Konrad-Zuse-Zentrum
für Informationstechnik Berlin

Takustraße 7
D-14195 Berlin-Dahlem
Germany

STEFAN LITSCHE

Zur Zugriffskontrolle im KOBV

Gefördert von der Senatsverwaltung für Wissenschaft, Forschung und Kultur des Landes Berlin, vom Ministerium für Wissenschaft, Forschung und Kultur des Landes Brandenburg und von den Mitgliedsbibliotheken des KOBV

ZIB-Report 02-53 (September 2002)

Zur Zugriffskontrolle im KOBV

Stefan Litsche
(litsche@zib.de)

25. September 2002

Zusammenfassung

Mit der Entwicklung des KOBV-Informationsportals soll den Benutzern in der Region Berlin-Brandenburg ein verbesserter Zugang zu Informationsressourcen geboten werden. Einen wesentlichen Anteil dieser Ressourcen bilden lizenzierte Daten, auf die bestimmte Nutzergruppen zugreifen dürfen. Für diese lizenzierten Materialien ist der Zugriff zu kontrollieren. Auf der Grundlage der Analyse der Rahmenbedingungen werden Anforderungen an die Zugriffskontrolle im KOBV definiert und Lösungsmöglichkeiten auf der Ebene allgemeiner Modelle diskutiert.

Inhaltsverzeichnis

1 Einleitung

Die Bibliotheken des KOBV stellen ihren Lesern verschiedene lizenzierte Dienste zur Verfügung. Für die Leser stellt sich als Problem, aus der Fülle der angebotenen Informationen die für sie passende zu finden. Der KOBV versteht es als seine Aufgabe [19], mit Hilfe eines Internet-Portals einen integrierten Zugang zu den Informationen zu schaffen, um damit den Leser bei der Recherche zu unterstützen. Da jedoch zur Zeit oftmals von den Anbietern der Zugriff auf das lizenzierte Material nur von Rechnern mit bestimmten IP-Adressen gewährt wird, sind die Leser in der Benutzung eingeschränkt. Diese Einschränkung aufzuheben, ist eine weitere Aufgabe des KOBV.

In verschiedenen Ländern wird die Informationsversorgung und die daraus resultierende erforderliche Zugriffskontrolle als eine Aufgabe verstanden, die landesweit gelöst werden muss (Großbritannien – JISC[1], Schweiz – SWITCH - AAI [10], Norwegen FEIDE-Project[2]). Im Rahmen der internationalen Organisation „Terena“[3] koordinieren die jeweils nationalen Initiativen ihre Anstrengungen und tauschen ihre Erfahrungen aus. Terena ist eine internationale Organisation, die selbst technische Entwicklungen ausführt und eine Plattform für Diskussionen bietet mit dem Ziel, eine hochwertige Computer Netzwerk Infrastruktur für die Europäischen Wissenschaften zu entwickeln

> „...to promote and participate in the development of a high quality international information and telecommunications infrastructure for the benefit of research and education.“ (TERENA Statutes).

In den verschiedenen Projekten und Initiativen wurde zur Lösung des Problems der landesweiten Zugriffskontrolle bereits viel diskutiert und es wurden verschiedene Überlegungen angestellt. Im Ergebnis dieser Arbeiten werden Anforderungen an die Zugriffskontrollsysteme formuliert, die auch für KOBV von Bedeutung sind. Dazu gehören u.a.: Zugang zu den Informationen unabhängig vom Aufenthaltsort, anonyme Benutzung durch die Leser, Authentifizierung in den lokalen Systemen, Management und Durchführung der Autorisierung bei den Anbietern.

In dieser Arbeit werden auf der Grundlage der bisherigen Erfahrungen im KOBV und anderer Initiativen Anforderungen an die Zugriffskontrolle im KOBV formuliert und ein Lösungsansatz vorgeschlagen.

2 Rahmenbedingungen und Begriffsbestimmungen

In den letzten Jahren hat die Bedeutung elektronischer Publikationen ständig zugenommen. Neben Zeitschriften, welche sowohl als gedruckte als auch als elektronische Version erscheinen, finden sich auch zunehmend Zeitschriften, welche ausschließlich in elektronischer Form angeboten werden.

Neben den Verlagen, die diese elektronischen Produkte publizieren, gibt es verschiedene Agenturen, die am Vertrieb dieser Zeitschriften beteiligt sind. Aufbauend auf den elektronischen Publikationen werden außerdem verschiedenste Dienstleistungen angeboten (Referenz-, Abstract-, Indexdatenbanken), die den Wissenschaftlern zusätzliche Möglichkeiten bei der Arbeit mit der Literatur bieten. Die Publikationen und die darauf aufbauenden Dienstleistungen, die von

[1] http://www.jisc.ac.uk/

[2] http://www.uninett.no/prosjekt/feide/index.en.html

[3] http://www.terena.nl/

Verlagen und den Herstellern der Informationssysteme (**die Anbieter**) vertrieben werden, sind das **lizenzierte Material**. Für den Vertrieb des lizenzierten Materials verwendet jeder Anbieter eigene Software.

Aus Lizenzverträgen, die zwischen Anbietern und Institutionen — den **Lizenznehmern** — geschlossen werden, ergibt sich die Verpflichtung, den Zugriff auf das lizensierte Material zu kontrollieren. Lizenznehmende **Institutionen** können Bildungs- und Forschungseinrichtungen wie Universitäten, Hochschulen, einzelne Fachbereiche innerhalb von Hochschulen, aber auch Bibliotheken sein.

Die Art der Nutzung und der Kreis der berechtigten Benutzer wird in Lizenzverträgen festgelegt. In den Lizenzverträgen setzt sich nach und nach durch, daß die Nutzung des lizenzierten Materials für autorisierte und Ortsbenutzer (*Walk-In Users*) erlaubt ist [2]. Neben vielen Informationsangeboten, die für alle Mitarbeiter einer Institution frei zugänglich sind, kann es auch Informationen geben, die nur für eingeschränkte Benutzergruppen (z.B. bestimmte Fachbereiche, definierte Anzahl gleichzeitiger Nutzer) zugänglich sind. Die Institution als Lizenznehmer ist für die Einhaltung der Lizenzbedingungen verantwortlich.

Autorisierte Benutzer sind die Angehörigen der lizenznehmenden Institution; dazu gehören die Mitarbeiter und die Studenten, die Zugriff auf das sichere Netzwerk (*secure network*) haben. Dazu müssen die Benutzer von der lizenznehmenden Institution ein Passwort oder eine andere Möglichkeit zur Authentisierung (**Identitätsnachweise**, *credentials*) erhalten.

Ortsbenutzer sind Personen, die keine autorisierten Benutzer sind, die jedoch Nutzer der Institution sind und (zumindest in den Gebäuden der lizenznehmenden Institution) die Möglichkeit haben, auf das sichere Netzwerk zuzugreifen.

Das **sichere Netzwerk** kann ein lokales Netz oder ein virtuelles Netz im Internet sein. Die lizenznehmende Institution kontrolliert den Zugang zu dem sicheren Netzwerk. Die Benutzer müssen sich dazu gegenüber der lizenznehmenden Institution authentisieren. Die Authentisierung sollte dem aktuellen Standard (*best current practice*) entsprechen.

Die Zugriffskontrolle umfasst das Authentisieren, das Autorisieren und das Auditing. **Authentisieren** ist der Vorgang, bei dem die Gültigkeit der Identitätsnachweise verifiziert wird. Die gängigste Form eines Identitätsnachweises ist eine Benutzerkennung in Verbindung mit einem Passwort. Daneben ist die Authentisierung mit Hilfe von Zertifikaten (x.509), Smartards, biometrischen Verfahren oder beliebige Kombinationen der genannten Nachweise möglich. In der Regel wird das Authentisieren von einem Programm durchgeführt. In einem Benutzerverzeichnis werden Informationen über die Benutzer und die zugehörigen Identitätsnachweise verwaltet. Das Programm kann das Vorhandensein der präsentierten Benutzerkennung und die *Kenntnis* des dazugehörigen Passwortes, den *Besitz* einer Chipkarte bzw. die Präsentation von Körpermerkmalen (Fingerabdruck) prüfen. Ziel einer Zugriffskontrolle kann es nicht sein, nicht-vertragskonformes Verhalten zu verhindern. Wohl aber soll Zugriffskontrolle so weit wie möglich den Mißbrauch verhindern. Im Falle eines Mißbrauchs muß dieser erkennbar sein und es muß festzustellen sein, wer dafür verantwortlich ist.

An einer Institution gibt es also (mindestens) eine Benutzerverwaltung. Eine Person kann jedoch verschiedenen Institutionen angehören. Daraus resultieren unterschiedliche Berechtigungen (Rollen) — ein Benutzer kann mehrere **digitale Identitäten** besitzen.

Vom Vorgang des Authentisierens ist (logisch) getrennt das **Autorisieren**. Durch das Autorisieren erhält der Benutzer das Recht, auf bestimmte Ressourcen zuzugreifen.

