Services (ADDS) zusammengefasst. Siehe auch [[W2K3AD2006](#)].

Domäne¹²⁹ gestattet allen Bibliotheksbenutzern die Authentifizierung an den fest installierten Rechnern der UB-Domäne mit lokalen, nicht permanenten Profilen. Außerdem ist eine Unterscheidung der Benutzer nach LBS-Benutzergruppen und damit nach den vorgegebenen Rollen A, B, C im Active Directory (AD) über die Zugehörigkeit zu einer Organisationseinheit (OU) und eine Gruppenzugehörigkeit möglich und gestattet eine Auswertung über Gruppenrichtlinien und das Anmelde-skript. Die Rechner der UB werden mit dem Betriebssystem Windows-XP/SP3 betrieben. Hochschulangehörige, die sich mit Ihrem Rechenzentrums-Account authentifizieren, haben über die Umgebungsvariable RZNTProfile Zugriff auf Ihre Nutzerprofile (RZNTProfile=\\uni-rostock.de\dfs\Profiles\NT) und die durch das Rechenzentrum bereitgestellten Ressourcen. Die Authentifizierung mit einem LBS-Account stellt hingegen lediglich den Zugang zu den elektronischen Ressourcen sowie ggf. zu weiteren von der UB bereitgestellten Services, wie etwa einem Druckservice für externe Benutzer, her.

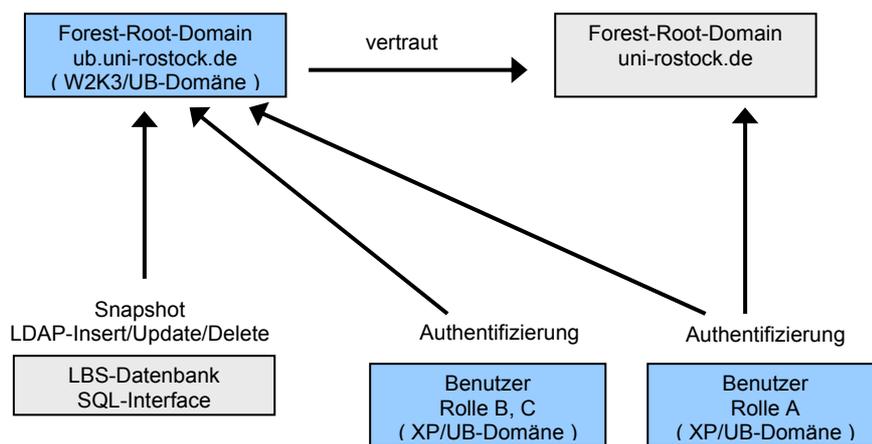


Abb. 2: Die Vertrauensstellung zwischen UB- und Rechenzentrumsdomäne und der Abgleich der Benutzerkonten zwischen LBS und AD der UB-Domäne ermöglichen die Authentifizierung der Benutzer entsprechend der zugewiesenen Rolle.

3.3.2 Abbildung der LBS-Benutzerverwaltung auf das Active Directory

In der LBS-Datenbank wird eine Tabelle xprivate_adstore erstellt, aus der alle Aktionen bzgl. der notwendigen Operationen im AD generiert werden können. Jede Aktion im LBS (Anlegen, Aktualisieren oder Löschen eines Benutzerkontos) wird mit einer Aktion im AD verknüpft, die mit einem SQL-Skript auf dem LBS-Host generiert und anschließend durch einen Active Directory-Client (kurz AD-Client) mit

¹²⁹ Repliziert werden nur wenige ausgewählte Attribute der Benutzerkonten im LBS. Bestimmte Attributwerte, wie etwa Personalsperre oder Ablauf der Mitgliedschaft, führen zum Löschen des Datensatzes im Active Directory.

entsprechenden Zugriffsrechten auf das AD ausgeführt wird. Der Abgleich zwischen LBS-Datenbank und AD erfolgt einmal täglich¹³⁰, so dass neu angelegte Benutzer sich erst am nächsten Tag an einem Rechner in der UB anmelden können.

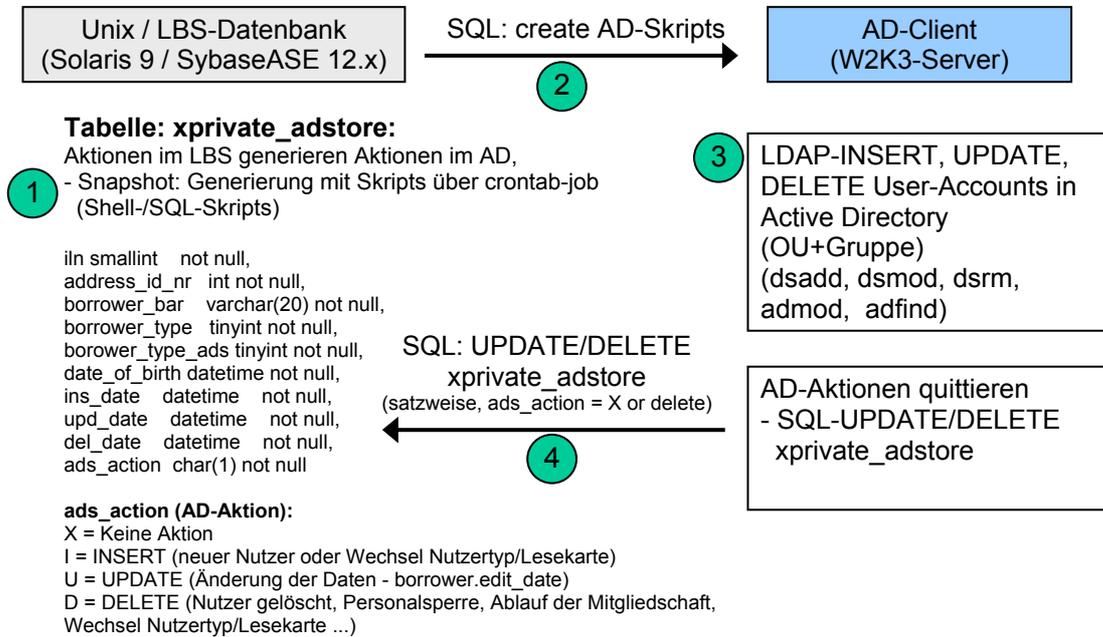


Abb. 3: Abgleich zwischen LBS-Datenbank und Active Directory.

Schritt 1: Über einen crontab-Job auf dem LBS-Host wird via Shell- und SQL-Skript¹³¹ vom aktuellen Stand der LBS-Benutzerkonten ein Snapshot mit codierten Aktionen für das AD in der Tabelle xprivate_adstore gespeichert. Diese Prozedur wird nur dann gestartet, wenn für alle Datensätze in xprivate_adstore ads_status=X gesetzt ist, d.h. wenn die letzte Verarbeitung eines Snapshots durch den AD-Client erfolgreich abgeschlossen wurde. Hier der Aufruf des SQL-Skripts aus dem über den crontab-Job aufgerufenen Shell-Skript hro_ADStore:

```
isql -U$user -P$bla -i${HOME}/com/hro_ADStore_sql | tee -a ${HOME}/log/hro_ADStore
```

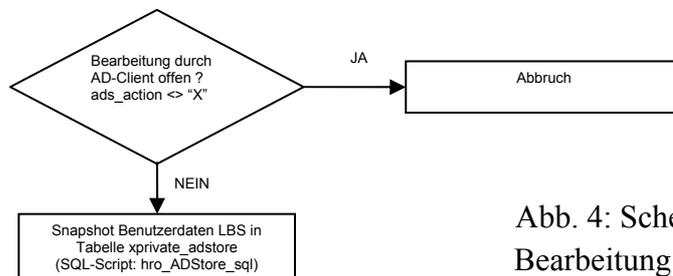


Abb. 4: Schematische Darstellung der Bearbeitung auf dem LBS-Host.

130 Die Ausführung erfolgt zu Zeiten, in denen nicht mit dem LBS gearbeitet wird. Die Bearbeitung einer größeren Anzahl von Datensätzen, etwa zu Semesterbeginn (> 5.000 und mehr) oder bei Neuaufbau der Tabelle xprivate_adstore, erfordert ggf. die Bereitstellung einer größeren Zeitscheibe.

131 Internet: <https://web10.ub.uni-rostock.de/uploads/simanowski/ma/source.pdf> [15.05.08]

Schritt 2: Der AD-Client generiert via SQL-Abfrage von xprivate_adstore ein Kommandoskript hro_ADStore_CMD.bat¹³².

Hier als Beispiel eine Zeile je AD-Operation aus hro_ADStore_CMD.bat:

```
CALL LBSUser_To_ADS DEL 00280039999 40 dummy dummy 40
CALL LBSUser_To_ADS INS 00280266999 70 220791 80508 118
CALL LBSUser_To_ADS UPD 00280004999 30 111252 80508 30
```

Alle für die Bearbeitung der Objekte im AD notwendigen Attribute werden dem Kommandoskript LBSUser_To_ADS als Parameter übergeben: die auszuführende Operation (DEL, INS, UPD), die Benutzernummer (0028...), die LBS-Benutzergruppe, das Geburtsdatum (Generierung des Erstpassworts), das aktuelle Datum sowie die Benutzergruppe im AD.

Schritt 3: Der AD-Client führt das Kommandoskript¹³³ aus. Zuerst ist immer das Löschen der Accounts auszuführen, weil z.B. ein Wechsel der LBS-Benutzergruppe bei gleichbleibender Benutzernummer über eine Löschaktion des alten Accounts und das folgende Einfügen des neuen Accounts in das AD realisiert wird. Gespeichert werden im AD lediglich die Benutzernummer, das Geburtsdatum als Erstkennwort und die Benutzergruppe¹³⁴.

Für die Ausführung der AD-Operationen werden die Microsoft ds-Tools¹³⁵ dsadd, dsmod, dsrm und die Joeware-Tools¹³⁶ ad-mod, adfind verwendet.

Schritt 4: Mit jedem Anlegen eines neuen Benutzers im AD wird eine Kommandozeile generiert, um dem Benutzer anschließend seine Benutzergruppe im AD entsprechend der LBS-Benutzergruppe oder anhand bestimmter Attributwerte des Benutzerkontos (z.B. virtuelle Benutzergruppe 118, U18-Benutzer) im AD zuzuweisen.

Auszug aus dem Kommandoskript zum Setzen der Gruppenzugehörigkeit im AD:

```
admod -b "cn=User_LBS_NTYP70_Group,ou=User_LBS_NTYP_Groups,dc=ub,dc=uni-rostock,dc=de" "member:+:cn=00280666666,ou=user_lbs_ntyp70,dc=ub,dc=uni-rostock,dc=de" -h ubdc.ub.uni-rostock.de
```

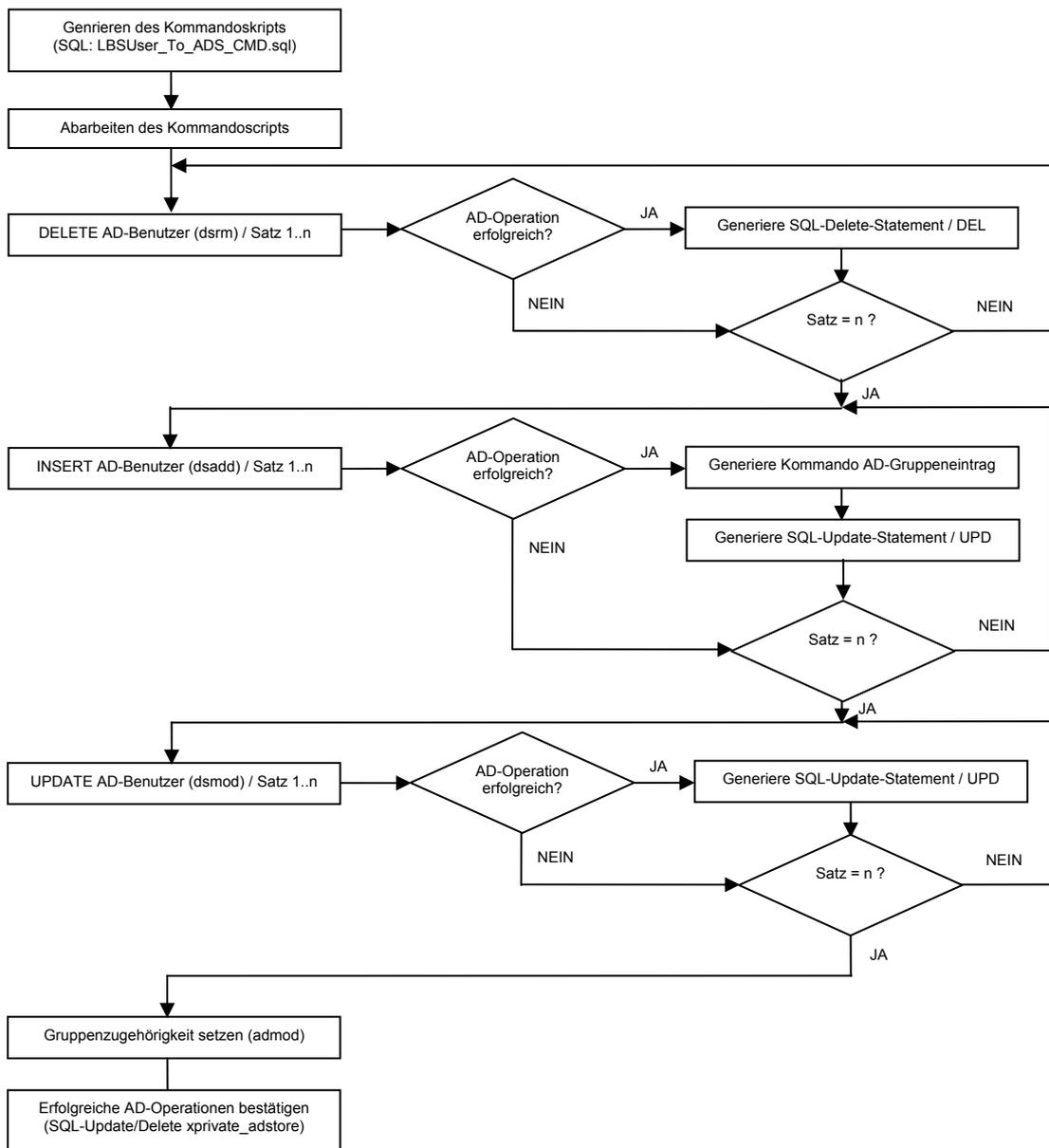
132 Ebd.

