eleed
e-learning
& education

Issue 10
2014

DiepRuR

Dienstleistungsportfolio von Hochschulen in der Ruhr Region

Mathias Orlowski
mathias.orlowski@tu-dortmund.de

Michael Koschinski
michael.koschinski@tu-dortmund.de

TU Dortmund
ITMC
Otto-Hahn-Str. 12
44227 Dortmund

urn:nbn:de:0009-5-40295

Zusammenfassung

Aufbau einer föderativen Dienstlandschaft in der Ruhr-Region auf Basis von SAML mit dem Ziel eine organisationsübergreifende Nutzung von webbasierten IT-Diensten zu ermöglichen

Stichwörter: e-learning; webbasierten IT-Dienste; Hochschule; dezentralen Benutzerverwaltung; identity management; collaboration

Abstract

Many Universities already provide a stack of different web-based applications to support their processes in teaching, learning, research and administration. The established authentication and authorization concepts for these services are mostly designed to restrict access to domestic users.

To manage the underlying identity date and to increase security and productivity most of these universities operate Identity Management Systems. At the TU Dortmund, as well as at a variety of other universities, the centrally managed identity information is used to gain a university-wide single-signon mechanism across all web-based and non-web-based services and applications for domestic scopes.

In addition to the fact that cooperation and collaboration among universities is a favorable and positive trend we also notice a increasing requirement to share domestic services with foreign facilities and their members.

The main goal of the DiepRuR project (translated abbreviation for: distributed service portfolio among Universities from Ruhr area) is to share web-based services among foreign facilities and therefore to establish an integrated and federated solution to exchange authentication and authorization information between the participating universities from Ruhr area.

In order to reduce the repetitive manual tasks of creating redundant user accounts and to improve the quality of identity information when permitting access for foreign users, web-based services can be federated using the Security Asseration Markup Language (SAML). It offers an extended singlesign-on solution beyond the intranet and is also selected by the

German National Research and Education Network (DFN e.V.) as an interoperable non-proprietary technology for their own "Authentication and Authorization Infrastructure" (DFN-AAI).

In cooperation with the DFN, the DiepRuR solution is integrated into the DFN-AAI relying on SAML as the backend technology. This solution is therefore an excellent candidate to provide a basis for secured inter-university collaborations in the state of North Rhine-Westphalia, federating web-based services, like learning-management-systems (Moodle), library-management-systems (Aleph by ExLibris, SISIS-Sunrise by OCLC) and so on.

One of the major achievement of the project, was to gain an easy access to new and existing webbased services for the members of participating universities from the Ruhr area, using their own local accounts, and to provide an establishment level in form of the DiepRuR federation, which defines a circle of trust for joining Identity and Service Providers. In order to minimize the entry level for new federation members, in the context of deploying required federation software-settings, the DiepRuR solution is designed to support easy applicability for existing components like Service and Identity Providers and offers a wide, open implementation description.

Keywords: e-learning; webbasierten IT-Dienste; Hochschule; dezentralen Benutzerverwaltung; identity management; collaboration

Einleitung und Motivation

Die Hochschulen und Universitäten der Ruhr Region stellen ihren Nutzerinnen und Nutzern eine große und stetig steigende Anzahl von webbasierten IT-Diensten zur Verfügung. Diese Dienste tragen in wesentlichem Maße zur Qualität und Attraktivität der jeweiligen Hochschulen bei. Gleichzeitig müssen die Hochschulen dem stetig wachsendem Bedarf nach weiteren IT-Diensten gerecht werden, wobei sie sich ebenfalls den Forderungen nach einem kostensparenden und effizienten Einsatz dieser Dienste stellen müssen. Daher ist der Bedarf für eine organisationsübergreifende Nutzung von Diensten als Kooperations- und Kollaborationsform für Hochschulen gestiegen. Nicht zuletzt ist dies auch der Auslöser und die Arbeitsgrundlage für das Projektvorhaben DiepRuR gewesen, bei dem der Aufbau einer eigenen Föderation mit einer dezentralen Benutzerverwaltung und einem dezentralen Betrieb der webbasierten IT-Dienste in der Ruhr-Region vorangetrieben worden ist.