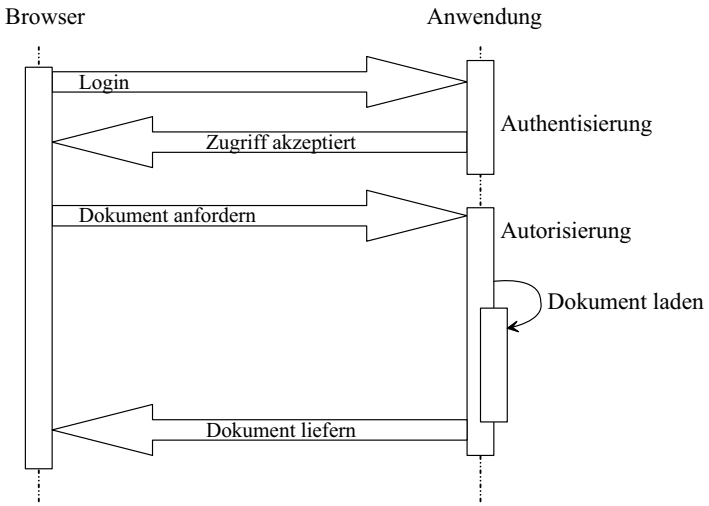

Abbildung 1: Authentisierung und Autorisierung in einer Anwendung.

In Abbildung 1 symbolisiert der erste Block in derjenigen Anwendung, die den Zugriff auf das lizenzierte Material realisiert, den Prozess der Authentisierung. Mit dem Login sendet der Benutzer seinen Identitätsnachweis, der von der Anwendung gegen die *eigenen* Benutzerdaten geprüft wird. Basiert die Authentisierung auf der Kontrolle der IP-Adresse des Rechners, dann erfordert dies keine Interaktion mit dem Benutzer (symbolisiert durch die Pfeile). Dabei wird auch nicht der Benutzer authentisiert, sondern der Rechner. Die lizenznehmende Institution ist in diesem Fall dafür verantwortlich, daß der Rechner nicht von Unberechtigten benutzt wird.

Wenn ein Benutzer dann ein Dokument anfordert, wird in der Anwendung ein neuer Prozess gestartet, der prüft, ob der Benutzer das Recht besitzt, die angeforderte Aktion (z.B. Lesen) mit einer bestimmten Ressource (z.B. ein Pdf-Dokument, das einen bestimmten Artikel enthält) auszuführen. Fällt die Prüfung positiv aus, wird das angeforderte Dokument ausgeliefert.

Auditing ist der Prozess, durch den die Zugriffe protokolliert werden, um die Kontrolle der Nutzung durch einen Menschen zu ermöglichen und dadurch Mißbrauch von Ressourcen aufzudecken. Die protokollierten Daten können in unterschiedlichem Grade Informationen über den Benutzer enthalten. *Anonyme* Daten sind praktisch keinem Benutzer zuzuordnen. *Pseudonyme* Daten sind praktisch keinem Benutzer zuzuordnen, solange die Zuordnungsregel nicht bekannt ist. Durch diese *Zuordnungsregel* wird bestimmt, welches Kennzeichen oder Pseudonym zu welchem Benutzer gehört. Die Zuordnungsregel kann allein dem Benutzer (Selbstregistrierung) oder einem Dritten bekannt sein. Das ist zum Beispiel dann der Fall, wenn Leser in einer Bibliothek eine aus Zahlen bestehende Benutzerkennung erhalten.

Über die lizenzierten Angebote hinaus bieten die Institutionen selbst Dienste an, für die sich der Benutzer authentisieren muß. Das kann die Bestellung von Büchern oder die Fernleihe sein. Dann tritt die Institution selbst als Anbieter auf.

Der Anbieter gewährt den Zugriff auf seine Angebote; er entscheidet, ob einem bestimmten Benutzer die Zugriffsrechte gewährt werden. Die Kontrolle des Zugriffs kann durch die Kontrolle der IP-Adresse, auf der Basis von Kennung und Passwort oder auf der Grundlage der Kenntnis der Zugehörigkeit des Benutzers zu einer Institution erfolgen.

Der Anbieter bietet seine Dienste über das Internet an. Auf der Grundlage des Internet Protokolls (IP) werden für Anwendungen weitere Protokolle definiert, die die Kommunikation zwischen Client und Server regeln. Für das Auffinden und Vertreiben des lizenzierten Materials spielen hauptsächlich diejenigen Dienste eine Rolle, welche über HTTP (das „Web“) transportiert werden. Andere mögliche Protokolle (z.B. Z39.50 oder Telnet) werden hier nicht betrachtet, da diese für den Informationszugriff durch Benutzer von untergeordneter Bedeutung sind und zudem die Informationsportale ihre Dienste über HTTP anbieten.

Die Dienste können von Servern angeboten werden, welche innerhalb des lokalen Netzwerks (LAN, **Intranet**) des Campus respektive der Bibliotheken stehen. Dieses lokale Netzwerk ist die **Heimatdomäne** (*origin domain*) des Benutzers. Einer der Dienste, der in der Heimatdomäne angeboten wird, ist der Authentisierungsdienst. Daneben werden von Anbietern auch Dienste auf Servern angeboten, die nicht im Intranet stehen. Auf diese Dienste wird über das Internet zugegriffen.

Der Benutzer kann im Web navigieren, indem er Links folgt. Diese Links, die auf die **Zieldomäne** (*target domain*) verweisen, können im einfachsten Fall von einer Linkliste oder auch von einem Portal angeboten werden. In diesem Fall würde der Link von der Heimatdomäne auf die Zieldomäne verweisen. Jedoch ist ein Portal nicht der einzige Startpunkt einer Recherche für einen Benutzer; abgesehen davon, daß verschiedene Bibliotheken im KOBV eigene Portale anbieten werden, so kann der Benutzer seine Recherche auch direkt in der Zieldomäne starten. Darüber hinaus werden von verschiedenen Anbietern innerhalb der Publikationen auch sogenannte Referenzlinks angeboten. Diese Links zeigen dann von einer Zieldomäne auf eine andere.

3 Anforderungen an die Zugriffskontrolle im KOBV

Nach dem im ersten Abschnitt die rechtlichen und technischen Rahmenbedingungen skizziert wurden, sollen nun im folgenden die Anforderungen an die Zugriffskontrolle im KOBV beschrieben werden. Diese Anforderungen ergeben sich einerseits aus den geschilderten Rahmenbedingungen, andererseits beschreiben die Anforderungen Ziele, die von den Bibliotheken im KOBV definiert werden.

Zur Zeit existieren verschiedene technische Systeme, mit denen sich eine Zugriffskontrolle auf Webdienste realisieren ließe [14, 21]. Jedoch müssen bei der Auswahl des Systems verschiedene organisatorische, administrative, juristische und sicherheitstechnische Bedingungen und Anforderungen berücksichtigt werden, welche die Auswahl des Systems einschränken.

Indem die Anforderungen an das System definiert werden, wird ein Zielzustand beschrieben, an welchen sich die konkreten Umsetzungen nach und nach annähern soll. Bei der konkreten Implementierung der Zugriffskontrolle für das lizenzierte Material eines bestimmten Anbieters spielen die Möglichkeiten des betreffenden Anbieters eine große Rolle.

Die Zugriffskontrolle muß den Anforderungen aller Parteien, die an dem Prozess der Zugriffskontrolle beteiligt sind — das sind die lizenznehmenden Institutionen, die Anbieter und die Benutzer —, gerecht werden. Darum muß für die Zugriffskontrolle eine Lösung gefunden werden, welche die externen Anbieter mit einbezieht. Dabei muß man sich bewußt sein, daß nicht alle Anforderungen von Anbeginn realisiert werden können, da die Realisierung von verschiedenen Parteien mitgetragen werden muß. Das Definieren eines Zielzustandes gibt jedoch eine Richtlinie an die Hand, die bei einer aktuellen Entscheidung für eine

bestimmte Implementierung berücksichtigt werden kann.

3.1 Sicht der Benutzer

Auf der Grundlage der heute zur Verfügung stehenden Erfahrungen mit den auf der Kontrolle der IP-Adresse basierenden Verfahren der Zugriffskontrolle ist es eine wesentliche Forderung, daß der Benutzer bei der Nutzung des lizenzierten Materials nicht an einen bestimmten Rechner oder ein bestimmtes Netzwerk gebunden ist.

> **Leitsatz 1** *Der Benutzer ist frei in der Wahl seines Arbeitsplatzes.*

Aus der Sicht des Benutzers sind Webdienste, welche aus dem Internet und aus dem Intranet angeboten werden, schwer zu unterscheiden. Für ihn gibt es auch keinen zwingenden Grund für eine solche Unterscheidung. Die Bestrebungen, dem Benutzer die vorhandenen Dienste über integrierte Umgebungen (KOBV-Informationsportal, lokale Portale) anzubieten, verstärken diese einheitliche Sicht auf die angebotenen Informationen. Dabei darf es für den Benutzer keine Rolle spielen, wie er zu diesem lizenzierten Material gelangt — ob über Links, die von der Heimatdomäne oder von den Zieldomänen selbst angeboten werden.

Ein Portal ist nur ein Einstiegspunkt neben vielen anderen. Nachdem ein Leser seinen Einstieg über ein Portal gefunden hat, benutzt er die zur Verfügung stehenden Ressourcen, indem er Referenzlinks folgt oder in den Recherchesystemen der Anbieter selbst recherchiert. Open-Linking-Systeme (z.B. SFX) bieten weitere Links an, die dynamisch generiert werden und die auch direkt auf einzelne Dokumente beim Anbieter verweisen können.