133 Ebd.

134 Im Sinne des Datenschutzes also nur die benötigten Daten und diese pseudonymisiert.

135 [\[DSTOOLS\]](#)

136 [\[JOEWARE\]](#)



(Hier nur betrachtet Satzzahl 1..n. Bei Satzzahl = 0 wird die jeweilige Operation übergangen.)

Abb. 5: Schematische Darstellung der Bearbeitung auf dem AD-Client.

Für jede erfolgreiche AD-Operation (Abfrage Errorlevel der eingesetzten Tools) wird außerdem durch den AD-Client ein SQL-Statement generiert, welches den entsprechenden Datensatz in der Tabelle `xprivate_adstore` zurücksetzt (`ads_action=X`) oder löscht.

Ein Beispiel eines Delete- / Update-Statements bei Wechsel der Benutzergruppe:

```

delete xprivate_adstore where borrower_bar = '00280389999' and borrower_type = 10 and
ads_action = 'D'
update xprivate_adstore set ads_action = 'X' where borrower_bar = '00280389999' and
borrower_type = 40 and ads_action = 'I'
  
```

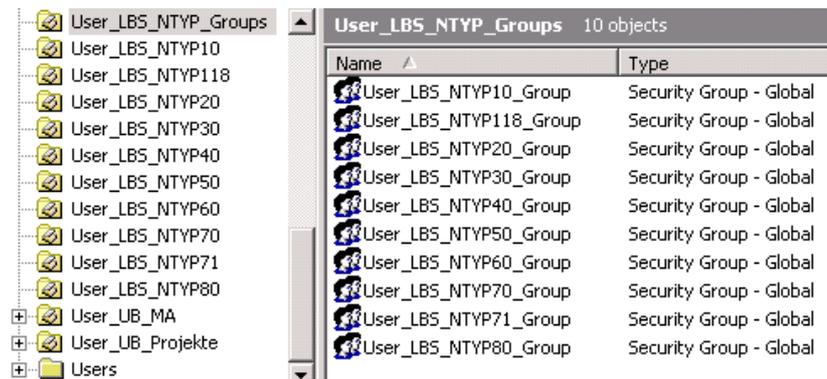


Abb. 6: Organisationseinheiten und Gruppen im Active Directory.

3.3.3 Möglichkeiten der Zugangssteuerung

Folgende grundlegende Verfahren werden eingesetzt, um den Zugang zu den Rechnern der UB und den angebotenen elektronischen Ressourcen zu steuern.

BIOS-Einstellungen / Sicherheit:

Durch bestimmte BIOS-Einstellungen wird verhindert, dass ein Benutzer den Rechner bzw. den Zugang zum Internet manipulieren kann.

Gruppenrichtlinien (computer-based):

Durch den Einsatz von Gruppenrichtlinien kann die Ausführung unerlaubter Software verhindert werden (Software-Restriction-Policies). Die Nutzung von IP-Security-Policies ermöglicht es zudem, den Zugang von Rechnern zum Internet durch IP-Security-Rules / IP-Filter einzuschränken.

Anmeldeskript:

Als Skriptsprache für alle Anmeldeprozeduren wird KiXtart¹³⁷ verwendet. Ein break off - Statement verhindert, dass Benutzer die Abarbeitung des Anmeldeskripts unterbrechen können. Alle Benutzer, die sich an den Rechnern der UB-Domäne authentifizieren, durchlaufen das Anmeldeskript logub.kix. Bei einer Authentifizierung für die Domäne des Rechenzentrums uni-rostock.de wird am Ende des Anmeldeskripts des Rechenzentrums das Anmeldeskript der UB aufgerufen:

```
Call \\ub.uni-rostock.de\Netlogon\logub.kix
```

Proxy-Server:

Der Zugang zu elektronischen Ressourcen erfolgt für alle Rechner der UB, d.h. auch für die Rechner der Mitarbeiter, über einen Proxy-Server. Zu diesem Zweck wurden

137 [\[KIXTART\]](#)

auf einem W2K3-Server drei Instanzen des Proxy-Servers Squid¹³⁸ aufgesetzt. Port 3127 ermöglicht den freien Zugang zu elektronischen Ressourcen (Rolle A - Hochschulangehörige), der Zugang über Port 3128 erfolgt über eine Blacklist (Rolle B - wnk-Benutzer) und der Zugang über Port 3129 über eine Black- und eine Whitelist¹³⁹ (Rolle C - externe und U18-Benutzer). Die Websites der Universität sowie der Katalog der UB laufen nicht über den Proxy-Server (ProxyOverride)¹⁴⁰.

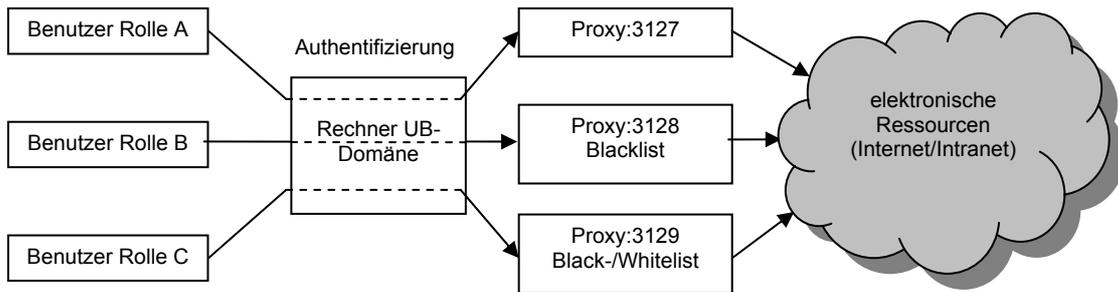


Abb. 7: Rollenbasierter Zugang zu elektronischen Ressourcen über Proxy-Instanzen.

Im Folgenden werden die realisierten Optionen für die Zugangssteuerung erläutert. Unterschieden wird dabei zwischen Optionen, die an den Rechner (computer-based) oder an die Rolle des Benutzers (role-based) gebunden sind.

3.3.3.1 Booten, Softwareausführung (computer-based)

Benutzer dürfen an den Rechnern der UB Disketten, CDs, DVDs und USB-Sticks verwenden. Über die BIOS-Einstellungen der Rechner wird verhindert, dass Benutzer die Rechner von Wechseldatenträgern booten und dass sie unberechtigt Zugang zu den BIOS- oder Intel-AMT-Einstellungen erhalten.

Für alle Rechner sind über die Gruppenrichtlinien Software-Restriction-Policies definiert, die das Ausführen von Programmen nur aus dafür vorgesehen Verzeichnissen gestatten, für die Benutzer keine Schreibrechte haben. Weitere Policies verhindern, dass Benutzer betriebsrelevante Einstellungen an den Rechnern vornehmen können. Aktuelle Updates werden automatisch über einen Windows Server Update Services (WSUS) eingespielt, ein zentraler Antivirus-Update-Server sorgt für die Verfügbarkeit eines aktuellen Antivirenprogramms (Sophos), die Personal-Firewall von Windows/XP ist auf allen Rechnern eingerichtet und aktiviert.

138 [SQUID]

139 Um einzelne Angebote im Universitätsnetz (z.B. CD-ROM-Server) für Benutzer der Rolle C zu sperren, wird vor der Whitelist noch eine Blacklist auf dem Proxy-Server Port 3129 abgearbeitet.

140 KiXtart-Skript (setenv.kix) mit möglichen Optionen für die Zuweisung der Proxy-Server-Instanzen in: Internet: <https://web10.ub.uni-rostock.de/uploads/simanowski/ma/source.pdf> [15.05.08]

3.3.3.2 Sperren Benutzergruppen (role-based)

Rechner, an denen externe Benutzer arbeiten dürfen, müssen über das Anmeldeskript explizit freigeschaltet werden. Dazu wird ein if-else-Konstrukt wie folgt verwendet:

Anmeldeskript (check_access.kix):

```
If      ( Ingroup("User_LBS_NTYP70_Group", "User_LBS_NTYP118_Group", ... ) )
;diese Rechner sind für obige Benutzergruppe(n) erlaubt
If ( @WKSTA="UB9NU999" OR @WKSTA= ... OR ... )
Else
    color n/w+
RUN ( "\\ub.uni-rostock.de\Netlogon\ub_scripts\" + "logoff_info_reserv.bat" )
    $ReturnCode=SetConsole("ALWAYSONTOP")
    $ReturnCode=SetConsole("MAXIMIZE")
    Sleep 20
    ;Nutzer abmelden
    logoff(1)
Endif
Endif
```

Alle hier nicht definierten Rechner gehören zum Typ AP1. Externe Benutzer, die sich an einem AP1-Rechner authentifizieren, erhalten eine Meldung, dass dieser Arbeitsplatz für die Nutzung durch Hochschulangehörige reserviert ist (logoff_info_reserv.bat).

3.3.3.3 Ressourcen nicht beschränken (role-based)

Für Benutzer der Rolle A (Hochschulangehörige) wird der Zugang zu den elektronischen Ressourcen nicht beschränkt. Realisiert wird dieses über die Zuweisung des Proxy-Servers Port 3127 im Anmeldeskript:

Anmeldeskript (setenv.kix)¹⁴¹:

```
SELECT
...
CASE (
    @LDDOMAIN="RECHENZENTRUM"
OR    Ingroup("User_LBS_NTYP10_Group", "User_LBS_NTYP30_Group", ...)
OR    ...
)
    SetProxy ("1", "$ProxyUB:3127", $BasicOverride)
    Gosub "GroupAOverride"
...

```

141 Bei Anwendung des SELECT-Statements ist die Reihenfolge der CASE-Blöcke zu beachten (processed top to bottom, only one case-statement executed).
Bsp.: Internet: <https://web10.ub.uni-rostock.de/uploads/simanowski/ma/source.pdf> [15.05.08]

3.3.3.4 Ressourcen beschränken mit Blacklist (role-based)

Für Benutzer der Rolle B (wnk-Benutzer) werden lediglich solche elektronischen Ressourcen gesperrt, deren Nutzung laut Lizenzvertrag nur für Hochschulangehörige zugelassen ist. Realisiert wird dieses über die Zuweisung des Proxy-Servers Port 3128 mit definierter Blacklist im Anmeldeskript:

Anmeldeskript (setenv.kix):

```
SELECT
...
CASE (
Ingroup("User_LBS_NTYP20_Group", "User_LBS_NTYP50_Group", "User_LBS_NTYP71_Group")
)
SetProxy ("1", "$ProxyUB:3128", $BasicOverride)
...
```

Proxy-Server (squid.conf):

```
...
acl blacklist url_regex -i "e:/squid3128/etc/blacklist3128.conf"
...
```

Proxy-Server (blacklist3128.conf):

```
...
# beck-online
beck-gross.digibib.net
# juris online
www.juris.de
...
# CD-ROM-Server
# DBIS:
# Beck SteuerDirekt
^.*CONFIGID=BECK_STEUERD.*$
# Beilstein CrossFire Online
^.*CONFIGID=BELSTEIN.*$
...
```

Bei Aufruf einer gesperrten Ressource wird die Fehlermeldung des Proxy-Servers (ERR_ACCESS_DENIED) auf eine Webseite der UB mit entsprechender Meldung umgeleitet¹⁴².

142 Internet: http://www.uni-rostock.de/ub/xGeneral/proxy_restrict_xde.shtml [15.05.08]

3.3.3.5 Ressourcen beschränken mit Black-/Whitelist (role-based)

Für Benutzer der Rolle C (externe und U18-Benutzer) wird lediglich eine Auswahl elektronischer Ressourcen zugelassen. Diese Auswahl beinhaltet alle öffentlich zugänglichen Seiten der Universität inkl. Homepage und Online-Katalog der UB, die Regensburger Verbundklassifikation als Aufstellungssystematik der UB, den KVK sowie die deutschen Verbundkataloge, um ggf. auch verbundübergreifende Fernleihen zu ermöglichen, den Online-Katalog der Stadtbibliothek Rostock, die freie Enzyklopädie Wikipedia sowie weitere ausgewählte Ressourcen. Auch lizenzierte elektronische Ressourcen wie z.B. SpringerLink, die über den Online-Katalog recherchierbar und zur Benutzung an den Rechnern der UB auch für externe Benutzer zugelassen sind, können genutzt werden.