Innerhalb einer Föderation ist der Austausch von lokal gepflegten Identitätsinformationen über ein gegenseitiges Vertrauensverhältnis der Föderationspartner auf technischer Basis möglich, was wiederum eine verteilte Dienstnutzung ohne den zusätzlichen Betrieb eines zentralen Benutzerverzeichnisses zur Konsequenz hat. Dies bedeutet, dass verschiedene Dienste und Ressourcen Angehörigen der kooperierenden Hochschulen in Form eines gemeinsames Dienstleistungsportfolios zugänglich gemacht werden können und zwar unabhängig davon, an welchem Standort die Ressourcen tatsächlich physikalisch betrieben werden. Ein Zugriff auf das Portfolio ist mit lokalen Benutzerkonten möglich, die weiterhin an den Heimatorganisationen ausgestellt und verwaltet werden, was wiederum die Datensparsamkeit begünstigt aber auch die Ausfallssicherheit entscheidend erhöht, da hierfür keine zentrale Nutzerdatenbank aufgebaut werden muss.

Auf Basis dieses Föderationsgedankens hatte die Technische Universität Dortmund in einem gemeinsamen Projekt mit den Universitäten der Universitätsallianz Ruhr (UA Ruhr) im Jahr 2013 ein Konzept für ein föderatives Identitätsmanagement in der Ruhr Region entwickelt. Dieses beinhaltet ein Verfahren für eine komfortable Authentifizierung und Autorisierung an standortfremden Diensten unter Verwendung lokaler Benutzerkonten, die in den unangetasteten Identitätsmanagementsystemen der Heimatorganisationen weiterhin autonom verwaltet werden. Weiterhin stellt es Dienstbetreibern von Systemen mit einer eigenen Nutzerverwaltung geeignete Registrierungsvorgänge zur Verfügung, mit denen sich die übermittelten Identitätsdaten automatisch auf dienst-lokale Konten abbilden lassen ohne die jeweiligen betrieblichen und datenschutzrechtlichen Vorgaben zu unterwandern.

Mittels der aus dem Projekt hervorgegangenen Spezifikationen und Referenzimplementierungen wurde demnach auf Ebene der Authentifizierung und Autorisierung ein effektives und effiziente Verfahren für die organisationsübergreifende Nutzung von Diensten geschaffen, das nicht nur den jetzigen Föderationspartnern des Pilotprojekts vorbehalten ist, sondern bei Bedarf auch auf Hochschulen und Universitäten in der Ruhr-Region bzw. Nordrheinwestfalens ausgeweitet werden kann. Darauf aufbauend wurde exemplarisch ein Testsystem verankert, das den verteilten Zugriff auf elektronische Ressourcen und IT-Dienste der Bibliotheken innerhalb der UA Ruhr demonstriert.

Beim Aufbau des Testsystems und der darauf aufbauenden Referenzimplementierungen wurde explizit darauf geachtet, dass Softwaresysteme zum Einsatz kommen, die im Hochschulsektor weit verbreitet sind, so dass die Einstiegshürden bei Implementierung der Föderationslösung für künftige Mitglieder gering ausfallen und dass sich das Verfahren auch auf andere webbasierte Dienste anwenden lässt.

1 Beschreibung des Projektvorhabens

1.1 Projektziele

Ziel dieses Projektvorhabens ist der Aufbau einer gemeinsamen Infrastruktur für eine organisationsübergreifende Dienstnutzung durch die Bildung einer Föderation. Wesentliche Merkmale dieser Föderation sind:

- Verteilte Nutzerverwaltung in Form von dezentralen Authentifizierungsquellen und Autorisierungsstellen
- vertrauenswürdige Kommunikation der verteilten Komponenten untereinander, für den Austausch von Identitätsinformationen beim Dienstzugriff

Aus diesem Grund wurde innerhalb dieses Projekts zur Umsetzung einer solchen Föderation auf die vom Deutschen Forschungsnetz (DFN) erprobte und verlässliche Authentifizierungs- und Autorisierungsinfrastruktur (DFN-AAI) zurückgegriffen. Die DFN AAI wird vom DFN-Verein als Dienst für wissenschaftliche Einrichtungen betrieben. Im Prinzip schafft sie einen organisatorischen und technischen Rahmen für den Austausch von Benutzerinformationen zwischen den daran beteiligten Einrichtungen und deren Systemen. Innerhalb der DFN-AAI können Strukturierungsmerkmale gepflegt werden, mit denen sich sog. Subföderationen abbilden lassen. Mit Hilfe einer solchen Subföderation kann die

verstärkte und zielgerichtete Zusammenarbeit ausgewählter Einrichtungen, die in der DFN-AAI bereits vertreten sind, explizit zum Ausdruck gebracht werden. Darüber hinaus wird hierüber die exklusive Vertrauensbeziehung zwischen den beteiligten IT-Systemen der Föderationspartner hergestellt.