Darum muß die Zugriffskontrolle es ermöglichen, daß Links auf einzelne Dokumente in der Zieldomäne am Recherchesystem des Anbieters vorbei möglich werden. Dazu muß jeder beteiligte Partner separat den angemessenen Zugriff gewähren. Für den Benutzer muß die Zugriffskontrolle transparent und unaufdringlich sein — sie darf den Leser in der Art der Benutzung nicht beeinflussen oder beeinträchtigen. Er kann seine Recherche in einem der Portale, die von den Bibliotheken im KOBV angeboten werden, starten oder seine Suche mit Hilfe des Recherche-Werkzeugs eines Anbieter durchführen. Darum darf die angestrebte Lösung nicht nur für ein Informations-Portal funktionieren. Die Zugriffe auf das lizenzierte Material muß über Links, die vom Portal angeboten werden, ebenso möglich sein wie Zugriffe von anderen Quellen aus.

> **Leitsatz 2** *Der Benutzer ist frei in der Art und Weise des Zugriffs auf das lizenzierte Material.*

Mehrfaches Anmelden bei verschiedenen Anbietern, auf die über das Portal zugegriffen wird, ist für den Benutzer nicht nachvollziehbar. Das zeigen auch die Erfahrungen mit dem System „Athens“ in Großbritannien [26].

> **Leitsatz 3** *Der Benutzer authentisiert sich nur* einmal *gegenüber [genau] einer Anwendung.*

Alle anderen Dienste dürfen keine weitere Authentisierung vom Benutzer erfordern; damit wird auch ein sicherer Umgang mit dem Paßwort gewährleistet[4].

[4] Die Sicherheitsrichtlinie kann dann die Maßgabe enthalten, daß Paßwort nur einem bestimmten Authentisierungsserver über SSL zu übermitteln, damit das Risiko gemindert wird, das Paßwort an unsichere Server weiterzugeben.

Die anonyme Benutzung der Dienste ist ein Wunsch, der nicht nur die Akzeptanz des Dienstes durch die Benutzer fördert. Da viele Forschungsprojekte von interessierter Seite gefördert werden und auch schnell in ein marktfähiges Produkt überführt werden sollen, ist der vertrauliche Umgang mit persönlichen Daten der Benutzer bei der Informationsversorgung auch ein ökonomisches Erfordernis:

> „To the extent that researchers are pursuing patents, developing grant applications in a competitive environment, or seeking precedence for discoveries, confidential access to information resources is a critical issue with potentially significant economic consequences.“ [21].

Daraus folgt, daß es nicht möglich sein sollte, die Identität des Benutzers aus den Informationen, welche für die Zugriffskontrolle übermittelt werden, zu bestimmen. Die Benutzung muß also anonym oder zumindest pseudonym erfolgen.

Daneben muß das System zur Zugriffskontrolle jedoch auch die Nutzung personalisierter Dienste ermöglichen, da gerade diese in einem Portal von besonderem Wert für die Benutzer sind (z.B. Rechercheprofil, Benachrichtigungsdienst). Um personalisierte Dienste nutzen zu können, wird einem Benutzer ein eigenes Profil zugeordnet. Oftmals ist es für diese personalisierten Dienste (wie z.B. in der KOBV-Suchmaschine) nicht erforderlich, daß diese Profile einer realen Person zugeordnet werden. Jeder Leser kann sich ein oder mehrere Profile unter beliebigen Benutzerkennungen anlegen. Will er von den Ergebnissen einer Recherche ausgehend auf die lizenzierten Inhalte (z.B. Volltext des Dokuments) zugreifen, so muß er sich gegenüber der Heimatdomäne mit dem von der Heimatdomäne *zugewiesenen* Identitätsnachweis authentisieren.

Wünschenswert ist es hier, die personalisierten Dienste eines Portals zu nutzen, ohne sich nochmals gegenüber dem Portal authentisieren zu müssen. Dazu muß der Authentisierungsdienst dem Portal Informationen übermitteln, welche es ermöglichen, einem Benutzer immer das gleiche Profil zuzuordnen. Gleichzeitig sollen diese identifizierenden Informationen nicht an Server übermittelt werden, welche keine personalisierten Dienste bieten bzw. deren personalisierte Dienste der Benutzer nicht nutzt (zum Datenschutz siehe auch Seite 9).

> **Leitsatz 4** *Die Privatsphäre des Benutzers wird während des Zugriffs gewahrt.*

Das erfordert vom System zur Zugriffskontrolle Methoden, die es erlauben, die Freigabe von persönlichen Informationen der Benutzer gegenüber den Zielsystemen sehr fein zu steuern.

3.2 Sicht der Institution

Die lizenznehmende Institution ist Vertragspartner der Anbieter. Damit ist jede Institution innerhalb des KOBV gegenüber den Anbietern dafür verantwortlich, die jeweiligen Lizenzbedingungen einzuhalten. Das Authentisieren ist Aufgabe der Heimatdomäne des Benutzers (das geht auch aus den Bestimmungen im „Modell Lizenzvertrag“ [2] hervor). Wie die Authentisierung durchgeführt wird, unterliegt der Entscheidung der betreffenden Institution. Das bedeutet auch, daß nicht notwendig verschiedene Stufen der Sicherheit (Kennung/Paßwort vs. Smartcards) für alle Benutzer unterstützt werden *müssen*. Die Institution *kann* jedoch für verschiedene Gruppen von Nutzern (Angestellte, administrative Mitarbeiter, Fellows, Emeriti...) unterschiedliche Methoden zur Authentisierung einsetzen, die sich qualitativ hinsichtlich der Sicherheit unterscheiden.

> **Leitsatz 5** *Die Wahl des Systems zur Authentisierung liegt in der Verantwortung der jeweiligen Institution.*

Wie auch bei den Bibliothekssystemen, so werden auch für die Authentisierung sehr unterschiedliche Systeme eingesetzt werden. Darum muß das zu wählende System zur Zugriffskontrolle mit einer großen Vielzahl an lokalen Systemen zusammenarbeiten können.

Ein Grundprinzip des KOBV ist Heterogenität.

> „Die Bibliotheken sollen sich auch künftig für das System entscheiden können, das ihren lokalen Bedürfnissen in bezug auf Funktionalität, Leistungsumfang und finanziellen Rahmen am besten gerecht wird. Das heterogene Konzept erlaubt auf der organisatorischen Ebene die Einbindung von Bibliotheken unterschiedlicher Sparten in den KOBV.“ [18].

Dieses Prinzip muß auch auf die Zugriffsverwaltung im KOBV angewendet werden. Das bedeutet, daß die Wahl einer Methode zur Authentisierung eine souveräne Entscheidung der jeweiligen Institution ist. Darum muß das einzusetzende System in der Lage sein, verschiedenste technische Lösungen (Kennung und Passwort, X.509 Zertifikate, auf Smartcards gespeicherte Zertifikate, biometrische Verfahren) zur Authentisierung zu unterstützen. Das System zur Zugriffsverwaltung muß auch dann funktionieren, wenn eine Institution den Mechanismus zur lokalen Authentisierung ändert.

Aus dem Prinzip der Heterogenität folgt weiterhin auch die Autonomie hinsichtlich der Entscheidung, welche Hard- und Software in den Institutionen für die Informationsversorgung eingesetzt werden. Damit die notwendige Kommunikation trotzdem möglich wird, müssen offene und möglichst standardisierte Protokolle und Verfahren eingesetzt werden (Offenheit als Prinzip des KOBV). Das bedeutet, daß auf der Seite der Arbeitsplatzrechner außer einer aktuellen Version eines Browsers keine zusätzliche Software notwendig ist. Daneben muß dieses System mit den gängigsten Webservern zu betreiben sein.

> **Leitsatz 6** *Das System zur verteilten Zugriffsverwaltung basiert auf offenen Protokollen.*

Vor allem die Universitäten und Hochschulen betreuen mehrere Tausend Angehörige. In jedem Semester kommen neue Angehörige hinzu, andere verlassen die Institution. Daraus ergibt sich ein erheblicher administrativer Aufwand, wodurch die Institutionen bestrebt sind, die dafür notwendigen Arbeitsgänge zu automatisieren.

Wenn in den Verträgen festgelegt ist, daß alle Angehörige der Institution die Ressource nutzen können, so gilt dies auch dann, wenn neue Angehörige hinzukommen oder ausscheiden. Somit bleiben die Regeln für die Autorisierung unberührt. Änderungen bei den Benutzerdaten sollen keine administrativen Maßnahmen auf der Seite erfordern, die die Autorisierung durchführt. Das ist auch deshalb notwendig, damit der Aufwand für die teilnehmenden Parteien nicht steigt — eine notwendige Bedingung für die Akzeptanz des Konzeptes. Außerdem müssen neue Knoten leicht in das Netz eingefügt werden können.

> **Leitsatz 7** *Die Zugriffsverwaltung muß mit möglichst geringem Aufwand zu administrieren sein.*

3.3 Sicht der Anbieter

Anbieter von lizenzpflichtigen Dienstleistungen haben ein Interesse daran, ihre Dienstleistungen vor unberechtigtem Zugriff zu schützen. Sie müssen eine Möglichkeit haben, die Einhaltung der Lizenzbedingungen zu kontrollieren.

> **Leitsatz 8** *Die Autorisierung ist ein lokale Entscheidung der Anbieter.*

Die Anbieter bieten die Informationen in einem Markt an. Sie brauchen Informationen über die Nutzung ihrer Dienstleistungen, um ihre Angebote wechselnder Nachfrage anpassen zu können. Das Sammeln dieser Informationen muß den geltenden datenschutzrechtlichen Bestimmungen genügen.