Realisiert wird dieses über die Zuweisung des Proxy-Servers Port 3129 mit definierter Black- und Whitelist im Anmeldeskript:

Anmeldeskript (setenv.kix):

```
SELECT
...
CASE (
Ingroup("User_LBS_NTYP118_Group", "User_LBS_NTYP70_Group")
)
SetProxy ("1", "$ProxyUB:3129", $BasicOverride)
Gosub "MsgWhiteList"
...
```

Proxy-Server (squid.conf):

```
...
acl blacklist url_regex -i "e:/squid3129/etc/blacklist3129.conf"
...
acl whitelist url_regex -i "e:/squid3129/etc/whitelist3129.conf"
...
```

Proxy-Server (blacklist3129.conf):

```
...
# Diese Blacklist wird nur benoetigt, um Angebote aus dem UNI-Netz zu sperren !
# CD-ROM-Server
ublcd002.ub.uni-rostock.de
ubmf6.ub.uni-rostock.de
...
```

Proxy-Server (whitelist3129.conf):

```
...
# Uni-Netz
```

```

uni-rostock.de
# Hochschulen
hs-nb.de
uni-regensburg.de
...
# Bibliotheken
#-- stadtbibliothek rostock
195.37.188.172
...
# Verbuende
#-- GBV
gbv.de
...
# SpringerLink
dx.doi.org
www.springerlink.com
...
# sonstiges
wikipedia
...

```

Bei Aufruf einer gesperrten Ressource wird die Fehlermeldung des Proxy-Servers (ERR_ACCESS_DENIED) auf eine Webseite der UB mit entsprechender Meldung umgeleitet¹⁴³.

3.3.3.6 Ressourcen beschränken (computer-based)

Die Proxy-Server-Zuweisung für Benutzer der Rolle C kann analog auch für ausgewählte Rechner erfolgen (Katalog-Arbeitsplätze). An diesen Rechnern stehen dann allen Benutzern lediglich die über Black- und Whitelist des Proxy-Servers Port 3129 verfügbaren elektronischen Ressourcen zur Verfügung.

Anmeldeskript (setenv.kix):

```

SELECT
...
CASE ( @WKSTA="UB1NU001" ;BB1 Eingangsbereich
OR @WKSTA="UB1NU002" ;BB1 Eingangsbereich
...
)
SetProxy ("1", "$ProxyUB:3129", $BasicOverride)
Gosub "MsgKatalogAPC"
...

```

Analog wird bei Aufruf einer gesperrten Ressource die Fehlermeldung des Proxy-Servers (ERR_ACCESS_DENIED) auf die Webseite der UB umgeleitet¹⁴⁴.

143 Internet: http://www.uni-rostock.de/ub/xGeneral/proxy_whitelist_xde.shtml [15.05.08]

144 Ebd.

3.4 Organisatorische Realisierung

3.4.1 Planung (Aktionsplan) und Einführung

Die Erweiterung des LBS um einen rollenbasierten Zugang zu den elektronischen Ressourcen auf Basis einer Abbildung der LBS-Benutzerverwaltung auf das Active Directory und die rechner- und rollenbezogene Zuweisung verschiedener Proxy-Server-Instanzen mit definierten Access Control Lists (ACL) wird parallel zur Planung und Realisierung eines HBFG-Antrages ausgeführt, in dessen Ergebnis die UB Rostock bis Mitte 2008 über ca. 150 fest installierte Rechner im öffentlichen Bereich verfügen wird, die lediglich 2 baugleichen Gerätetypen entsprechen (HP Compaq d530 / HBFG 2004 und HP Compaq dc7800 / HBFG 2006) und die alle einheitlich mit dem Betriebssystem Windows XP/SP3 arbeiten. Die derzeit noch wenigen in Benutzung befindlichen alten, auszusondernden Rechner mit dem Betriebssystem Windows NT 4.0 können nicht in das zentrale Management der UB-Domäne unter Einsatz von Gruppenrichtlinien eingebunden werden, sind technisch veraltet (HBFG 1997) und stellen aus verschiedenen Gründen ein permanentes Sicherheitsrisiko dar.

Für die Mitarbeiter der UB wurde eine Einweisung¹⁴⁵ in Grundlagen und Funktionsweise durchgeführt, um Fragen der Benutzer qualifiziert und sicher beantworten zu können. Erste Erfahrungen nach etwa einem halben Jahr belegen, dass es von Seiten der externen Benutzer wenige Nachfragen gibt, warum der Zugang zu den elektronischen Ressourcen eingeschränkt wurde. Die Anzahl der Benutzer, die einen Antrag auf wissenschaftliche Nutzung des Datennetzes (Anlage 2) gestellt haben, ist derzeit kleiner als 10. Die geringe Anzahl der Nachfragen kann aus der Anzeige entsprechender Informationstexte bei der Authentifizierung an den Rechnern der UB und dem Verständnis der externen Benutzer dafür, dass eine Bibliothek kein kostenloses Internetcafé ist, der Zugang für jugendliche Benutzer selbstverständlich eingeschränkt werden muss (für derzeit ca. 100 U18-Benutzer) und Lizenzverträge zur Nutzung elektronischer Ressourcen eingehalten werden müssen, erklärt werden. Möglich ist aber auch, dass die Anzahl der externen Benutzer, die wirklich die Rechner in der UB nutzen, wesentlich kleiner als die Anzahl der zur Nutzung zugelassenen externen Benutzer ist oder vielleicht auch, dass die von der UB angebotene Positivliste die Informationsbedürfnisse der externen Benutzer weitestgehend abdeckt. Die Einführung erfolgt anhand eines Aktionsplans (Tabelle 1).

145 Internet: https://web10.ub.uni-rostock.de/uploads/simanowski/ma/Zugang_Externe_InfoMA_public.pdf
[15.05.08]

Aktion	Termin	Verantwortlich
1. Liste aller Rechner in den öffentlichen Bereichen für die Festlegung der Arbeitsplatztypen: AP1: nur Hochschulangehörige AP2: Zulassung auch für externe Benutzer AP3: Katalog-AP	Ende November 2007	IuK gibt Liste der Rechner an Dezernat II (Informationsdienst und Bestandsvermittlung) und Leiter Bereichsbibliotheken
2. Abstimmung der anzuzeigenden Texte bei der Anmeldung externer Benutzer	Ende 2007	Dezernat II + IuK
3. Entwerfen des Formulars für wnk-Benutzer / Benutzergruppe 71	Ende 2007	Dezernat II
4. Allgemeinen Account Benutzergruppe 70 für Fremdanmeldungen einrichten ¹⁴⁶	Ende November 2007	IuK
5. Whitelist / Blacklist erstellen	Ende 2007	Dezernat II + IuK
6. Information Info-Bibliothekare und Mitarbeiter an den Theken	Bereichsbibliothek 1 - Ende 2007, andere sukzessive mit Aufstellung der neuen Rechner	IuK
7. Aktivierung der Zugangssteuerung	Bereichsbibliothek 1 - Ende 2007, andere sukzessive mit Aufstellung der neuen Rechner	IuK
8. Kennzeichnung der Geräte (Monitore) als Katalog-AP (AP3) und als AP für externe Benutzer (AP2)	Bereichsbibliothek 1 - Ende 2007, andere sukzessive mit Aufstellung der neuen Rechner	IuK
9. Abschluss Umsetzung Zugangskonzeption	Ende II/2008 mit Abschluss der Aufstellung der neuen Rechner	IuK
10. Weiterentwicklung des Zugangskonzepts	laufende Aufgabe	Leitung + IuK

Tab. 1: Aktionsplan Einführung

Legende:

abgeschlossen
in Arbeit
offen

¹⁴⁶ Fremdanmeldungen an Rechnern in der UB werden von Mitarbeitern für Benutzer ausgeführt, deren Account noch nicht verfügbar ist (z.B. bei Erstanmeldung oder bei Ablauf/Verlängerung der Mitgliedschaft ist eine Authentifizierung erst am nächsten Tag möglich) oder die aus anderen Gründen nur einen kurzzeitigen Zugang benötigen. Der allgemeine Account für diese Fremdanmeldungen ist der Benutzergruppe 70 zugeordnet, hat also lediglich Zugang zur bereitgestellten Positivliste.

4 Alternativen und weitere Entwicklung

Das beschriebene Verfahren zur Abbildung der LBS-Benutzerverwaltung auf ein Active Directory basiert auf der Speicherung von lediglich drei Daten des Benutzers in der Verzeichnisdatenbank: Benutzernummer, Geburtsdatum als Erstkennwort und Benutzergruppe. Durch die Kombination von Gruppenrichtlinien und Zuweisung rechner- oder rollenbezogener Zugänge zu den elektronischen Ressourcen können so verschiedenste Zugangsszenarien auf einfache Art und Weise realisiert werden. Die Nutzung ist derzeit auf fest installierte Rechner in der Bibliothek beschränkt.

Alternative Lösungsansätze wären z.B. die Implementierung von Verfahren, welche die Authentifizierung direkt gegen die LBS-Datenbank ausführen oder aber die Abbildung der LBS-Benutzerverwaltung auf einen zentralen Verzeichnisdienst der Hochschule. Für beiden Ansätze sind im Bereich der PICA-Systeme Lösungen vorhanden, die alternativ oder ergänzend bzgl. bestimmter Funktionalitäten und Module eingesetzt werden können.

4.1 Lösung der UB Rostock

Die Lösung der UB Rostock ist in Kap. 3 ausführlich beschrieben, so dass hier nur auf Vor- und Nachteile sowie weitere Entwicklungsmöglichkeiten eingegangen wird.

Abbildung LBS-Benutzerverwaltung auf Active Directory (UB Rostock)

Vorteile:

- einfach zu implementieren und mit vorhandenen Systemen realisierbar,
- keine Kosten für Software, Verwendung von Standard-Software und -Tools,
- direkte Einbindung in das Active Directory, dadurch einfache Nutzung von Gruppenrichtlinien und rollenbasierter Zuweisung von Ressourcen und Services möglich,
- redundante und alternative Authentifizierung für Hochschulangehörige.

Nachteile:

- keine Passwortsynchronisation mit LBS (WINIBW), Entwicklung eigener Prozedur notwendig (Einbindung in Benutzerverwaltung Online-Katalog),
- Zeitverzögerung beim Abgleich der Benutzerdaten (Snapshot),
- umständliche Einrichtung virtueller Benutzergruppen über das SQL-Skript anhand bestimmter Eigenschaften der Benutzer (z.B. U18-Benutzer),
- kein hochschulweiter Einsatz durch Beschränkung auf fest installierte Rechner der UB-Domäne, dadurch keine hochschulweiten Identitäten.

Weitere Entwicklung:

Passwortsynchronisation: Die Prozedur zur Änderung des Passwortes im Online Katalog soll so modifiziert werden, dass der Eintrag gleichzeitig in LBS und Active Directory erfolgt. Die Realisierung ist mit PHP geplant, ein Modul zur Aufsatzlieferung, welches eine Authentifizierungsfunktion enthält, wurde bereits im Layout des Online-Katalogs implementiert und kann als Basis verwendet werden¹⁴⁷.

Einspielen von Benutzerdaten: Das Einspielen der Benutzerdaten der Hochschulangehörigen soll automatisiert werden, so dass ein Eintrag im Hochschul-Informationen-System (HIS) über das Metadirectory der Universität (DirX Identity¹⁴⁸) einen Eintrag in der LBS-Datenbank generiert. Bislang werden lediglich die Benutzerdaten der Studenten zu Semesterbeginn offline in das LBS eingespielt.

Pflege der Access Control Listen: Die Access Control Listen der Proxy-Server-Instanzen sollen ihre Einträge aus Datenbanken, die Adressen und Zugriffsrechte der elektronischen Ressourcen enthalten, über Schnittstellen (z.B. HTTP/XML) beziehen. Mit BSZ (DIB) und ZLB (Linksammlung) soll Kontakt aufgenommen werden, um die Bereitstellung einer Schnittstelle zum Bezug aktueller und verifizierter Adressen zu prüfen. Diese können in die Positivliste für Benutzer der Rolle C aufgenommen werden. Von großem Interesse wäre eine zusammengefasste Datenbank mit Informationen zu allen lizenzierten elektronischen Ressourcen der wissenschaftlichen Bibliotheken. Bislang sind Informationen in ZDB, EZB und DBIS verteilt enthalten. Sinnvoll wäre der Aufbau einer nationalen Datenbank, die alle Informationen diesbezüglich enthält und über eine Schnittstelle verfügbar macht. Die Katalogisierungsrichtlinien der ZDB¹⁴⁹ erlauben unter den Exemplardaten die Verwaltung codierter Angaben zu den Zugriffsrechten (Kategorie 7133), so dass z.B. die Codierung des Zugriffsrechts „Zugriff durch externe Benutzer in der Bibliothek erlaubt“ hier möglich wäre.

AAI/Shibboleth: Mittelfristig ist die Anbindung an ein System zur verteilten Authentifizierung und Autorisierung geplant.¹⁵⁰ Ob der zu realisierende Identity-Provider über LDAP an einen Verzeichnisdienst oder über eine SQL-Schnittstelle an die LBS-Datenbank angebunden wird, ist dabei noch offen.

147 Aufsatzlieferdienst der UB Rostock im Internet: <https://katalog.ub.uni-rostock.de/ald/> [05.05.08]

148 [\[DIRX\]](#)

149 Katalogisierungsrichtlinien der ZDB (ZETA) im Internet: <http://www.zdb.spk-berlin.de/katalogisierung/zeta.html> [05.05.08]

150 Siehe Kap. 4.3 zum Thema AAI/Shibboleth.

4.2 Alternative Lösungsansätze

4.2.1 Lösung der SUB Hamburg

Ein Verfahren, welches die Authentifizierung direkt gegen die LBS-Datenbank ausführt und zusätzliche Funktionalitäten zur Steuerung des Zugangs zu den Internet-Arbeitsplätzen ermöglicht, wurde bereits 2002 durch Christian Karolyi auf der Verbundkonferenz des GBV in Kiel vorgestellt¹⁵¹. Das Verfahren ist bereits in mehreren Bibliotheken des GBV im Einsatz¹⁵².

Grundfunktionalitäten dieser Lösung sind:

- Authentifizierung gegen die LBS-Datenbank,
- Steuerung der Benutzungsdauer,
- Vergabe individueller Zeitkontingente,
- Mögliche Sperrung einzelner Benutzer für den Zugang zum Internet,
- Einrichtung von Gastkonten ohne LBS-Benutzerkonto,
- Webinterface für die Administration durch Mitarbeiter der Bibliothek.

Für den Betrieb wird ein Webserver (Apache) benötigt, auf dem eine MySQL-Datenbank, PHP für die Ausführung der Skripts sowie ein Sybase-Client für den Zugriff auf die LBS-Datenbank installiert ist.

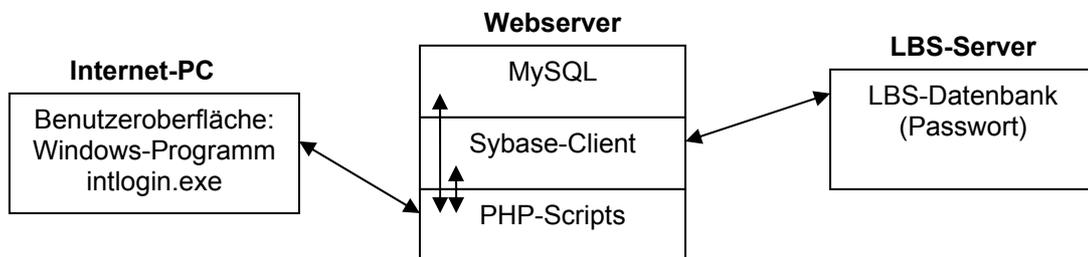


Abb. 8: Lösung der SUB Hamburg - Basismodule

Prinzipiell könnten mit dieser Lösung die Funktionalitäten der Lösung der UB Rostock bzgl. des Zugangs zu elektronischen Ressourcen auch realisiert werden. Über die PHP-Skripts können beliebige Attribute der Benutzer zur Auswertung herangezogen werden, so dass eine rollenbasierte Zuweisung von Proxy-Server-Instanzen mit verschiedenen Access Control Listen hier auch möglich wäre¹⁵³. Vorteile diese Lösung liegen in der nicht benötigten Passwortsynchronisation, da die

151 [\[Karolyi2002\]](#)

152 U. a. in der SUB Hamburg, der SUUB Bremen und der UB Greifswald.

153 Eine derzeit nicht vorhandene Funktionalität, die auch nicht der primären Intention der Lösung entspricht.

Authentifizierung direkt gegen die LBS-Datenbank erfolgt, sowie in den zusätzlichen Funktionen zur Verwaltung der Benutzerkonten und Rechner, die sich via PHP-Skript einfach anpassen und erweitern sowie über einen Webbrowser administrieren lassen. Seit 2008 kommt in der SUB eine Weiterentwicklung der oben genannten Lösung zum Einsatz, bei welcher der Anmeldevorgang unter Verwendung der Software pGina in die Windows-Anmeldeprozedur integriert ist. Die Anmeldefunktionen aus „intlogin.exe“ wurden hierfür in ein neu entwickeltes pGina-Authentifizierungs-Plugin übertragen. So wird bei der Benutzeranmeldung eine lokale Benutzerkennung erstellt, die der LBS-Benutzerausweisnummer entspricht. Bei der Abmeldung werden Kennung und Benutzerprofil automatisch gelöscht.¹⁵⁴

Nachteilig für die Lösung der SUB Hamburg ist die Authentifizierung gegen die LBS-Datenbank, wenn es um die Zuweisung von Ressourcen und Services geht, die an einen Verzeichnisdienst gebunden sind und über Gruppenrichtlinien oder die Ausführung des Anmeldeskripts zugewiesen werden. Außerdem ermöglicht die Lösung der UB Rostock den Hochschulangehörigen eine Anmeldung an der Domäne des Rechenzentrums und damit die Nutzung aller für diesen Account verfügbaren Ressourcen und Services, so auch die Nutzung der zentral abgelegten hochschulweiten Benutzerprofile.

4.2.2 H+H / Hidden Automatic Navigator (HAN)

Der Hidden Automatic Navigator (HAN)¹⁵⁵ ist ein kommerzielles Produkt der Firma H+H Software GmbH und befindet sich in mehreren Bibliotheken im Einsatz.

HAN unterstützt die folgenden Funktionalitäten¹⁵⁶:

- Authentifizierung mit mehreren Optionen für das Zielsystem (Microsoft AD, Novell NDS, LDAP, SISIS, PICA, ODBC ...),
- Automatische Hintergrundanmeldung,
- Management der Zugriffsrechte auf verschiedenen Ebenen (IP, DNS, Benutzer, Rechner für beliebige Gruppierungen von Titeln und Verlagen),
- Transparenter, ortsunabhängiger Zugriff durch Reverse-Proxy Funktionalität,
- Lizenzkontrolle (Anzahl Benutzer für gleichzeitige Nutzung),
- Erstellen von Nutzungsstatistiken,
- EZB-Schnittstelle für manuelle oder automatisierte Importfunktion,
- Verwaltung von elektronischen Ressourcen mit Subskriptionszeiträumen.

154 Information zum Einsatz von pGina in der SUB Hamburg von Christian Karolyi, 21.05.2008. Siehe auch Internet: <http://www.pgina.org/> [15.05.08].

155 Internet: <http://www.hh-han.com/de/> [15.05.08]

156 [[HAN](#)]

HAN wird z.B. an der BSB seit mehreren Jahren eingesetzt, um registrierten Benutzern den Zugang zu elektronischen Zeitschriften, CD-ROMs und Online-Datenbanken auch von Arbeitsplätzen außerhalb der Räumlichkeiten der Staatsbibliothek zu ermöglichen. Im Rahmen eines Projektes zur überregionalen Bereitstellung und Förderung von Online-Datenbanken im Bereich geisteswissenschaftlicher Sondersammelgebiete wird HAN an der BSB u. a. für die Bereitstellung einer Pay-per-Use Funktionalität für externe Benutzer genutzt¹⁵⁷.

Die Anbindung von HAN an ein LBS-PICA erfolgt über einen Sybase-Client auf dem HAN-Server und ODBC durch Einrichtung eines System-DSN mit Angabe von LBS-Server und -Datenbank.

Der Einsatz eines professionellen Produktes wie HAN sollte mit nicht unerheblichen finanziellen Mitteln verbunden sein. Eine Komponente für die Authentifizierung an den Rechnern in der Bibliothek ist nicht enthalten.

4.2.3 OCLC / Identity Management Connector

Im Rahmen des Metadirectory-Projektes CODEX führen die Hochschulen des Landes Thüringen ein System zum Identitätsmanagement auf Basis eines integrierenden Verzeichnisdienstes ein. Das Identitätsmanagement ermöglicht eine hochschulweite Verwaltung der Identität von Personen und soll die Grundlage für Services wie Benutzer-Provisioning sowie eine zentrale Authentifizierung und Autorisierung sein.¹⁵⁸

Eines der Quellsysteme für das Metadirectory ist das LBS-PICA, welches von allen im GBV befindlichen Thüringer Bibliotheken eingesetzt wird. 2006 wurde das Pilotprojekt CODEX-Pica v2 zur Anbindung des LBS-PICA an das Metadirectory gestartet. Grundlage ist der auf Java basierende OCLC Identity Management Connector¹⁵⁹. Die Aufnahme des Produktionsbetriebs ist für 2008 geplant¹⁶⁰.

Im Gegensatz zum Projekt der UB Rostock werden im CODEX-Pica v2 Projekt alle Benutzer, auch die externen, echtzeitsynchron in einem zentralen Metadirectory abgebildet und einer Bibliotheksbenutzerrolle zugewiesen. Die Bibliothek unterhält keinen eigenen Verzeichnisdienst. Der Workflow einer Benutzerregistrierung in LBS und Metadirectory ist in [Rosifka2007] dargestellt.

157 BSB: Überregionale Bereitstellung und Förderung von Online-Datenbanken im Bereich geisteswissenschaftlicher Sondersammelgebiete. Internet: http://www.bsb-muenchen.de/UEberregionale_Bereitstellung.705.0.html?&L=tx_ttnews%5Bpointer%5D%3D16 [15.05.08]

158 [Rosifka2004]

159 [Weinberger2006] und Internet: <http://www.oclc.org/de/de/idmconnector/> [15.05.08]

160 [Rosifka2007]

Dieses kommerzielle System kann als Grundlage für alle rollenbasierten Zuweisungen von Ressourcen und Services eingesetzt werden. Die Einführung ist allerdings sehr komplex und umfangreich und bedarf einiger personeller und finanzieller Kapazitäten. Eine Kooperation von Hochschulen wie im Falle des Thüringer Projektes kann nur empfohlen werden, da es dadurch zu erheblichen Synergieeffekten bei der Einführung, der Betreuung, der weiteren Entwicklung und vielleicht auch in finanzieller Hinsicht kommen kann.

4.2.4 OCLC / SISIS-SunRise webControl

SISIS-SunRise webControl¹⁶¹ ist eine Lösung im SISIS-SunRise¹⁶² Umfeld, die eine Authentifizierung direkt gegen die LBS-Datenbank ausführt und auf dieser Basis Funktionalitäten zur Steuerung des Zugangs zu elektronischen Ressourcen im Internet inklusive einer Abrechnungsfunktion ermöglicht. SISIS-SunRise webControl befindet sich z.B. an der BSB im Einsatz.

Folgende Funktionalitäten werden unterstützt:

- Browserintegrierte Authentifizierung gegen SISIS-SunRise-Datenbank mit Auswertung in Abhängigkeit von der Benutzergruppe:
 - o Zugangsberechtigung
 - o Maximale Dauer der Internet-Nutzung pro Tag
 - o Fällige Gebühr für den Internet-Zugang pro Zeitintervall
 - o kostenfreie Surfzeit pro Tag,
- Administration direkt über SISIS-SunRise-System,
- Verwaltung kostenfreier und kostenpflichtiger Ressourcen,
- Anzeige der kostenfreien Ressourcen für die Benutzer,
- Zugang zu kostenfreien Ressourcen für gesperrte oder nicht registrierte (Walk-in-User) Benutzer möglich,
- Automatische Verbuchung und Ausweisung der Gebühren in den Benutzerkonten von SISIS-SunRise.

SISIS-Sunrise webControl wurde bislang im LBS-PICA-Umfeld noch nicht implementiert. Die Kommunikation mit der SISIS-SunRise Ausleihe erfolgt über eine SLNP-Schnittstelle. Zur Verwaltung der Internetzugriffe wird ein separater Proxy-Server (Squid) eingesetzt. Außerdem wird Perl benötigt. SISIS-SunRise webControl ist für den Microsoft Internet Explorer getestet und freigegeben¹⁶³.

161 Internet: http://www.sisis.de/sisis_news/sisis_news_10/news.html [15.05.08]

162 SISIS-SunRise ist ein Lokales Bibliothekssystem, welches ehemals von SISIS und jetzt von OCLC vertrieben wird. SISIS-SunRise kommt u. a. im BVB zum Einsatz. Internet: <http://www.oclc.org/de/de/sunrise/> [15.05.08]

163 Stand Januar 2008: Internet Explorer 6 und 7, Mozilla mit Einschränkungen.

4.3 AAI / Shibboleth

Ausgehend vom BMBF-geförderten AAR-Projekt¹⁶⁴ wird derzeit eine deutschlandweite Infrastruktur zur Authentifizierung und Autorisierung (AAI) eingeführt. Koordinierende Einrichtung für den Aufbau einer Föderation von Anbietern und Nutzern elektronischer Ressourcen unter dem Titel DFN-AAI auf der Grundlage einheitlicher Richtlinien ist der DFN-Verein¹⁶⁵. Als Verfahren kommt das im Rahmen des Internet2-Projektes¹⁶⁶ entwickelte Shibboleth¹⁶⁷ zum Einsatz.

Folgende Ziele werden mit dem Projekt verfolgt¹⁶⁸:

- Zugriff auf lizenzierte elektronische Ressourcen von beliebigen Internet-Arbeitsplätzen (auch außerhalb der Bibliothek),
- Einmalige Anmeldung zur Nutzung aller lizenzierten elektronischen Ressourcen (Single Sign-On),
- Anbindung an bestehende Authentifizierungssysteme (LDAP, SQL ...),
- Schutz lizenzierter elektronischer Ressourcen vor unberechtigtem Zugriff,
- Wegfall der Benutzerverwaltung für Anbieter elektronischer Ressourcen,
- Statistische Auswertung der Nutzungsdaten auch mit dem Hintergrund der Einführung von Abrechnungssystemen.

Die Komponenten eines Shibboleth-Systems im Rahmen der DFN-AAI sind:

- Identity-Provider bei den nutzenden Einrichtungen (Bibliothek, Rechenzentrum ...),
- Service-Provider beim Anbieter der elektronischen Ressourcen (Verlage, ...),
- WAYF-Service (Where-Are-You-From) als Liste der teilnehmenden Einrichtungen und Anbieter (DFN-Verein).