> **Leitsatz 9** *Die Anbieter dürfen in einem festzulegenden Maße statistische Informationen über Zugriffe sammeln.*

Während der Nutzung der Dienste der Anbieter soll die Privatsphäre des Benutzers gewahrt bleiben. Das bedeutet, aus den Informationen, die an den Anbieter übermittelt werden, darf die Identität des Benutzers nicht abgeleitet werden können. Um jedoch für den Anbieter nutzbringende Statistiken zu ermöglichen, müssen die Zugriffe verschiedener Benutzer zu unterscheiden sein.

> **Leitsatz 10** *Zugriffe von unterschiedlichen Benutzern sind unterscheidbar.*

3.4 Sicherheitsaspekte

Geschäfte erfordern Vertrauen. Besonders im e-business ist Sicherheit eine wesentliche Grundlage für das Vertrauen. Die beteiligten Partner sind unterschiedlichen Risiken ausgesetzt.

- Die Anbieter befürchten den Mißbrauch, der ihnen zum finanziellen Nachteil erwächst.
- Die lizenznehmende Institution befürchtet einen unsicheren Umgang mit den Identitätsnachweisen.
- Der Benutzer fürchtet, daß zu viele Daten über ihn gesammelt werden.

Die Zugriffskontrolle muß sicher sein, damit das Geschäft überhaupt realisierbar ist. Dabei muß die Lösung den Bedürfnissen aller Beteiligten gerecht werden. Sicherheit kann auf verschiedenen Ebenen der Qualität realisiert werden: authentisieren mit Kennung und Paßwort ist unsicherer als ein Verfahren, das zusätzlich noch den Besitz eines Schlüssels (Zertifikats) und einen Fingerabdruck prüft. Höhere Sicherheit beeinträchtigt auf der anderen Seite immer die Benutzbarkeit. Das notwendige Maß an Sicherheit (Aufwand) muß in angemessenem Verhältnis zu dem möglichen Schaden stehen, der verhindert werden soll (Nutzen).

Zugriffskontrolle, die auf Identitätsnachweisen basiert (*credential based access management*), birgt die Gefahr, daß über die Benutzer personenbezogene Daten (wer hat wann von wo auf welches Dokument zugegriffen) gesammelt werden. Allein für den (sich aus dem Vertrag ergebenden) Zweck der Abrechnung und Kontrolle der Einhaltung der Lizenzbedingungen aber sind personenbezogene Daten nicht notwendig.

Da die Anbieter oftmals ausländische Organisationen sind, kann sich der Nutzer einer Institution im KOBV nicht darauf verlassen, daß diese Anbieter ihre Datenverarbeitung nach deutschem Datenschutzrecht organisieren. Insgesamt werden die Informationssysteme immer komplexer, so daß es für den Nutzer immer undurchschaubarer wird, wer welche Informationen über ihn sammelt. Darum muß der Datenschutz zunehmend auch durch den Nutzer selbst als *Selbstdatenschutz* umgesetzt werden . Pseudonyme haben Eigenschaften, die unter den genannten Aspekten deren Anwendung als sinnvoll erscheinen lassen [27].

- Pseudonyme ermöglichen es, den Benutzer wiederzuerkennen. Das ermöglicht es Anwendungen (wie einem Portal), dem Benutzer personalisierte Dienste anzubieten. Dem Pseudonym können Informationen in einem Profil zugeordnet werden (z.B. eine Suchhistorie), was durchaus im Interesse des Nutzers sein kann.
- Mit Pseudonymen können bestimmte Berechtigungen verknüpft werden, die es z.B. dem Nutzer ermöglichen, auf lizenziertes Material zuzugreifen. Dabei muß der Nutzer seine Identität nicht preisgeben.
- Durch die Zuordnungsregel läßt sich ein Pseudonym auflösen. Wird ein Pseudonym, mit oder ohne Wissen des Nutzers, mißbraucht, so kann einerseits die Nutzung dieses Pseudonyms unterbunden werden, ohne andere Nutzer zu beeinträchtigen, andererseits läßt sich darüber der Nutzer zur Verantwortung ziehen.

Die Eigenschaft pseudonymer Daten, nicht personenbezogen zu sein, muß langfristig gesichert werden, denn wenn ein Pseudonym einmal aufgedeckt wird, dann sind mit einem Schlag *alle* bisher nicht personenbezogenen Daten zu diesem Pseudonym personenbezogen.

Das Risiko der Aufdeckung des Pseudonyms ergibt sich zum einen aus dem Bekanntwerden der Zuordnungsregel. Diese kann zufällig oder absichtlich bekannt werden. Zum anderen ergibt sich das Risiko der Aufdeckung daraus, daß das Pseudonym in verschiedenen Situationen verwendet wird (z.B. wenn ein Benutzer mit der gleichen Kennung in verschiedenen Bibliotheken recherchiert). Dadurch könnten Dritte an Informationen gelangen, die die Reidentifizierung pseudonymer Daten ohne Kenntnis der Zuordnungsregel ermöglichen.

Das erste Risiko zu mindern, liegt wesentlich in der Verantwortung der Institution, da sie diese Zuordnungsregel verwaltet. Das zweite Risiko zu mindern, liegt in der Verantwortung jedes einzelnen (Selbstdatenschutz).

Damit die Institution ihrer Verantwortung gerecht wird, werden Sicherheitsrichtlinien veröffentlicht, die Regeln für den Umgang mit den Identitätsnachweisen definieren. Für die Sicherheit in der Institution ist es wichtig, daß von den Benutzern diese Sicherheitsrichtlinien eingehalten werden. Ob und wie die Sicherheitsrichtlinien von den Benutzern umgesetzt werden, hängt auch wesentlich davon ab, wie praktikabel sie für den Benutzer sind. Oftmals muß ein Benutzer sich viele verschiedene Kennungen und Paßworte merken, um seine Arbeit erledigen zu können. Da es für viele Benutzer schwer ist, sich verschiedene Kennungen und die dazugehörigen Paßworte einzuprägen, verleitet das zu einem unsicheren Umgang mit den Paßworten (z.B. das Wählen unsicherer, leicht zu erratender Paßworte, Notieren von Paßworten auf leicht zugänglichen Unterlagen etc.). Aus diesem Grunde wird durch die Institutionen für die Informationsressourcen ein Single-Sign-On (SSO) angestrebt, wobei sich der Benutzer mit einer Kennung authentisiert und daraufhin alle Dienste nutzen kann.

Wichtig für das Single-Sign-On im Bereich der Zugriffskontrolle für lizenziertes Material ist, daß der Benutzer von autorisierter Seite authentisiert wurde,

denn die autorisierenden Stellen müssen einer anderen Autorität vertrauen. Darum kommt in diesem Einsatzgebiet eine SSO-Lösung, die wie PASSPORT[5] auf der Selbstregistrierung der Benutzer beruht, nicht in Frage.

Aus der Sicht der Institution ist das Ziel für das Single-Sign-On, daß ein Benutzer alle zu seiner (ihm von der Institution verliehenen) digitalen Identität zugänglichen Dienste mit *einem* Identitätsnachweis nutzen kann. Aus der Sicht des Benutzers stellt sich das Problem anders dar. Da er in verschiedenen Institutionen angemeldet ist, besitzt er verschiedene digitale Identitäten (Rollen), für die er jeweils einen eigenen Identitätsnachweis erhält. Für den Benutzer erscheint eine SSO-Lösung erstrebenswert, bei der er seine verschiedenen digitalen Identitäten mit nur einem Identitätsnachweis nutzen kann. Für die Institution ist dieses Ziel problematisch, denn die Institution A muß dafür der Authentisierung der Institution B vertrauen und umgekehrt. Dies wird genau dann zum Problem, wenn A und B verschiedene Sicherheitsrichtlinien oder gar unterschiedlich sichere Authentisierungsmethoden verwenden.

Um das zweite Risiko zu mindern, kann der Benutzer die Sicherheit seines Pseudonyms verbessern. Dazu sollte ein Nutzer mehrere Pseudonyme besitzen, unter denen er seine Transaktionen tätigt. Dadurch wird die Wahrscheinlichkeit verringert, daß die Menge der Informationen, die zu einem Pseudonym gesammelt werden, nicht ausreicht, das Pseudonym *ohne* Kenntnis der Zuordnungsregel zu reidentifizieren.

Diese Strategie widerspricht dem Wunsch der Benutzer, sich so wenige Kennungen und Paßworte wie möglich merken zu müssen. Für den Benutzer wäre es sicher einfacher, in allen Bibliotheken in Berlin und Brandenburg nur eine Benutzerkennung zu besitzen. Technisch ist das durchaus möglich, jedoch widerspricht dies dem Prinzip des Selbstdatenschutzes auf der einen und der lokalen Autonomie der Institutionen auf der anderen Seite. Letztendlich ist es der Benutzer, der entscheidet, mit welchem Aufwand er seinen Selbstdatenschutz realisieren will. Die Institution muß ihm die Möglichkeit dazu bieten.

In jedem Falle führt die Bestrebung der Institution nach einer SSO-Lösung dazu, daß der einzelne Benutzer weniger Möglichkeiten besitzt, die Vertraulichkeit und Zuverlässigkeit seiner Pseudonyme zu sichern. Diesen Interessengegensatz gilt es zu lösen.

4 Diskussion möglicher Lösungen

4.1 Kontrolle der IP-Adresse

Gegenwärtig wird die Zugriffskontrolle für viele Dienste, die lizenziertes Material zur Verfügung stellen, über die Kontrolle der IP-Adresse durchgeführt. Dieses Verfahren ist aber wenig geeignet, den Lesern den Zugang ortsunabhängig zu gewähren.