Der Einsatz eines Shibboleth-Systems ist mit der Einführung einer elektronischen Identität für die Benutzer verbunden. Zu diesem Zweck müssen Attribute nach einem standardisierten Schema belegt werden¹⁶⁹, die dann nach zwischen Identity- und Service-Provider definierten Regeln ausgewertet werden können.

Die Verbundzentrale des GBV ist Mitglied der DFN-Föderation und hat bereits 2007 einen Identity-Provider mit Einzelnutzerverwaltung sowie einen Service-Provider

164 Siehe [Ruppert2007] und Internet: <http://aar.vascoda.de/> [15.05.08]

165 Internet: <https://www.aai.dfn.de/> [15.05.08]

166 Internet: <http://www.internet2.edu/> [15.05.08]

167 Internet: <http://shibboleth.internet2.edu/> [15.05.08]

168 [Borel2007] gibt außerdem eine Liste mit internationalen Anbietern (Index of Shibboleth-Enabled Applications and Services) und Projekten in Deutschland an. S. 27.

169 Attribute z.B. nach eduPerson / US-AAI-Föderation InCommon.
Internet: <http://www.incommonfederation.org/attributes.html> [15.05.08]

mit Proxy für den individuellen Zugang zu den Nationallizenzen über ein Shibboleth-System realisiert¹⁷⁰.

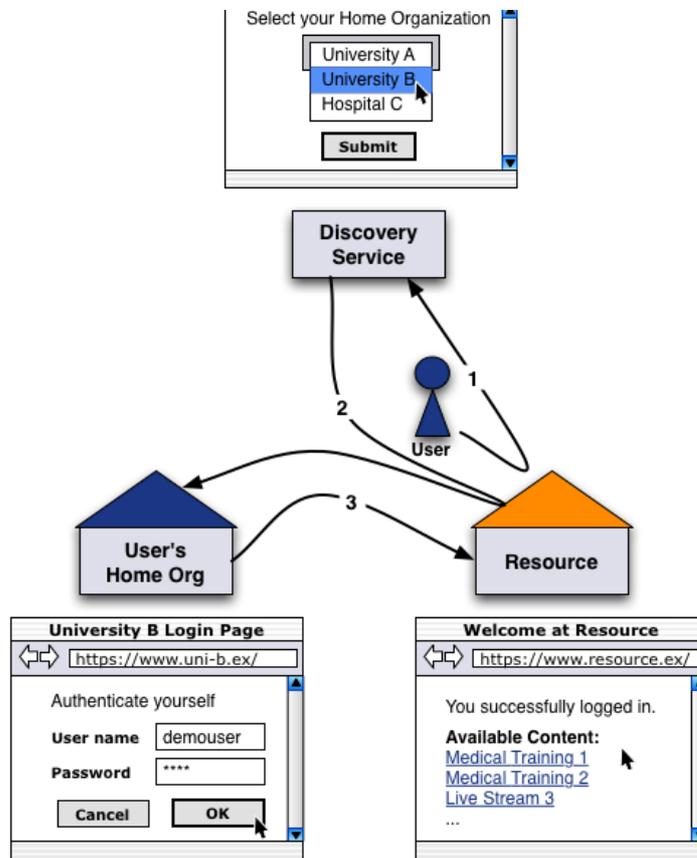


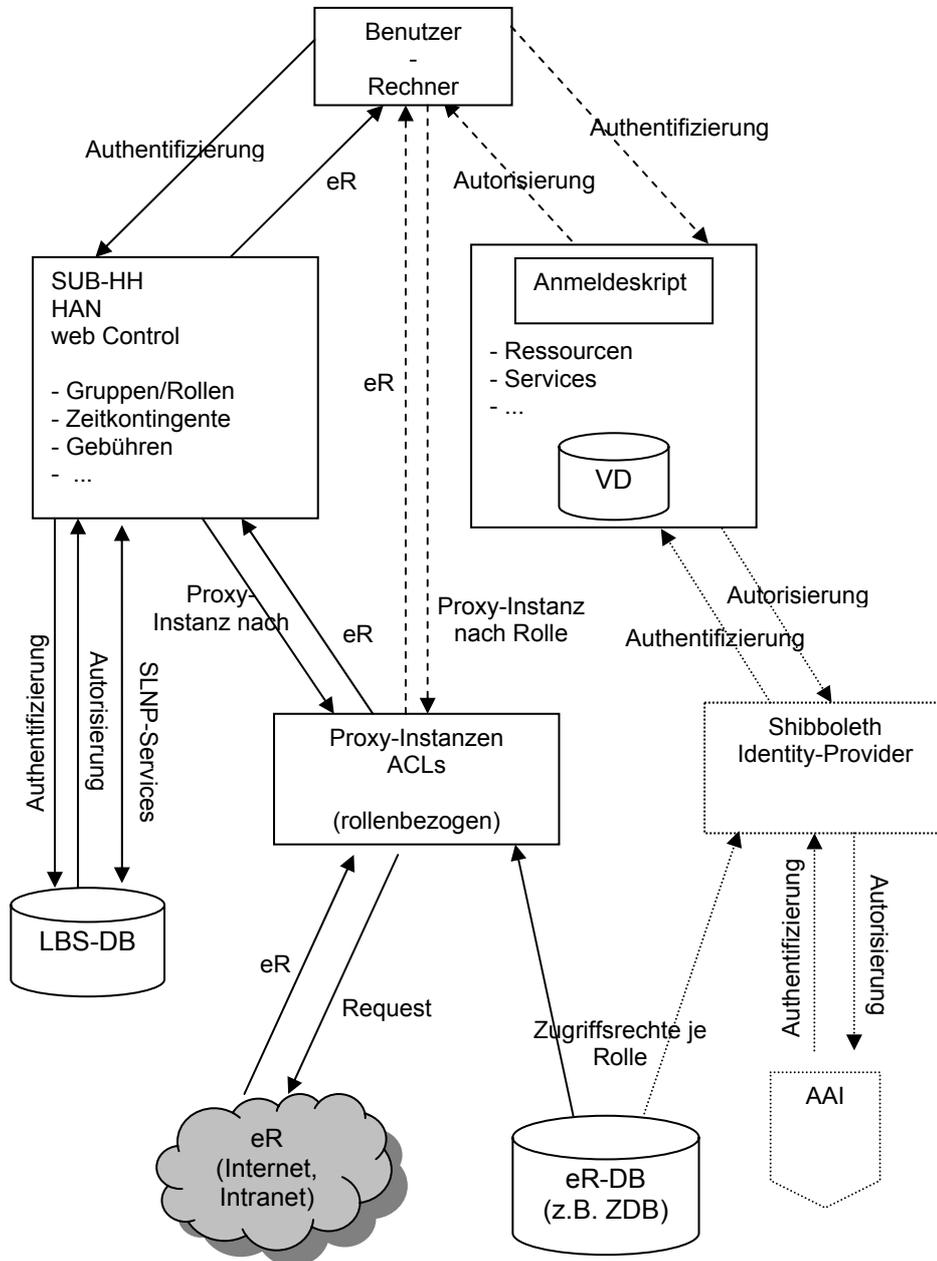
Abb. 9: Ablauf von Authentifizierung und Autorisierung beim Zugriff eines Benutzers auf eine elektronische Ressource in einer AAI¹⁷¹. (User's Home Org = Identity-Provider, Discovery-Service = WAYF-Service, Resource = Service-Provider)

Es kann davon ausgegangen werden, dass Shibboleth sich weltweit als Standard für die verteilte Authentifizierung und Autorisierung beim Zugriff auf lizenzierte elektronische Ressourcen durchsetzen wird. Die Implementierung und Anbindung eines Identity-Providers an einen hochschulweiten Verzeichnisdienst unter Einbeziehung des Lokalen Bibliothekssystems ist eine Aufgabe, die kaum eine Bibliothek im Alleingang bewältigen kann. Hier ist eine Kooperation von Rechenzentren und Bibliotheken auf Landes-, Bundesebene sowie mit dem DFN-Verein notwendig.

170 [Steilen2007]

171 Quelle SWITCH. Internet: <http://switch.ch/aa1/demo/2/simple.html> [15.05.08]

Die abschließende Abbildung zeigt schematisch das Prinzip der bislang eingesetzten Verfahren und die mögliche Anbindung an eine auf Shibboleth basierende AAI.



Legende: AAI = Authentifizierungs- / Autorisierungs-Infrastruktur auf Basis Shibboleth
 ACL = rollenbasierte Access Control List
 eR = elektronische Ressource
 eR-DB = Datenbank mit Zugriffsinformationen zu elektronischen Ressourcen
 LBS-DB = Datenbank des Lokalen Bibliothekssystems
 VD = lokaler oder hochschulweiter Verzeichnisdienst

Abb. 10: Schematische Darstellung möglicher Komponenten einer rollenbasierten Authentifizierung und Autorisierung bei der Nutzung elektronischer Ressourcen

5 Schlussbemerkungen

Es sollte sichtbar geworden sein, dass die kommenden Aufgaben zur Schaffung einer international abgestimmten verteilten Authentifizierungs- und Autorisierungs-Infrastruktur (AAI) nur in kooperativen Strukturen und nicht durch lokale Bibliotheken und Rechenzentren allein zu bewältigen sind. DFN-Verein und Bibliotheksverbände bieten vorhandene Organisationsstrukturen, die in diesem Zusammenhang genutzt werden müssen. Ein Projekt wie das Metadirectory-Projekt CODEX schafft an allen Hochschulen des Landes Thüringen eine einheitliche Basis für die Integration der Lokalen Bibliothekssysteme in einen hochschulweiten Verzeichnisdienst und ist ein Beispiel für eine kooperative Planung und Einführung.

Für die Erfüllung ihrer Aufgaben, die in der Zukunft immer mehr an die Verwaltung und Bereitstellung elektronischer Ressourcen gebunden sein werden, ist eine Beteiligung der Bibliotheken an dieser Entwicklung existentiell, wenn sie auf einem globalen und vernetzten Informationsmarkt mit ihrem „Service Bibliothek“ bestehen wollen.

Wenn Hans-Gert Gräbe in seinem Aufsatz „Die Macht des Wissens in der modernen Gesellschaft“¹⁷² den Informationsvorteil und den Kompetenzvorteil als die beiden Vorteilsprinzipien bei der Sozialisation von Information und Wissen in der postmodernen Informationsgesellschaft charakterisiert und letztlich konstatiert:

„Kompetenz ist eine Gesellschaft strukturierende Macht und steht heute im Wettstreit und zunehmend im Widerspruch zur Gesellschaft strukturierenden Macht des Geldes. Geldmacht ist [...] Definitionsmacht. Sie passt perfekt zum Ansatz "Informationsvorteil", denn dieser funktioniert nur, wenn man "die Regeln bestimmen" kann. Kompetenzmacht ist [...] Gestaltungsmacht, und zentral konstituierendes Element des Kompetenzvorteilsmodells ist das "Leben in fairen Regeln“,

so kann im dialektischen Sinne dieser Widerspruch als Paraphrase einer weiteren Entwicklung der Informationsgesellschaft verstanden werden, in deren Verlauf Bibliotheken einen nicht unerheblichen Anteil an der Erlangung von Kompetenz aller Individuen leisten und damit ihren Teil zur Strukturierung einer demokratischen Informationsgesellschaft auf Basis eines Lebens in fairen Regeln beitragen können.

172 [[Gräbe2005](#)], S. 643.

Anhang

Abkürzungsverzeichnis

AAI	Authentication and Authorization Infrastructure <ul style="list-style-type: none">• http://www.switch.ch/de/aai/
AAR	Verteilte Authentifizierung, Autorisierung und Rechteverwaltung, ein Projekt im Rahmen von Vasco, gefördert vom BMBF <ul style="list-style-type: none">• http://www.medigrid.de/u_veranst/070327security-ws/v14_aar_20070327-goettingen.pdf
AD	Active Directory, auch Active Directory Service (ADS), ab Windows Server 2008 Active Directory Domain Services (ADDS), Verzeichnisdienst von Microsoft <ul style="list-style-type: none">• http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/• http://de.wikipedia.org/wiki/Active_Directory
AD-Client	Rechner, der ein Kommandoskript mit AD-Aktionen ausführt und damit Accounts im AD anlegt, aktualisiert oder löscht.
AMT	Intel Activ Management Technology (Intel vPro Technology) <ul style="list-style-type: none">• http://www.intel.com/technology/vpro/
BMBF	Bundesministerium für Bildung und Forschung <ul style="list-style-type: none">• http://www.bmbf.de/
BMWi	Bundesministerium für Wirtschaft und Arbeit <ul style="list-style-type: none">• seit Ende 2005 in Bundesministerium für Wirtschaft und Technologie und Bundesministerium für Arbeit und Soziales aufgeteilt• http://www.bmwi.de/• http://www.bmas.bund.de/
BNB	British National Bibliography <ul style="list-style-type: none">• http://www.bl.uk/bibliographic/natbib.html
BPJM	Bundesprüfstelle für jugendgefährdende Medien <ul style="list-style-type: none">• http://www.bundespruefstelle.de/
BSZ	Bibliotheksservice-Zentrum Baden-Württemberg <ul style="list-style-type: none">• http://www2.bsz-bw.de/cms/
BVB	Bibliotheksverbund Bayern <ul style="list-style-type: none">• http://www.bib-bvb.de/
BVerfG	Bundesverfassungsgericht <ul style="list-style-type: none">• http://www.bundesverfassungsgericht.de/
DBIS	Datenbank Infosystem <ul style="list-style-type: none">• http://rzblx10.uni-regensburg.de/dbinfo/
DIB	Deutsche Internetbibliothek <ul style="list-style-type: none">• http://www.internetbibliothek.de/dibl/
DNB	Deutsche Nationalbibliothek <ul style="list-style-type: none">• http://www.d-nb.de/
DSL	Digital Subscriber Line (Digitaler Teilnehmeranschluss) <ul style="list-style-type: none">• http://de.wikipedia.org/wiki/DSL

DSN	Data Source Name <ul style="list-style-type: none"> • siehe ODBC
EZB	Elektronische Zeitschriftenbibliothek <ul style="list-style-type: none"> • http://rzblx1.uni-regensburg.de/ezeit/
FAST	FASTData Search / Produkt der Firma FastSearch & Transfer (FAST) <ul style="list-style-type: none"> • http://www.fastsearch.com/
FRBR	Functional Requirements for Bibliographic Records <ul style="list-style-type: none"> • http://www.ifla.org/VII/s13/wgfrbr/ (IFLA FRBR Review Group) http://www.collectionscanada.gc.ca/jsc/docs/5rda-frbrmappingrev.pdf (RDA to FRBR mapping, December 2007) http://www.d-nb.de/standardisierung/pdf/frbr_deutsch.pdf http://www.d-nb.de/standardisierung/afs/frbr_workshop.htm
GBV	Gemeinsamer Bibliotheksverbund <ul style="list-style-type: none"> • http://www.gbv.de/
HBZ	Hochschulbibliothekszentrum des Landes Nordrhein-Westfalen <ul style="list-style-type: none"> • http://www.hbz-nrw.de/
HeBIS	Hessisches Bibliotheks-Informationssystem <ul style="list-style-type: none"> • http://www.hebis.de/
HTTP	HyperText Transfer Protocol
KOBV	Kooperativer Bibliotheksverbund Berlin-Brandenburg <ul style="list-style-type: none"> • http://www.kobv.de/
LDAP	Lightweight Directory Access Protocol zur Abfrage und Modifikation von Informationen eines Verzeichnisdienstes <ul style="list-style-type: none"> • http://de.wikipedia.org/wiki/LDAP
LoC	Library of Congress <ul style="list-style-type: none"> • http://www.loc.gov/
Lucene	Open-Source-Bibliothek, Teil des Apache Software Foundation-Projekts <ul style="list-style-type: none"> • http://lucene.apache.org/
MARC	MAchine Readable Catalogue <ul style="list-style-type: none"> • http://www.loc.gov/marc/ (Library of Congress – Network Development and MARC Standards Office)
OAI	Open Archives Initiative <ul style="list-style-type: none"> • http://www.openarchives.org/
OAI-PMH	Open Archives Initiative – Protocol for Metadata Harvesting <ul style="list-style-type: none"> • http://www.openarchives.org/pmh/
OBV	Österreichischer Bibliotheksverbund <ul style="list-style-type: none"> • http://www.obvsg.at/
OCLC	Online Computer Library Center (Ohio / USA) <ul style="list-style-type: none"> • http://www.oclc.org/ • http://www.oclc.org/de/de/services/management/
ODBC	Open Database Connectivity <ul style="list-style-type: none"> • http://msdn.microsoft.com/en-us/library/ms710252(VS.85).aspx
OLJB	Oberste Landesjugendbehörden <ul style="list-style-type: none"> • http://www.bmfsfj.de/bmfsfj/generator/Politikbereiche/kinder-und-jugend.did=16638.html

OU	Organisation Unit, administrativer Container für Objekte im Active Directory <ul style="list-style-type: none">• siehe AD (Active Directory)
PICA	Project of Integrated Catalogue Automation, ehemalige Stiftung in Leiden (Niederlande), ab 2005 OCLC PICA, ab 2007 OCLC <ul style="list-style-type: none">• siehe OCLC
PSI	Pica Searching & Indexing, Bestandteil der PICA-Systeme
RDA	Resource Description and Access <ul style="list-style-type: none">• http://www.collectionscanada.gc.ca/jsc/ (Joint Steering Committee for Development of RDA (JSC))
SLNP	Simple Library Network Protocol <ul style="list-style-type: none">• http://www.suub.uni-bremen.de/verbundkonferenz/vor/keck.ppt
SSG	Sondersammelgebiet nach Sondersammelgebietsplan der DFG <ul style="list-style-type: none">• http://webis.sub.uni-hamburg.de/
SWB	Südwestdeutscher Bibliotheksverbund <ul style="list-style-type: none">• siehe Bibliotheksservice-Zentrum Baden-Württemberg (BSZ)
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights (Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums) <ul style="list-style-type: none">• http://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm
VLAN	Virtual Local Area Network <ul style="list-style-type: none">• http://de.wikipedia.org/wiki/VLAN
VPN	Virtual Private Network <ul style="list-style-type: none">• http://de.wikipedia.org/wiki/Virtual_Private_Network
W2K3	Microsoft Windows Server 2003 <ul style="list-style-type: none">• http://www.microsoft.com/germany/windowsserver2003/
WIPO	World Intellectual Property Organization (Weltorganisation für geistiges Eigentum) <ul style="list-style-type: none">• http://www.wipo.int/
WLAN	Wireless Local Area Network <ul style="list-style-type: none">• http://de.wikipedia.org/wiki/WLAN
wnk	wissenschaftlich, nichtkommerziell in Zusammenhang mit der Nutzung elektronischer Ressourcen, z.B. wnk-Benutzer
WTO	World Trade Organization (Welthandelsorganisation) <ul style="list-style-type: none">• http://www.wto.org/
Z39.50	Netzwerkprotokoll zur Abfrage von bibliographischen Informationssystemen <ul style="list-style-type: none">• http://www.loc.gov/z3950/agency/ (International Standard Maintenance Agency - Z39.50 der Library of Congress)• http://de.wikipedia.org/wiki/Z39.50
ZDB	Zeitschriftendatenbank <ul style="list-style-type: none">• http://www.zeitschriftendatenbank.de/
Zing/SRU	Z39.50 International Next Generation / Search/Retrieve via URL <ul style="list-style-type: none">• http://www.loc.gov/standards/sru/
ZLB	Zentral- und Landesbibliothek Berlin <ul style="list-style-type: none">• http://www.zlb.de/

Literaturverzeichnis

Kapitel 1 – Einleitung

[AEMR]

Office of the High Commissioner for Human Rights (Hrsg.): *Die Allgemeine Erklärung der Menschenrechte. Resolution 217 A (III) vom 10.12.1948*. Offizielle deutsche Übersetzung, 1948. Internet: <http://www.unhchr.ch/udhr/lang/ger.pdf> [22.04.08]

[AGVB53]

Arbeitsgemeinschaft der Verbundsysteme: *Aus der 53. Sitzung der Arbeitsgemeinschaft der Verbundsysteme am 6. und 7. November 2007 in München*. München, 2007. Internet: http://www.d-nb.de/standardisierung/pdf/ag_verbund_sitzungsbericht_53.pdf [22.04.08]

[AHLB2003]

Deutsche Forschungsgemeinschaft (DFG) (Bibliotheksunterausschusses für Informationsmanagement / Kommission für Rechenanlagen): *Die Ausstattung von Hochschulbibliotheken mit lokalen Bibliothekssystemen im HBFV-Verfahren (A H L B)*. Vierte, aktualisierte Auflage, 2003. Internet: http://www.dfg.de/forschungsfoerderung/wissenschaftliche_infrastruktur/wgi/download/ahlb2003a4.pdf [05.05.08]

[Beger2002]

Beger, Gabriele: *Urheberrecht und elektronische Bibliotheksangebote. Ein Interessenkonflikt*. 1. Aufl., Berlin: Logos-Verlag, 2002.

[BMBF2007]

Bundesministerium für Bildung und Forschung (Hrsg.): *IKT 2020. Forschung für Innovation*. Bonn u. a.: BMBF, 2007.

Internet: <http://www.bmbf.de/pub/ikt2020.pdf> [22.04.08]

[BMWi2006] Bundesministerium für Wirtschaft und Technologie (Hrsg.): *iD 2010 : Informationsgesellschaft Deutschland 2010. Aktionsprogramm der Bundesregierung*. Berlin: BMWi, 2006. Internet:

http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/id2010_E2_80_93informationsgesellschaft-deutschland-2010.property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf
[22.04.08]

[Broschard2001]

Broschard, Monica: *Fachinformationspolitik in der Bundesrepublik Deutschland*, Bachelor-Arbeit, Hagen, 2001.

Internet: <ftp://ftp.zew.de/mbr/polba-fip2001.pdf> [22.04.08]

[DNB2006]

Bundesministerium der Justiz (Hrsg.): *Gesetz über die Deutsche Nationalbibliothek vom 22. Juni 2006 (BGBl. I S. 1338)*.

Internet: <http://www.gesetze-im-internet.de/dnbg/> [22.04.08]

[EMRK]

Kanzlei des Europäischen Gerichtshofs für Menschenrechte (Hrsg.): *Konvention zum Schutze der Menschenrechte und Grundfreiheiten in der Fassung des Protokolls Nr. 11 samt Zusatzprotokoll und Protokolle Nr. 4, 6, 7, 12 und 13 Auswahl von Vorbehalten und Erklärungen*. Offizielle deutsche Übersetzung, Straßburg, 2003. Internet:

<http://www.echr.coe.int/NR/rdonlyres/F45A65CD-38BE-4FF7-8284-EE6C2BE36FB7/0/German.pdf> [22.04.08]

[Gräbe01]

Gräbe, Hans-Gert, Benutzereintrag im DorfWiki / Online-Community.

Internet: <http://www.dorfwiki.org/wiki.cgi?HansGertGraebe> [22.04.08]

[Gräbe2005]

Gräbe, Hans-Gert: *Die Macht des Wissens in der modernen Gesellschaft*. In: UTOPIE kreativ, Juli/August 2005, 177/178, S. 629-643. Internet:

http://www.rosalux.de/cms/fileadmin/rls_uploads/pdfs/177_78Graebe.pdf [22.04.08]

[Gräbe2005Okt]

Gräbe, Hans-Gert: *Neoliberalismus, Wissenschaft und Gemeineigentum*. In: Der Dezenten-Dissens. Die deutsche Hochschul-Reform-Kontroverse als Verlaufsform. Berlin: Trafo Verlag, 2006, S. 297-313.

Internet: <http://www.hg-graebe.de/EigeneTexte/wisos-05.pdf> [22.04.08]

[Haller2007]

Haller, Klaus: *Digitalisierung und Erschließung der im deutschen Sprachraum erschienenen Drucke des 18. Jahrhunderts*. Halle (Saale): Universitäts- und Landesbibliothek Sachsen-Anhalt, 2007.

[HavemannKaufmann2006]

Havemann, Frank / Kaufmann, Andrea: *Der Wandel des Benutzerverhaltens in Zeiten des Internet - Ergebnisse von Befragungen an 13 Bibliotheken*. In: Hauke, Petra / Umlauf, Konrad (Hrsg.): *Vom Wandel der Wissensorganisation im Informationszeitalter - Festschrift für Walther Umstätter zum 65. Geburtstag*. Berlin: Humboldt-Universität zu Berlin, 2006.

Internet: <http://nbn-resolving.de/urn:nbn:de:kobv:11-10069459> [22.04.08]

[Kuhlen2008]

Kuhlen, Rainer: *Erfolgreiches Scheitern - eine Götterdämmerung des Urheberrechts?* 1. Aufl., Boizenburg: Hülsbusch, 2008. Internet:

http://www.inf-wiss.uni-konstanz.de/RK2008_ONLINE/ [22.04.08]

[SchmiedchenSpennemann2007]

Schmiedchen, Frank / Spennemann, Christoph: *Nutzen und Grenzen geistiger Eigentumsrechte in einer globalisierten Wissensgesellschaft. Das Beispiel öffentliche Gesundheit*. VDW-Materialien 1/2007. Internet:

<http://www.vdw-ev.de/publikationen/VDW-Materialien%201-2007.pdf> [22.04.08]

[UrhG]

Bundesministerium der Justiz (Hrsg.): *Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), zuletzt geändert durch Artikel 12 Abs. 4 des Gesetzes vom 13. Dezember 2007 (BGBl. I S. 2897)*.

Internet: <http://www.gesetze-im-internet.de/urhg/> [22.04.08]

[ZML2004]

Zentrum für Multimedia in der Lehre (Hrsg.): *Abschlussbericht zum Vorhaben mobile-Campus Universität Bremen: Entwicklung, Erprobung und Einführung einer innovativen und integrativen mobile-learning Gesamtkonzeption in den Regelbetrieb der Universität*.

Bremen: Universität Bremen, 2004. Internet: <http://www.mobilecampus.uni-bremen.de/downloads/BMBF08NM236.pdf> [22.04.08]

Kapitel 2 - Rechtliche Rahmenbedingungen

[BDSG]

Bundesministerium der Justiz (Hrsg.): *Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970)*.

Internet: http://www.gesetze-im-internet.de/bdsg_1990/ [05.05.08]

[Beger2000]

Beger, Gabriele: *Benutzungsordnungen für Internet-Plätze*. In: Bibliotheksdienst, Bd. 34.2000, 9, S. 1499-1505. Internet:

http://bibliotheksdienst.zlb.de/2000/2000_09_Recht01.pdf [22.04.08]

[Beger2006]

Beger, Gabriele: *Urheberrecht für Bibliothekare : Eine Handreichung von A-Z*. 1. Aufl., München u. a.: Verlag Medien und Recht, 2006.