Lösungen, die den Benutzer auch am Arbeitsplatz zu Hause mit einer IP-Adresse aus dem Campus-Netz versorgen (z.B. DfN@home[6]), bieten eine Lösung, die den Benutzer zwingt, einen bestimmten Telefondienste- *und* Internetdiensteanbieter zu nutzen. Zudem vernachlässigt dieser Ansatz den Benutzer, der in verschiedenen Instituten arbeitet. Diese Institute bieten in der Regel keinen Internetzugang über Wählverbindungen an, so daß der Benutzer am aktuellen Arbeitsplatz die Ressourcen, auf die er vom Arbeitsplatz in der anderen Institution

[5] http://www.passport.com/

[6] http://www.dfn.de/DFNZugang/home.html: „Der Dienst ist von allen Telefonanschlüssen der Deutschen Telekom nutzbar...“

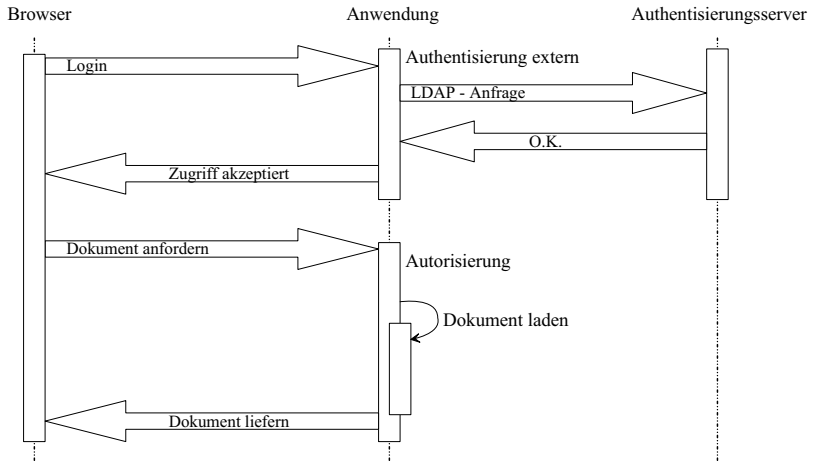

Abbildung 2: Wird von der Anwendung eine externe Authentisierung durchgeführt, sind Anwendung und Authentisierungsdienst eng gekoppelt.

Zugriff hätte, nicht nutzen kann. Dieser Ansatz ist außerdem nicht für jede Institution angemessen, denn diese müssen von ihrer Seite aus bestimmte Voraussetzungen schaffen. Nicht jede Institution ist in der Lage, den dafür notwendige Aufwand zu leisten bzw. es hat nicht jede Institution das Personal, um die notwendigen technischen Anlagen zu betreiben.

Da in den Institutionen verschiedene Rechner von mehreren Personen benutzt werden, läßt sich bei einer Zugriffskontrolle, die auf der Kontrolle der IP-Adresse basiert, ein eventueller Mißbrauch nur einem Rechner zuordnen. Deutlich schwieriger ist es dann, persönlich Verantwortliche festzustellen.

Mit Hilfe von Proxies kann der Benutzer die Ortsbindung umgehen. Allerdings beeinträchtigt diese Lösung die Nutzung von Referenzlinks. Für den Anbieter ist dieses Verfahren insofern ungünstig, als daß Zugriffe unterschiedlicher Benutzer schwieriger zu unterscheiden sind.

4.2 Identitätsnachweis-basierte Verfahren

Gegenüber der Kontrolle der IP-Adresse haben Systeme, die auf der Kontrolle von Identitätsnachweisen basieren, deutliche Vorteile. Hier besteht die Möglichkeit, Zugriffe einzelnen Personen zuzuordnen und der einzelne Nutzer ist bei der Nutzung der Dienste nicht mehr an ein bestimmtes Netzwerk gebunden.

Daraus ergibt sich die Notwendigkeit, daß die Anwendungen, welche Zugriff auf das lizenzierte Material vermitteln, auf die Benutzerdaten zugreifen müssen. Damit die personenbezogenen Daten der Benutzer in den Benutzerdatenbanken weitgehend geschützt werden, sollen die Benutzerdatenbanken in jeder Institution selbst verwaltet werden.

Anwendungen können auf bestehende Benutzerdaten zugreifen, indem die Anwendung mit einer externen Benutzerdatenbank gekoppelt wird. Wie in der Abbildung 2 skizziert, nimmt die Anwendung die Identitätsnachweise — in der Regel Benutzername und Passwort — entgegen. Die übermittelten Identitätsnachweise werden nun nicht wie in Abbildung 1 gegen eine eigene Benutzerdatenbank geprüft, sondern sie werden über ein standardisiertes Protokoll (z.B. LDAP) dem Authentisierungsserver übermittelt, der deren Gültigkeit überprüft. Mit diesem Verfahren läßt sich das Replizieren von Benutzerdaten vermeiden,

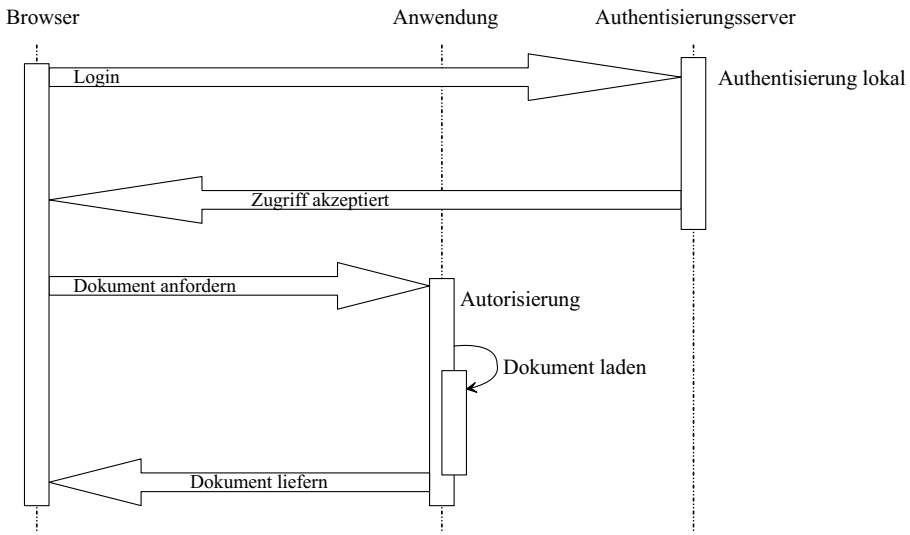

Abbildung 3: Die Zugriffskontrolle wird von zwei Anwendungen, die an verschiedenen Orten betrieben werden können, realisiert.

was vor allem dann von Bedeutung ist, wenn viele unterschiedliche Anwendungen diese eine Benutzerdatenbank benutzen. Jedoch ist die Heimatdomäne gezwungen, die Authentisierung mit Benutzername und Passwort durchzuführen. Änderungen des Authentisierungsverfahrens sind schwierig durchzuführen, weil *alle* angeschlossenen Anwendungen ebenfalls geändert werden müssen.

Eine weitere Lösung bietet der u.a. im Rahmen von ReDI[7] eingesetzte IBPlusServer. Der IBPlusServer fungiert quasi als Vermittler, der auf Seiten der Institution verschiedenste Benutzerdatenbanken (AFS, SQL-Datenbanken, verschiedene Bibliothekssysteme, LDAP) und auf Seiten der Anbieter verschiedene Authentisierungsmethoden unterstützt. Die verschiedenen proprietären Anmeldungsprozeduren bei den Anbietern werden für den Benutzer gekapselt. Nach der Anmeldung des Benutzers am IBPlusServer baut dieser eine Verbindung zu einem gewünschten Zielsystem auf. Der IBPlusServer authentisiert sich gegenüber dem Zielsystem. Wenn die Authentisierung erfolgreich war, wird die initiierte Session an den Benutzer weitergereicht. Das geschieht z.B. dadurch, daß die URI's des Zielsystems, die eindeutige Sessionkennzeichen enthalten, mit einem HTTP-Redirect an den Benutzer weitergeleitet werden. Obwohl der Einsatz eines Proxies prinzipiell möglich ist, wird dies im Rahmen von ReDI nicht praktiziert. Da jedoch der Zugriff auf die Zielsysteme *immer* durch den IBPlusServer vermittelt wird, schränkt das die Nutzung von Referenzlinks ein.

Die Einführung eines Systems zur verteilten Zugriffsverwaltung ist sicher keine triviale Aufgabe. Darum sollte die anzustrebende Lösung zumindest mittelfristig tragfähig sein. Das wiederum schließt die Möglichkeit ein, daß in dem Zeitraum, in dem das Zugriffskontrollsystem eingesetzt wird, sich neue Standards und Methoden für die Authentisierung durchsetzen werden.

Die dritte mögliche Architektur trennt Authentisierung und Autorisierung nicht nur logisch, sondern auch physikalisch (Abbildung 3). Die Authentisierung wird lokal in der Heimatdomäne des jeweiligen Benutzers durchgeführt. Autorisierung ist die Entscheidung, die beim Anbieter lokal in seinem System gefällt wird. Diese Entscheidung muß natürlich für jeden Benutzer neu getrof-

[7] http://www.redi-fr.belwue.de/

fen werden. Für diese Entscheidung braucht der Anbieter Informationen über die erfolgreiche Authentisierung des Benutzers und weitere Informationen über den Benutzer, aufgrund derer die Autorisierungsentscheidung getroffen werden kann.