[Bizer2007]

Bizer, Johann: *Vorratsdatenspeicherung: Ein fundamentaler Verfassungsverstoß*. In: Datenschutz und Datensicherheit. 31.2007, 8, S. 586-589. Internet:

<http://www.springerlink.com/content/1p365222581x2855/fulltext.pdf> [03.06.2008]

[BR63105]

Bundesrat (Hrsg.): *Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation - Telekommunikations-Überwachungsverordnung - TKÜV*. Bundesrats-Dr. 631/05 vom 12.08.05. Internet:

http://www.bundesrat.de/cln_051/nn_8336/SharedDocs/Drucksachen/2005/0601-700/631-1-05_templateId=raw_property=publicationFile.pdf/631-1-05.pdf [22.04.08]

[BTP16124]

Deutscher Bundestag (Hrsg.): *Stenografischer Bericht : 124. Sitzung. Berlin, Freitag, den 9. November 2007*.

Internet: <http://dip.bundestag.de/btp/16/16124.pdf> [22.04.08]

[BVerfG25608]

Bundesverfassungsgericht: *BVerfG, 1 BvR 256/08 vom 11.3.2008, Absatz-Nr. (1 - 188)*.

Internet:

http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html [22.04.08]

[DFN2006]

DFN-Verein: *Entwurf einer Musterbenutzungsordnung für Hochschulrechenzentren und sonstige wissenschaftliche Forschungseinrichtungen im Deutschen Forschungsnetz*. 2006.

Internet: <http://www.dfn.de/fileadmin/3Beratung/Recht/Mubenord092006.pdf> [05.05.08]

[DBV2006]

Stellungnahme der DBV-Rechtskommission *Internetarbeitsplätze in der Bibliothek: Verpflichtung zur Errichtung von Überwachungseinrichtungen nach § 110 Telekommunikationsgesetz (TKG)?* In: Bibliotheksdienst, Bd. 40.2006, 8-9, S. 1040-1049. Internet:

<http://www.bibliotheksverband.de/ko-recht/dokumente/BD08-09061.pdf> [22.04.08]

[DFNBIB2006]

DFN-Verein und Vertreter der bayrischen wissenschaftlichen Bibliotheken: *Ergebnisse der Sitzung vom 21.10.2006 zum Thema § 110 TKG*. Sitzungsprotokoll, Würzburg, 2006.

[Dierking2005]

Dierking, Laura: *Zählen, speichern, spionieren. Datenschutz und seine Bedeutung im Rahmen technischer Entwicklungen*. Präsentation der Forschungsstelle Recht im DFN, 2005. Internet:

http://www.dfn.de/fileadmin/3Beratung/Recht/vortraege/Vortrag_Recht_2005-11-23.pdf

[22.04.08]

[Engasser2005]

Engasser, G.: *Strukturen und rechtliche Grundlagen des Jugendmedienschutzes*. Präsentation des Sozialministeriums Baden-Württemberg, 2005. Internet:

http://www.ajs-bw.de/media/files/download/forum3_strukturenjugendmedienschutz.pdf

[22.04.08]

[G10]

Bundesministerium der Justiz (Hrsg.): *Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), zuletzt geändert durch Artikel 5 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198)*.

Internet: http://www.gesetze-im-internet.de/g10_2001/ [22.04.08]

[GG]

Deutscher Bundestag (Hrsg.): *Grundgesetz für die Bundesrepublik Deutschland. Textausgabe - Stand Januar 2007*. Internet:

http://www.bundestag.de/parlament/funktion/gesetze/gg_jan2007.pdf [22.04.08]

[GünterSchindler2006]

Günter, Thomas / Schindler, Friedemann: *Technische Möglichkeiten des Jugendschutzes im Internet*. In: *Recht der Jugend und des Bildungswesens (RdJB)*, 2006, Heft 3, S. 341 ff.

Internet: http://www.jugendschutz.net/pdf/Aufsatz_RdJB3_06.pdf [22.04.08]

[Haupt2006]

Haupt, Stefan (Hrsg.): *Urheberrecht von A - Z: Einführung in das Urheberrecht anhand der wichtigsten Begriffe von A - Z*. 1. Aufl., München u. a.: Verlag Medien und Recht, 2006.

[Hoeren2008]

Hoeren, Thomas: *Internetrecht*. Stand März 2008. Internet: http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Maerz2008.pdf [22.04.08]

[HRG]

Bundesministerium der Justiz (Hrsg.): *Hochschulrahmengesetz in der Fassung der Bekanntmachung vom 19. Januar 1999 (BGBl. I S. 18), zuletzt geändert durch Artikel 2 des Gesetzes vom 12. April 2007 (BGBl. I S. 506).*

Internet: <http://www.gesetze-im-internet.de/hrg/> [05.05.08]

[JuSchG]

Bundesministeriums für Familie, Senioren, Frauen und Jugend (Hrsg.): *Jugendschutzgesetz (JuSchG) vom 23. Juli 2002 (BGBl. I S. 2730, 2003 I S. 476), geändert durch Artikel 7 Abs. 2 des Gesetzes vom 27. Dezember 2003 (BGBl. I S. 3007), geändert durch Artikel 3 des Gesetzes vom 29. Dezember 2003 (BGBl. I S. 3076), geändert durch Artikel 2 des Gesetzes vom 23. Juli 2004 (BGBl. I S. 1857, 2600), geändert durch Artikel 2 des Gesetzes vom 27. Februar 2007 (BGBl. I S. 179, 251), geändert durch Artikel 3 des Gesetzes vom 20. Juli 2007 (BGBl. I S. 1595).*

Internet: http://www.bmfsfj.de/bmfsfj/generator/RedaktionBMFSFJ/Abteilung5/Pdf-Anlagen/jugendschutzgesetzflie_C3_9Ftext-01-09-07.property=pdf.bereich=,sprache=de.rwb=true.pdf [22.04.08]

[JuSchG_JMStV]

Bundesministeriums für Familie, Senioren, Frauen und Jugend (Hrsg.): *Jugendschutzgesetz und Jugendmedienschutz-Staatsvertrag der Länder.* Stand: August 2008. Internet:

<http://www.bmfsfj.de/bmfsfj/generator/RedaktionBMFSFJ/Broschuerenstelle/Pdf-Anlagen/Jugendschutzgesetz-Jugendmedienschutz-Staatsvertrag.property=pdf.bereich=,rwb=true.pdf> [20.10.08]

[Kirchner1991]

Kirchner, Hildebert: *Grundriß des Bibliotheks- und Dokumentationsrechts.* Frankfurt am Main: Klostermann, 1991.

[Köcher2006]

Köcher, Jan K.: *Speicherfristen von Verkehrsdaten in Hochschulen.* Präsentation der Forschungsstelle Recht im DFN auf der 26. Tagung der Datenschutzbeauftragten Niedersächsischer Hochschulen, 16. Februar 2006. Internet:

<http://www.dfn.de/fileadmin/3Beratung/Recht/vortraege/DSBNdsTagung26koe.pdf>
[22.04.08]

[LDSGMV]

Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz - DSG M-V) vom 28. März 2002 (GVOBl. M-V S. 154), zuletzt geändert am 25. Oktober 2005 (GVOBl. M-V S. 535).

Internet: http://www.informationsfreiheit-mv.de/dschutz/ges_ver/guv/guv_c_20.html
[05.05.08]

[LHGMV]

Gesetz über die Hochschulen des Landes Mecklenburg-Vorpommern
(Landeshochschulgesetz - LHG M-V) vom 5. Juli 2002 (GVOBl. M-V 2002, S. 398).
Internet: http://mv.juris.de/mv/HSchulG_MV_2002_rahmen.htm [05.05.08]

[LieschingGünter2000]

Liesching, Marc / Günter, Thomas: *Verantwortlichkeit von Internet-Café-Betreibern - Besonderheiten bei pornografischen oder sonstigen jugendgefährdenden Inhalten*. In: *Multi-media und Recht*, 2000, Heft 5, S. 260 ff.
Internet: <http://www.webmania.li/downloads/pdf/haftung.pdf> [05.05.08]

[OLJB2005]

Arbeitsgemeinschaft der Obersten Landesjugendbehörden (AGOLJB): *Rechtsauffassung der Obersten Landesjugendbehörden (OLJB) zur jugendschutzrechtlichen Einordnung von Computerräumen mit und ohne Internetzugang in Jugendeinrichtungen oder Schulen, sowie zur Veranstaltung sog. LAN-Parties durch Schulen bzw. Einrichtungen im nicht gewerblichen Bereich*. In: *BPJM-Aktuell* 2/2005. Internet:
<http://www.bundespruefstelle.de/bmfsfj/generator/bpjm/redaktion/PDF-Anlagen/bpjm-aktuell-lan-parties-rechtsauffassung-der-oljb-aus-02-05.property=pdf,bereich=bpjm,sprache=de,rwb=true.pdf> [22.04.08]

[RsC30106]

Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften (Hrsg.): *Klage, eingereicht am 6. Juli 2006 - Irland/Rat der Europäischen Union, Europäisches Parlament. (Rechtssache C-301/06)*. In: *ABI. C. 237* vom 30.09.2006, S.5.
Internet: [http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=DE&Submit=Rechercher\\$docrequire=alldocs&numaff=C-301/06](http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=DE&Submit=Rechercher$docrequire=alldocs&numaff=C-301/06)
[03.06.08]

[SBB2006]

Staatsbibliothek zu Berlin - Preußischer Kulturbesitz: *Benutzungsordnung Gebührenordnung vom 4. Dezember 2006 mit Wirkung vom 2. Januar 2007*.
Internet: http://staatsbibliothek-berlin.de/deutsch/abteilungen/benutzungsabteilung/Benutzungs_Gebuehrenordnung.pdf
[22.04.08]

[Schaar2007]

Schaar, Peter (Bundesbeauftragter für Datenschutz und Informationsfreiheit): *Antwort an den Arbeitskreis Vorratsdatenspeicherung zur kurzfristigen Speicherung von Verkehrsdaten*. 20. März 2007. Internet:
http://www.bfdi.bund.de/cln_007/nn_530308/DE/Themen/KommunikationsdiensteMedien/Telekommunikation/Artikel/VorratsdatenspeicherungLGDarmstadt.html [22.04.08]

[Schindler2000]

Schindler, Friedemann: *Rating und Filtering. Zukunftstechnologien im Jugendschutz?!?* In: Freiwillige Selbstkontrolle Fernsehen: tv-diskurs, Januar 2000, Heft 11. Internet: <http://www.lpm.uni-sb.de/jugendschutz/rating-tvdiskurs.html> [22.04.08]

[StPO]

Bundesministerium der Justiz (Hrsg.): *Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 78 Abs. 6 des Gesetzes vom 23. November 2007 (BGBl. I S. 2614 mWv 30.11.2007).* Internet: <http://bundesrecht.juris.de/stpo/> [22.04.08]

[SUUB2000]

Staats- und Universitätsbibliothek Bremen: *Benutzungsordnung vom 16. September 1998 zuletzt geändert durch Änderungsordnung vom 17.02.2000.* <http://www.suub.uni-bremen.de/benutzung/ordnung/benutzung.pdf> [22.04.08]

[TKG]

Bundesministerium der Justiz (Hrsg.): *Telekommunikationsgesetz vom 22. Juni 2004, (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198).* Internet: http://www.gesetze-im-internet.de/tkg_2004/ [22.04.08]

[TKÜ2007]

Bundesministerium der Justiz (Hrsg.): *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EGl.* Gesetzentwurf der Bundesregierung, verabschiedet durch den Deutschen Bundestag in seiner 124. Sitzung am 9. November 2007. Internet: <http://www.bmj.bund.de/files/-/2047/> [22.04.08]

[TKÜV]

Bundesministerium der Justiz (Hrsg.): *Telekommunikations-Überwachungsverordnung vom 3. November 2005 (BGBl. I S. 3136), geändert durch Artikel 13 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198).* Internet: http://www.gesetze-im-internet.de/tk_v_2005/ [22.04.08]

[TMG]

Bundesministerium der Justiz (Hrsg.): *Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179).* Internet: <http://www.gesetze-im-internet.de/tmg/> [22.04.08]

[TRTKÜ]

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
(Hrsg.): *Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜ)*. Ausgabe 5.1, Februar 2008.

Internet: <http://www.bundesnetzagentur.de/media/archive/12804.pdf> [22.04.08]

[TVerleihV]

Bundesministerium für Post und Telekommunikation (Hrsg.): *Telekommunikations-Verleihungsverordnung (TVerleihV)*. 19.10.1995

[UNIRO1995]

Universität Rostock (Hrsg.): *Betriebsregelung und Benutzungsordnung für das Datenkommunikationsnetz der Universität Rostock RUN*. Amtliche Bekanntmachung der Universität Rostock, 1995. Internet: <http://www.uni-rostock.de/Rechenzentrum/URZ-Home/Netzordnung.shtml> [22.04.08]

Internet: <http://www.uni-rostock.de/Rechenzentrum/URZ-Home/Netzordnung.shtml> [22.04.08]

[UNIRO1999]

Universität Rostock (Hrsg.): *WWW-Ordnung für die Universität Rostock*. Amtliche Bekanntmachung der Universität Rostock, 1999. Internet: <http://www.uni-rostock.de/Rechenzentrum/URZ-Home/WWW-Ordnung.shtml> [22.04.08]

Internet: <http://www.uni-rostock.de/Rechenzentrum/URZ-Home/WWW-Ordnung.shtml> [22.04.08]

[UNIRO2008]

Universität Rostock (Hrsg.): *Benutzungsordnung für die Universitätsbibliothek Rostock*. Amtliche Bekanntmachung der Universität Rostock, 2008. Internet:

<http://www.uni-rostock.de/ub/xGeneral/content/BenutzungsordnungUB.pdf> [03.06.08]

Kapitel 3 – Umsetzung am Beispiel der UB Rostock

[DSTOOLS]

Microsoft Corporation: *Verzeichnisdienst-Befehlszeilenprogramme*.