Damit basiert die Entscheidung über die Autorisierung nicht auf einer Authentisierung, die der Anbieter selbst durchführt, sondern auf einer Aussage der Heimatdomäne (genauer des Authentisierungsdienstes der Heimatdomäne) über den Benutzer. Dafür müssen das authentisierende und das autorisierende System kooperieren — die Systeme müssen interoperabel sein. Dazu müssen Authentisierungsdienst und Autorisierungsdienst ein Protokoll vereinbaren, wie die notwendigen Informationen über den Benutzer ausgetauscht werden. Idealerweise sollte der Austausch der notwendigen Informationen in standardisierter Weise erfolgen.

OASIS[8] ist eine Vereinigung von Organisationen und Personen aus der ganzen Welt, die sich mit der Entwicklung und Anwendung von Standards im Bereich des e-business beschäftigt. Eines der technischen Komitees erarbeitete einen Entwurf für den XML-basierten Austausch von Informationen zur Authentisierung und Autorisierung (SAML - Security Assertion Markup Language). Dieser Entwurf befindet sich zur Zeit im Standardisierungsprozeß und kann damit zukünftig die Basis für den Austausch von Sicherheitsinformationen bilden. In den Projekten Liberty Alliance und Shibboleth wird SAML bereits angewendet.

Damit wird es zur Voraussetzung für die Realisierung der verteilten Zugriffskontrolle, daß die Heimatdomäne einen Authentisierungsdienst anbietet. Damit der Benutzer sich nicht jedes Mal von neuem authentisieren muß, ist es die Aufgabe des Authentisierungsdienstes, sich zu merken, welche Benutzer schon angemeldet sind.

Aus den Projekten und Initiativen, die zur Zeit in verschiedenen Organisationen (Liberty Alliance, ReDI, FEIDE, FEIDHE, SwUPKI, SWITCH, TERENA, SURFNET) diskutiert werden, wurden zwei Modelle ausgewählt, die ein solches Protokoll definieren. Diese sind unter den Namen PAPI und Shibboleth bekannt und sollen im Folgenden kurz skizziert werden. Aktuelle detaillierte technische Beschreibungen finden sich auf den jeweiligen Webseiten der Projekte.

PAPI

Das PAPI-System wurde in Spanien von RedIRIS[9] entwickelt. RedIRIS ist ein nationales Forschungsnetzwerk, dem ca. 250 Organisationen angehören.

Eine Sitzung eines Benutzers beginnt damit, daß er sich an einem sogenannten Authentisierungsserver (AS) authentisiert. Dieser AS ist ein Perlprogramm, das als ein CGI-Programm vom Webserver gestartet wird. Der AS unterstützt mit Installation der Version 1.1.0 verschiedene Mechanismen zur Authentisierung (LDAP, POP3, eine eigene Benutzerdatenbank). Weitere Authentisierungsmethoden können eingebunden werden.

Die Autorisierung erfolgt an einem sogenannten Point of Access (PoA), dieser wird ebenfalls als ein CGI-Programm vom Webserver gestartet. Wo dieser PoA administriert wird, ist offen: er kann als ein Proxy innerhalb der lizenznehmenden Institution betrieben werden, er kann aber auch von einem Anbieter selbst administriert werden.

Nachdem sich der Benutzer erfolgreich am AS angemeldet hat, wird er automatisch zu allen betreffenden PoA weitergeleitet. Dabei wird dem PoA vom AS ein eindeutiger Bezeichner für den Benutzer und zusätzliche Informationen

[8] http://www.oasis-open.org/

[9] http://www.rediris.es/app/papi/index.en.html

über diesen Benutzer übermittelt. Diese Informationen dienen dem PoA für die Autorisierungsentscheidung.

Während dieser Anmeldung am PoA werden im Browser des Benutzers ein temporärer Schlüssel und ein Sessionschlüssel in Form von Cookies gespeichert. Die Schlüssel sind deshalb zeitlich begrenzt gültig, um den Mißbrauch des Schlüssels durch Kopieren des Cookies (CookieCopying) zu verhindern. Somit sind im Browser des Benutzers nach der Anmeldung aller relevanten PoA Cookies gespeichert. Greift nun der Benutzer während der Sitzung auf eine URL auf einem der PoA zu, so wird auch das entsprechende Cookie mitgesendet. Der PoA wertet die Informationen aus dem vom ihm selbst gespeicherten Cookie aus und fällt daraufhin die Entscheidung, ob der Benutzer das Dokument lesen darf. Nach diesem Zugriff auf den PoA wird das Cookie, das den Benutzer identifiziert, mit einem neuen Cookie überschrieben.

Die Informationen in den Cookies werden verschlüsselt abgelegt, dabei werden keinen Zertifikate verwendet. Die Implementierungen des Authentisierungsdienstes und des Point of Access liegen im Quellcode vor und basiert auf freier Software. Es werden OpenSSL, Perl und CPAN Module (mod_perl und andere) eingesetzt.

PAPI ist in Spanien bereits im produktiven Einsatz und wird stetig weiterentwickelt. So wird mit der Version 1.1.0 eine neue Instanz — der Group-wide Point of Access (GPoA) — eingeführt, da das ursprüngliche System nicht für sehr viele Dienste mit jeweils einem eigenen PoA skalierte. Viele PoA implementieren die gleiche Sicherheitsrichtlinie, jedoch muß dafür jeweils ein eigenes Cookie im Browser des Benutzers gespeichert werden. Nun können PoA mit der gleichen Sicherheitsrichtlinie in einem GPoA gruppiert werden.

Shibboleth

Internet2[10] ist ein Konsortium, das von über 190 Universitäten gebildet wird. Diese arbeiten in enger Partnerschaft mit ca. 100 Firmen und Behörden an der Entwicklung von Internettechnologien. „Shibboleth“[11] ist eines der Projekte von Internet2, in dessen Rahmen zur Zeit ein Prototyp entwickelt wird, der ein System für die Trennung von Authentisierung und Autorisierung bietet.

Shibboleth bietet eine Plattform, auf der verschiedenste Systeme mit dem Ziel kooperieren, über Organisationsgrenzen hinweg Ressourcen im Internet gemeinsam zu nutzen. Dazu werden Protokolle spezifiziert, wie die verschiedenen Instanzen miteinander kommunizieren. Dieses Protokoll bildet die Grundlage für die Interoperabilität der an der Zugriffskontrolle beteiligten Systeme.

Bei diesem System muß sich der Benutzer nicht notwendig vor dem Zugriff auf lizenziertes Material authentisieren. Wenn ein nicht authentisierter Benutzer auf eine solche Ressource zugreifen will, wird die Zieldomäne ihn fragen, „Woher kommst du?“ (*Where Are You From, WAYF*). Dieser WAYF-Dienst fragt nach der *Herkunft*, nicht nach den Identitätsnachweisen. Er leitet daraufhin den Benutzer weiter zu seinem jeweiligen Authentisierungsserver.

Der Benutzer identifiziert sich gegenüber seinem Authentisierungsserver, in dem er den vereinbarten Identitätsnachweis präsentiert. Nach der erfolgreichen Prüfung desselben wird der Benutzer zu der ursprünglichen Domäne weitergeleitet. Dabei wird der Zieldomäne ein zufällig erzeugter Bezeichner auf den Benutzer und Informationen über diesen Benutzer übermittelt. Dies ist im ersten Schritt die sogenannte Attribute Authority (AA), bei welcher die Zieldomäne Auskünf-

[10] http://www.internet2.edu/

[11] http://middleware.internet2.edu/shibboleth/

te über den Benutzer abfragen kann. Die Informationen werden in Form eines SAML-Dokumentes übertragen.

Die Autorisierung ist eine lokale Entscheidung der Zieldomäne. Die Entscheidung, ob einem bestimmten Benutzer Zugriff auf die angeforderte Ressource gewährt wird, fällt das Autorisierungssystem auf der Grundlage von Informationen (Attributen) über den Benutzer. Das Zielsystem fragt beim Heimatsystem (genauer bei der AA) nach den erforderlichen Informationen, die es für die Autorisierungsentscheidung benötigt. Welche Informationen von der AA an die Zieldomäne übermittelt werden, hängt nicht nur davon ab, nach welchen Attributen gefragt wurde, sondern auch davon, welche Attribute der Benutzer für diese Zieldomäne freigegeben hat. Shibboleth ermöglicht es dem Benutzer zu bestimmen, welches Zielsystem welche Informationen über ihn abfragen darf (Selbstmanagement, siehe Leitsatz 4).

Im August 2002 befindet sich die Implementierung im Stadium des Alpha-Tests. Von den entwickelnden Institutionen ist geplant, die erste Beispielimplementierung nach Fertigstellung als Open Source zur Verfügung zu stellen.

5 Resümee und Ausblick

Die bisher verbreiteten Systeme zur Zugriffskontrolle — Kontrolle der IP-Adresse des Absenders oder Benutzerkennung/Passwort in einer lokalen Benutzerdatenbank — erfüllen die Aufgabe für große Mengen von verteilten Ressourcen und große Benutzerzahlen nur unzureichend.

Darum wurden und werden neue Lösungen gesucht, welche die Kooperation der authentisierenden und der autorisierenden Systeme ermöglichen sollen. Um die Interoperabilität der Systeme zu unterstützen, werden auch von OASIS[12] Anstrengungen unternommen, um standardisierte Austauschformate für Sicherheits-, Authentisierungs- und Autorisierungsinformationen zu schaffen.

Wie in den Anforderungen definiert, soll gewährleistet werden, daß jede lizenznehmende Institution die für sie passende Lösung wählen kann. Dazu gehört die Wahl der Identitätsnachweise und die Definition der Sicherheitsrichtlinie für den Umgang mit diesen. Das schließt die Architekturen wie in Abbildung 1 und 2 als Lösung für den KOBV aus. Aus Gründen des Datenschutzes und der Aktualität der Informationen muß auch die Replikation der Benutzerdaten zu den Anbietern ausgeschlossen werden.

Ein Konzept für eine Zugriffskontrolle, das Authentisierung und Autorisierung trennt, erscheint somit als das angemessenste. In beiden vorgestellten Konzepten ist die Authentisierung ein lokaler Vorgang, der in der Heimatdomäne des Benutzers durchgeführt wird. Das setzt voraus, daß die lizenznehmende Institution ein einheitliches Authentisierungssystem besitzt, in dem jeder Benutzer mit einer eindeutigen Kennung versorgt wird[13]. Benutzerdaten müssen jedoch nicht repliziert werden, das lokale System kann das den lokalen Anforderungen entsprechende System einsetzen. Hingegen ist die Autorisierung eine lokale Entscheidung des Anbieters.

5.1 Vergleich von PAPI und Shibboleth

Die beiden vorgestellten Systeme PAPI und Shibboleth definieren jeweils ein eigenes Protokoll, wie die Kommunikation der beteiligten Instanzen realisiert

[12] http://www.oasis-open.org/

[13] Das Realisieren des Single-Sign-On ist damit auch eine Aufgabe des Authentisierungsdienstes der Institution.

wird. Beide Implementierungen unterscheiden sich auch im Hinblick darauf, wie sich die oben genannten Anforderungen im KOBV realisieren lassen. Auf diese Unterschiede soll im Folgenden eingegangen werden.

Bei beiden Systemen werden generierte Kennungen, die selbst keinen Rückschluß auf die Identität des Benutzers zulassen, vom Authentisierungsdienst an die autorisierende Stelle übermittelt. Die Realisierung der Trennung von Authentisierung und Autorisierung bei Shibboleth in Verbindung mit den Möglichkeiten für den Benutzer, die Freigabe von Informationen zu steuern, löst auch den Interessenkonflikt zwischen Selbstdatenschutz des Benutzers und SSO-Lösung auf der Seite der Institution. Die Pseudonyme werden hauptsächlich für die Authentisierung verwendet, wohingegen für die Autorisierung zufällige Bezeichner generiert werden. Welche Aussagen zu diesem möglich sind, kann der Benutzer selbst bestimmen. Damit werden für die Autorisierung gegenüber nichtpersonalisierten Diensten nur anonymisierte Daten übermittelt. Außerdem scheint es möglich zu sein, personalisierte Dienste (z.B. ein Portal) einzubinden, in dem diesem ein Pseudonym übermittelt wird. Ein weiterer wesentlicher Aspekt ist, daß die Sicherheitsinformationen in einem offenen, in Standardisierung befindlichen Format (SAML) transportiert werden.

Falls ein Leser Benutzer in verschiedenen Institutionen mit unterschiedlichen digitalen Identitäten ist, fördert die Nutzung dieser unterschiedlichen Pseudonyme die Zuverlässigkeit aller Pseudonyme und verringert so die Wahrscheinlichkeit der Reidentifizierung ohne Kenntnis der Zuordnungsregel.

In beiden Systemen wird das Referenz Linking nicht beeinträchtigt. Da die Sicherheitsinformationen nicht in dem URI übermittelt werden, die auf die referenzierten Dokumente verweisen, besteht somit die Möglichkeit, daß sowohl direkte Referenzlinks als auch durch ein Open-Link-System (z.B. SFX) generierte Links durch den Benutzer verwendet werden können. Die Sicherheitsinformationen werden bei beiden Systemen unabhängig von diesen URIs zwischen den beteiligten Komponenten ausgetauscht.

In der Spezifikation von Shibboleth [12] wird einerseits die allgemeine Architektur und Kommunikation definiert. Zum anderen wird die Bindung der Kommunikation an das HTT-Protokoll definiert (diese orientiert sich an der Standardisierung durch OASIS). Damit ist die Bindung der Kommunikation an andere Transportprotokolle möglich und eine Übertragung des Modells auf andere Bereiche denkbar.

PAPI besitzt eine einfache Architektur, ist bereits implementiert und wird produktiv eingesetzt. Mit Apache, OpenSSL und Perlmodulen scheint die technische Hürde für eine Implementierung relativ niedrig zu sein. In Spanien existieren gute Erfahrungen mit PAPI, insbesondere wenn das lizenzierte Material auf Servern angeboten wird, die von den lizenznehmenden Institutionen selbst administriert werden.

Das Modell von Shibboleth macht den besseren Eindruck, da es eine größere Skalierbarkeit verspricht. Die Implementierung von Shibboleth erscheint komplexer, da hier mehrere unterschiedliche Instanzen mit unterschiedlichen Aufgaben definiert werden. Bislang sind noch keine Aussagen darüber möglich, wie hoch die Aufwendungen für die technische Realisierung bei den Anbietern und den Bildungseinrichtungen sein werden. Eine funktionierende Implementierung ist bislang noch nicht verfügbar.

5.2 Kurzfristige Realisierung im KOBV

Bei der Entscheidung für das eine oder andere System ist nicht allein von Bedeutung, welches aus technischer und funktionaler Seite das Bessere ist bzw. besser

zu den eigenen Anforderungen paßt. Wenn es um die konkrete Realisierung geht, spielt es auch eine Rolle, ob die verschiedenen Parteien dem Konzept zustimmen und in welchem Zeitraum das Konzept umgesetzt werden soll. Wenn ein interoperables, kooperatives System zu Zugriffskontrolle in einer konkreten Umgebung eingesetzt werden soll, so sind Änderungen an den Programmen sowohl auf der Seite der lizenznehmenden Institution als auch auf der Seite der Anbieter notwendig. Eine ebenso wichtige Rolle spielt hierbei, wie die Entscheidung in den anderen, insbesondere in den anderen europäischen Ländern getroffen wird.

Da noch geraume Zeit vergehen wird, bis alle Anbieter ein System unterstützen, muß dieses System schrittweise eingeführt werden. Außerdem soll die Zugriffskontrolle baldmöglichst umgesetzt werden. Auch deshalb erscheint es nicht angebracht, auf funktionierende Implementierungen von Shibboleth zu warten. Für einen Übergangszeitraum bleibt die Zugriffskontrolle auf der Grundlage der Kontrolle der IP-Adresse eine praktikable Methode.

Außerdem wird es noch in einem längerem Zeitraum Anbieter geben, welche das eine oder andere Modell nicht unterstützen. Um den Zugriff auf diese Systeme zu ermöglichen bietet sich PAPI an, da sich mit diesem ein Proxy innerhalb der lizenznehmenden Institution betreiben läßt. Der Einsatz als Proxy ist eine Zwischenlösung, da er das Referenz Linking beeinträchtigen würde. Dies erscheint jedoch tolerabel im Hinblick auf die zusätzlichen Nutzungsmöglichkeiten, die den Nutzern daraus erwachsen. Hinzu kommt die Möglichkeit, daß sich in Zukunft Anbieter davon überzeugen lassen, den PoA als ein Modul bei sich zu implementieren. Dadurch würde sich für die Nutzer auch das Referenz Linking über die Grenzen eines Anbieters hinaus transparent gestalten.

Mit dem Einsatz von PAPI wird die Trennung von Authentisierung und Autorisierung als Prinzip eingeführt und der mögliche Übergang zum Shibboleth Modell erfordert keine Änderungen an der grundsätzlichen Architektur. Die Entwickler von PAPI und Shibboleth planen in der Zukunft die Integration beider Systeme[14], so daß ein nahtloser Übergang vom einen zum anderen möglich werden könnte.

Welches System sich im europäischen Rahmen durchsetzen wird, ist zur Zeit noch nicht abzusehen. In jedem Fall ist mit PAPI eine Architektur eingeführt, welche im Rahmen von Terena diskutiert wird und bei der die Möglichkeit besteht, daß sie sich auch bei Forschungs- und Bildungseinrichtungen anderer europäischer Länder durchsetzen wird. Das wiederum steigert die Wahrscheinlichkeit, daß ein solches verteiltes Verfahren der Zugriffskontrolle auch von den Anbietern akzeptiert und implementiert wird.

Im nächsten Schritt des Projektes muß in praktischen Tests geprüft werden, ob die Granularität der Zugriffsteuerung, die mit PAPI möglich ist, ausreicht, die Vielfalt der Bedingungen in den Bibliotheken im KOBV abzubilden. In einem weiteren Schritt sind dann für den Authentisierungsserver die entsprechenden Schnittstellen zu schaffen, damit die verschiedenen Benutzerdatenbanken eingebunden werden können. Hierbei besteht aber auch die Möglichkeit, daß die vorhandenen Schnittstellen (LDAP, POP3) genutzt werden.