Aktualisiert: Januar 2005. Internet:

<http://technet2.microsoft.com/windowsserver/de/library/714070bb-22a5-420b-ac0f-2f7c558f82fa1031.msp?mfr=true> [15.05.08]

[JOEWARE]

Richards, Joe: *joeware.net free tools*.

Internet: <http://www.joeware.net/freetools/> [05.05.08]

[KIXTART]

Internet: <http://www.kixtart.org/> [05.05.08]

[SQUID]

Internet: <http://www.squid-cache.org/> [05.05.08]

[W2K3AD2006]

Microsoft Corporation: *Windows Server 2003 Active Directory-Betriebshandbuch*.

Aktualisiert: Juli 2006. Internet:

<http://www.microsoft.com/germany/technet/prodtechnol/windowsserver/technologies/featurered/ad/active-directory-betriebshandbuch-00.msp> [15.05.08]

Kapitel 4 – Alternativen und weitere Entwicklung

[Borel2007]

Borel, Franck: *Einführung in Shibboleth*. 5. Shibboleth-Workshop der AAR in Kooperation mit der DFN-AAI. Berlin, 2007. Internet:

<https://www.aai.dfn.de/fileadmin/documents/WS5/shibboleth-einfuehrung-borel.pdf>
[05.05.08]

[DIRX]

Siemens AG: *DirX Identity V8.0. Identity Management for the Global Enterprise and Organization*. Internet:

http://www.medical.siemens.com/siemens/en_INT/gg_gs_FBAs/files/brochures/Data_Sheets/DirX_Identity_V8.0_en.pdf [05.05.08]

[HAN]

H+H Software GmbH: *Hidden Automatic Navigator. Geregelter Zugriff auf zentrale verwaltete eJournale und Onlinedatenbanken*. Internet:

<http://www.hh-software.com/hh2003/upload/showpdf.cfm?ID=96&LY=1> [15.05.08]

[Karolyi2002]

Karolyi, Christian: *Zugangskontrolle für Internet-PCs*. GBV Verbundkonferenz, Kiel, 2002.

<https://www.gbv.de/cls-download/fag-lokale-geschaeftsgaenge/workshops/kiel-2002/karolyi.pdf> [05.05.08]

[Rosifka2004]

Rosifka, Klaus: *Meta Directory Projekt CODEX. Integrierende Benutzer- und Ressourcenverwaltung an den Thüringer Hochschulen*. März 2004. Internet:

http://www.zdv.uni-mainz.de/ak-sys/2004/040303_AK-SYS_Bommerholz.pdf [05.05.08]

[Rosifka2007]

Rosifka, Klaus: *Projekt Meta Directory CODEX-PICA. IDM-Konnektor von OCLC PICA: Bindeglied zwischen dem Metadirectory der Hochschule und dem PICA-Lokalsystem*. November 2007. Internet:

http://www.suub.uni-bremen.de/verbundkonferenz/vor/meta_directory.ppt [05.05.08]

[Ruppert2007]

Ruppert, Ato: *Der Einsatz von Shibboleth als Single-SignOn-System in wissenschaftlichen Bibliotheken. Das Projekt Authentifizierung, Autorisierung und Rechteverwaltung (AAR)*. D-Grid Security Workshop, Göttingen, 27.3.2007. Internet:

http://www.medigrid.de/u_veranst/070327security-ws/v14_aar_20070327-goettingen.pdf [05.05.08]

[Steilen2007]

Steilen, Gerald: *DFG-Nationallizenzen: VHO und Shibboleth*. 5. Shibboleth-Workshop der AAR in Kooperation mit der DFN-AAI. Berlin, 2007. Internet:

<https://www.aai.dfn.de/fileadmin/documents/WS5/VZG.steilen.pdf> [05.05.08]

[Weinberger2006]

Weinberger, Norbert: *Anwendungsintegration an Hochschulen am Beispiel von Identity Management*. Sun Summit, Bonn, 26.4.2006. Internet:

<https://www.gbv.de/cls-download/fag-erschliessung-und-informationsvermittlung/arbeitsdokumente-fag-ei/Weinberger-norbert-Sisis-Pica.pdf> [22.05.08]

Anlage 1

DFN-Verein und Vertreter der bayrischen wissenschaftlichen Bibliotheken: *Ergebnisse der Sitzung vom 21.10.2006 zum Thema § 110 TKG*. Sitzungsprotokoll, Würzburg, 2006.

Ergebnisse der Sitzung vom 21.10.2006 zum Thema § 110 TKG

I. Ziel

In der Besprechung vom 21.10.2006 zwischen Vertretern des DFN-Vereins und Vertretern der bayrischen wissenschaftlichen Bibliotheken wird die Frage diskutiert, ob die Beteiligten Maßnahmen nach § 110 Telekommunikationsgesetz (TKG) treffen müssen, wenn die Bibliotheken ihren Benutzern einen Internetzugang zur Verfügung stellen. Es ist gemeinsamen Anliegen, zu klären, ob solche Pflichten bestehen bzw. ob und wie sie ggf. vermieden werden können.

II. Diskussion

Ausgangspunkt der Diskussion ist die rechtlich unstreitige Auslegung, dass keine Pflichten bestehen, soweit mit dem Bereitstellen eines Internetzugangs keine Telekommunikationsleitungen für die Öffentlichkeit erbracht werden, sondern – kurz gesagt – für eine geschlossene Benutzergruppe.

Im Bereich der **Hochschulen** ist davon auszugehen, dass die Hochschulangehörigen (Mitarbeiter, Studierende) eine geschlossene Benutzergruppe bilden. Das heißt, eine Nutzung der Internetzugänge in Hochschulbibliotheken durch Hochschulangehörige führt nicht zu Pflichten nach § 110 TKG. Als unschädlich dürften dabei auch eine private Nutzung des Internetzugangs und die Nutzung von hochschulnahen Einrichtungen z.B. im Rahmen von gemeinsamen Forschungsprojekten einzustufen sein. Ein Zugang für Alumni wäre wohl problematisch. Es sollte daher darauf verzichtet werden. Die Nutzung durch **sonstige Bibliotheksbenutzer**, die nicht Hochschulangehörige sind, stellt sich etwas differenzierter dar. Alleine eine – soweit bestehende – Pflicht zur Authentifizierung reicht nicht aus, eine geschlossene Benutzergruppe zu bilden. Es muss ein darüber hinausgehender gemeinsamer Zweck da sein. Der Auftrag der wissenschaftlichen Bibliotheken in Bayern erfordert es jedoch, auch diesen Nutzern den Internetzugang zu wissenschaftlichen Zwecken (vgl. § 2 Allgemeine Benützungsbedingungen der Bayrischen Staatlichen Bibliotheken (ABOB)) zur Verfügung zu stellen. Allerdings nur zu diesen Zwecken. In diesem Sinn handeln die Bibliotheken regelmäßig. Nur wer einen entsprechenden Zweck verfolgt, ist nach § 4 ABOB benützungsberechtigt. Dies wird im Rahmen der Zulassung zur Bibliotheksbenutzung geklärt. Liegt ein entsprechender Zweck vor, so wird die Zulassung zur

Nutzung erteilt. Damit in der Regel auch die Möglichkeit zur Internetnutzung zu diesem Zweck. Zumeist weisen auch die Internetnutzungsbedingungen nochmals darauf hin. Es ist daher davon auszugehen, dass auch die sonstigen Bibliotheksbenutzer den gemeinsamen Zweck der wissenschaftlichen Nutzung haben und daher mit den Hochschulangehörigen eine geschlossene Benutzergruppe bilden – wobei die sonstigen Bibliotheksbenutzer nur einen sehr geringen Anteil an der gesamten Gruppe haben. Für die Bayerische Staatsbibliothek und die Regionalen Staatlichen Bibliotheken lässt sich die Argumentation übertragen. Ihr[e] Benutzungsklientel ist durch ihre Aufgabenstellung zwar weiter als das der Hochschulen, doch für sie gilt ebenso die Fokussierung auf den wissenschaftlichen Zweck bei der Nutzung ihrer Angebote. Auch hier erfolgt die Zulassung zur Nutzung nach § 4 ABOB zu wissenschaftlichen Zwecken, so dass auch hier von einer geschlossenen Benutzergruppe gesprochen werden kann, die durch den wissenschaftlichen Zweck ihrer Arbeit definiert wird. Anzumerken ist auch hier, dass auch der Großteil der Nutzer zudem Hochschulangehörige sind.

Aus diesen Ergebnissen ergeben sich für die Beteiligten übereinstimmend folgende Lösungsansätze, die dazu dienen sollen, die vorhandenen geschlossenen Benutzergruppen deutlich und nachvollziehbar abzugrenzen, um Maßnahmen nach § 110 TKG zu vermeiden:

III. Lösungsansätze

1. Authentifizierung: Pflicht zur Authentifizierung der Internetnutzer.

Eine solche Pflicht ist – soweit noch nicht vorhanden – einzuführen, da nur so verhindert werden kann, dass jemand das Internet nutzt, der nicht der geschlossenen Benutzergruppe angehört. Zudem werden die Sicherheitsrisiken reduziert. Die Authentifizierung kann durch technische Zugangsmaßnahmen oder – bei wenigen Plätzen – einfach durch Ausweiskontrolle/Zweckangabe etc. geschehen.

2. Zulassung zur Internet-Nutzung: Voraussetzung für die Erteilung der Zugangsdaten zur Authentifizierung an nicht-hochschulangehörige Benutzer ist der wissenschaftliche Zweck der Nutzung. Dies wird bei der Zulassung geprüft. Nur dann kann eine Zulassung zur Internet-Nutzung erfolgen. Aus Nachweisgründen sollte eine schriftliche Erklärung verlangt werden, dass der Benutzer einen wissenschaftlichen Zweck verfolgt.

Die Beteiligten bevorzugen einvernehmlich diesen Lösungsansatz (1.+2.), der durch geringe Maßnahmen die geschlossene Benutzergruppe verdeutlicht und abgrenzt. Sollte diese Argumentation zu irgendeinem späteren Zeitpunkt angegriffen

werden, so gäbe es noch einen weiteren Lösungsansatz, der jedoch mit deutlich mehr Aufwand und Kosten verbunden wäre, und daher nur ersatzweise zum Zuge kommen sollte:

3. Unterschiedliche Provider für Externe und Hochschulangehörige: Für die nicht hochschulangehörigen Benutzer wird ein zweiter (privater) Provider herangezogen. Private Access-Provider halten in der Regel ohnehin schon Überwachungseinrichtungen im Sinne des § 110 TKG vor. Es müsste ein Konzept und eine technische Lösung erarbeitet werden, die es erlaubt, dass unterschiedliche Subnetze von verschiedenen Providern versorgt werden.

Sollte dieser Ansatz irgendwann zum Zug kommen müssen, so würde der DFN-Verein zur Konzeption und technischen Umsetzung den Bibliotheken Hilfestellung leisten. Zudem würde für Mitglieder des DFN-Vereins der kommerzielle Provider kostenneutral bereitgestellt werden können.

4. Abschließend ist noch darauf zu verweisen, dass die Beteiligten nicht nur aus grundsätzlichen Erwägungen eine Lösung bevorzugen, die mit wenig Aufwand verbunden ist, sondern auch im Hinblick auf die anstehende Umsetzung der **Richtlinie 2006/24/EG** „über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden“. Es ist zur Zeit noch nicht absehbar, welche Belastungen und Anforderungen damit einher gehen werden für den Wissenschaftsbereich und wie sich dies auf das TKG auswirken wird. Um den spezifischen Anliegen des Wissenschaftsbereichs Rechnung zu tragen, werden die Bibliotheken – gemeinsam mit der Rechtsstelle des DFN – auf die Umsetzung der Richtlinie zur Vorratsdatenspeicherung dahingehend versuchen einzuwirken, dass für Provider wissenschaftlicher Einrichtungen eine Bereichsausnahme von der Verpflichtung festgelegt wird.

Anlage 2

Antrag auf wissenschaftliche Nutzung des Datennetzes der Universität Rostock

Nutzernummer: 0028

Name:

Vorname: geb.:

PLZ: Wohnort:

Straße:

Erstantrag Folgeantrag

Hiermit beantrage ich für ein Jahr die **Nutzung des Datennetzes der Universität Rostock**
für **persönliche wissenschaftliche und nichtkommerzielle Zwecke**.

Begründung/Forschungsvorhaben*:

.....
.....
.....
.....
.....
.....
.....
.....

Ich erkenne die Regeln der Benutzungsordnung des Rechenzentrums
der Universität Rostock und die Benutzungsordnung der Universitätsbibliothek Rostock an.

Rostock, den Unterschrift:

Bearbeitungsvermerke UB:

Bearbeiter: Bibliothek:

Nutzergruppe 71

befürwortet Fachreferent:

Ablauf der Frist

Ablage Anmeldung BB1

*) Nähere Ausführungen etwa zum Zeitraum der Arbeiten, beteiligten Forschungs- oder Bildungseinrichtungen und der geplanten Abschlusspublikation können in einer Anlage zu diesem Antrag abgegeben werden.