Die bisher im KOBV eingesetzten Portal-Systeme (Elektra, Metalib) realisieren über die Metasuche eine einheitliche Sicht auf die verfügbare Datenbasis. Der Einsatz dieser Systeme ist mit dem vorgestellten Konzept gut zu realisieren, solange die Datenbasis der Suche die häufig frei verfügbaren Metadaten sind. In diesem Fall erfolgt der Zugriff auf das lizenzierte Material direkt vom Nutzer, der Zugriff auf das lizenzierte Material wird nicht durch den Mediator vermittelt. Sind jedoch die Metadaten das lizenzierte Material, wird die Situation etwas

[14] nach einer persönlichen Mitteilung von D. Lopez

schwieriger. Bisher ist es noch ungeklärt, ob die und wie die Zugriffsinformationen durch die genannten Portal-Systeme an den Anbieter übermittelt werden können.

5.3 Ausblick

Bisher wurde nur die Frage betrachtet, wie die existierenden Zugriffsrechte realisiert werden können. Eine andere wesentliche Frage darüber hinaus ist, wie der Benutzer darüber informiert werden kann, auf welche Ressourcen er unter welchen Bedingungen zugreifen kann. Wenn er sich auf dem Campus bewegt, kann er eine Menge von Ressourcen benutzen. Jedoch ist er auch Leser einer anderen Bibliothek, die noch weitere Datenbanken anbietet. Diese Bibliothek bietet ihm die Möglichkeit die Ressourcen zu nutzen, nachdem er sich als Benutzer der zweiten Bibliothek neu authentisiert hat. Um weitere Datenbanken zu nutzen, könnte es nötig sein, daß er sich in die betreffende Bibliothek begibt.

Antworten auf diese Art von Fragen sind sicher wünschenswert, jedoch können sie die vorgestellten Systeme nicht geben. Diese Systeme erfordern keine Interoperabilität hinsichtlich des Austauschs der Informationen *über* die Zugriffsrechte. Da der Austausch von Informationen über Rechte an geistigem Eigentum eine kritische Frage für alle an der Verwertungskette Beteiligten ist, werden auch in diesem Bereich Standardisierungsanstrengungen unternommen. Einen ersten Schritt in diese Richtung hat das <indecs>-Projekt[15] unternommen. Mit Hilfe dieser Techniken ließe sich auch ein verteiltes Repository denken, das nach den Rechten für bestimmte Benutzer abfragbar ist.

Aus einem anderem Gesichtspunkt wurde ein solches Repository (FDRM - Federated digital Rights Management) diskutiert [22]. Bemerkenswert an dem Konzept von FDRM ist die nahtlose Verknüpfung des Systems für das Access Management (Shibboleth), mit dem Repository über Rechte an digitalen Ressourcen. Da dieses Repository der Rechte an digitalen Objekten nicht nur durch Menschen, sondern auch durch Maschinen abfragbar ist, könnte dies durchaus auch zur Vertrauensbildung beitragen, da die abfragbaren Informationen unmittelbar bei einer Autorisierungsentscheidung berücksichtigt werden und damit sich die Vertragspartner über die vertragskonforme Konfiguration der Zugriffskontrolle informieren können.

Somit erscheint das Konzept von Shibboleth als dasjenige, welches sich als das offenste und zukunftweisendste darstellt und damit für den KOBV einen langfristigen Einsatz wahrscheinlich erscheinen läßt.

[15] http://www.indecs.org

Literatur

[1] *<indecs> Putting Metadata to rights - Summary Final Report* (2000) – http://www.indecs.org/pdf/SummaryReport.pdf

[2] *PA/JISC 'model licence' - framework for material supplied in electronic form* (1999) – http://www.ukoln.ac.uk/services/elib/papers/pa/licence/Pajisc21.doc

[3] Arms, William Yeo (1998): *Implementing Policies for Access Management*. – http://www.dlib.org/dlib/february98/arms/02arms.html

[4] Biskup, Joachim; Flegel, U.; Karabulut, Y. (1999): *Secure Mediation: Requirements and Design*. In: Jajodia, Sushil (Hrsg.), Database Security XII - Status and Prospects. Kluwer Academic Publishers,Boston – http://ls6-www.cs.uni-dortmund.de/issi/archive/literature/1999/Biskup_Flegel_Karabulut:1999.ps.gz

[5] Biskup, Joachim; Flegel, Ulrich; Yücel, Karabulut (1999): *Towards Secure Mediation*. In: Röhm, Alexander; Grimm, Rüdiger; Fox, Dirk; Schoder, Detlef (Hrsg.), Sicherheit und Electronic Commerce - Konzepte, Modelle, technische Möglichkeiten. DuD Datenschutz und Datensicherheit, Verlag Vieweg,Wiesbaden – http://ls6-www.cs.uni-dortmund.de/issi/archive/literature/1999/Biskup_Flegel_Karabulut:1999b.ps.gz

[6] Carmody, Steven (2001): *Shibboleth Overview and Requirements*. – http://middleware.internet2.edu/shibboleth/docs/draft-internet2-shibboleth-requirements-01.html

[7] Castro, Rodrigo; Lopez, Diego R. (2002): *PAPI - Guide for Beginners*. – http://www.rediris.es/app/papi/dist/gb/PAPI-gb.html

[8] Castro, Rodrigo; Lopez, Diego R. (2001): *The PAPI-System: Point of Access to Providers of Information*. – http://www.rediris.es/app/papi/doc/TERENA-2001/

[9] Cross-Industry Working Team (1997): *Managing Access to Digital Information: An Approach Based on Digital Objects and Stated Operations*. – http://www.xiwt.org/documents/ManagAccess.html

[10] Droz, Serge et al. (2001): *Konzept für eine elektronische Akademische Gemeinschaft in der Schweiz*. – http://www.switch.ch/aai/concept_de.pdf

[11] Dugall, B; Hebgen, M. und König, W. (1997): *Empfehlungen zur zukünftigen Struktur der Informations-systeme der wissenschaftlichen Bibliotheken des Landes Berlin unter Berücksichtigung der wissenschaftlichen Bibliotheken des Landes Brandenburg*. – http://www.kobv.de/docs/empf.pdf

[12] Erdos, Marlena; Cantor, Scott (2002): *Shibboleth Architecture Draft v05*. – http://middleware.internet2.edu/shibboleth/docs/draft-internet2-shibboleth-arch-v05.pdf

[13] Franks, J. et al. (1999): *HTTP Authentication: Basic and Digest Access Authenication - RFC 2617*. – http://www.ietf.org/rfc/rfc2617.txt

[14] Glenn, Ariel; Millman, David (1998): *Access Management of Web-based Services - An Incremental Approach to Cross-organizational Authentication an Authorization*. – http://dlib.org/dlib/september98/millman/09millman.html D-Lib Magazine

[15] Harold, Elliot Rusty (2002): *Die XML Bibel* mitp-Verlag Bonn

[16] Jansen, Gus (2000): *The Common Information System*. – http://www.indecs.org/sydney/Jansen.PDF

[17] Kahn, Robert; Wilensky, Robert (1995): *A Framework for Distributed Digital Object Services*. – http://WWW.CNRI.Reston.VA.US/home/cstr/arch/k-w.html

[18] Kuberek, Monika (2001): *KOBV : institutionalisiert*. – ftp://ftp.zib.de/pub/zib-publications/reports/ZR-01-10.pdf

[19] Kuberek, Monika; Lill, Monika, Litsche, Stefan et al. (2001): *Entwicklungsprojekt KOBV-Informationsportal - Teilprojekte der 1. Stufe*. – ftp://ftp.zib.de/pub/zib-publications/reports/ZR-01-41.pdf

[20] Lynch, Clifford (1998): *Access Management for Networked Information Resources*. – http://www.arl.org/newsltr/201/cni.html

[21] Lynch, Clifford (editor) (1998): *A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resource*. – http://www.cni.org/projects/authentication/authentication-wp.html

[22] Martin, Mairéad; Agnew, Grace et al. (2002): *Federated Digital Rights Management - A Proposed DRM Solution for Research and Education*. – http://www.dlib.org/dlib/july02/martin/07martin.html D-Lib Magazine

[23] Oberknapp, Bernd (2000): *REDI - Ein Modell zur Integration elektronischer Fachinformation*. In: Wissen in Aktion - Wege des Knowledge Managements, hg. von Ralph Schmidt, Frankfurt am Main 2000, S. 84-94

[24] Oberknapp, Bernd; Reineke-Mannherz, Cordula (1998): *Authentifizierung im ReDI*

[25] Richter, Helmut (2001): *Verschlüsselung im Internet*. – http://www.lrz-muenchen.de/services/security/pki/pki.pdf

[26] Robiette, Alan (2000): *Sparta: the Second-Generation Access Management System for UK Further and Higher Education - A discussion paper on the requirements*. – http://www.jisc.ac.uk/pub00/sparta_disc.html

[27] Roßnagel, Alexander, Pfitzmann, Andreas; Garstka, Hansjürgen (2001): *Modernisierung des Datenschutzes*. – http://www.bmi.bund.de/Annex/de_11659/Download.pdf

[28] Rust, Godfrey; Bide, Mark (2000): *The <indecs> metadata framework*. – http://www.indecs.org/pdf/framework.pdf

[29] Shaw, Sandy (2000): *JISC Committee for Authentication and Security (JCAS) - Scoping study for interim DNER authentication developments*. – http://www.portal.ac.uk/documents/scoping_study_final.doc

[30] Westerinen, A. et al. (2001): *Terminology for Policy-Based Management - RFC 3198*. – ftp://ftp.rfc-editor.org/in-notes/rfc3198.txt

[31] Wilcox, Mark (1999): *Implementing LDAP* Wrox Press Ltd. Birmingham