Für das Projektvorhaben DiepRuR ist daher auch eine eigene Subföderation eingerichtet worden, die Ausgangsbasis für die Umsetzung nachfolgend genannter Anforderungen war, die innerhalb der Evaluations- und Konzeptionsphase des Projekts definiert worden sind:

- organisationsübergreifende Nutzung von Diensten soll standortunabhängig und aus dem Heimatkontext heraus möglich sein:
  - Einsatz dezentraler Authentifizierungsquellen, in denen die Benutzerinformationen weiterhin autonom verwaltet und bei Anfrage den Autorisierungsstellen zur Verfügung gestellt werden
  - Einhaltung datenschutzrechtlicher Grundsätze: Übertragung von Benutzerattributen zu den Autorisierungsstellen muss den Grundsatz der Datensparsamkeit erfüllen und darüber hinaus müssen die Einverständniserklärung des Benutzers für die Datenübertragung und ggf. seine Zustimmung zu den Nutzungsrichtlinien des Dienstes eingeholt werden
  - Einsatz webbasierte Registrierungsvorgänge zur automatischen Erzeugung und Aktualisierung von dienst-lokalen Benutzerkonten, falls diese aus systemtechnischen Gründen nicht vermeidbar sind
- wechselseitige Nutzung bereits bestehender Dienste, die physikalisch an mehreren Standorten getrennt voneinander betrieben werden
- Aufbau einer Infrastruktur mit einer zentralen Autorisierungsinstanz zur gemeinsamen Nutzung von Diensten, die physikalisch nur an einem Standort betrieben werden

Eine organisationsübergreifende Nutzung von Diensten hängt prinzipiell von der Teilnahme an einem gemeinsamen Verfahren ab, in dem die Autonomie der Dienstbetreiber erhalten bleiben soll. Diesbezüglich muss die verteilte Nutzung von Identitätsinformationen beim Dienstzugriff durch entsprechende Standards, Protokolle und Softwarelösungen sichergestellt werden. Zu Beginn des Gemeinschaftsprojekts mussten daher Fragestellungen in den Bereichen der dezentralen Weitergabe und Nutzung elektronischer Identitäten geklärt werden. In einer Analyse wurden zunächst die technischen Gegebenheiten an den Standorten der beteiligten Projektpartner untersucht. Weiterhin wurden praxistaugliche Methoden eruiert, die sich für das föderative Verfahren eignen, um einerseits die administrative Unabhängigkeit und andererseits eine Vertrauensbeziehung zwischen den verteilten Systemen sicherzustellen.

Hierbei erfolgte die Festlegung zu Gunsten von SAML als föderative Schicht für den Austausch von Authentifizierungs- und Autorisierungsinformationen, aufgrund der Verwendung innerhalb der DFN AAI und der Nähe und Kompatibilität zu der Softwarelösung Shibboleth, die im Hochschulsektor etabliert ist.

Die Ergebnisse und Erkenntnisse dieser Projektphase waren eine wesentliche Grundlage für die weiteren Projektaktivitäten, die in den folgenden Meilensteinen zusammengefasst sind:

- Implementierung technischer Grundlagen: Erstellung eines Anforderungskatalogs und Konzepts zur Implementierung der Föderationslösung
- Verdeutlichung der Betriebsfähigkeit des Konzepts anhand der verteilten Nutzung von Bibliotheksdiensten innerhalb der UA Ruhr
- Prototypische Einbindung weiterer webbasierter Verfahren am Beispiel der Lernplattform Moodle

1.2 Vorgehensweise im Projekt

Zu Beginn des Projekts hat sich während der Evaluationsphase gezeigt, dass bestehende Dienste der jeweiligen Standorte oftmals nur auf die Verwendung lokaler Identitätsmanagementsysteme der eigenen Hochschule optimiert sind. Dies bedeutet, dass Dienstbetreiber für Nutzer fremder Einrichtungen manuelle, z.T. zeitintensive und fehleranfällige Registrierungsvorgänge zur Einrichtung dienstlokaler Konten vorhalten müssen, die stark von den standortbezogenen Gegebenheiten des betreffenden Systems abhängig sind.

An dieser Stelle setzt das Konzept des föderativen Verfahrens an, dass innerhalb des Gemeinschaftsprojekts entwickelt worden ist, um die technische Lücke zu schließen. Während der Evaluations- und Konzeptionsphase war in gemeinsamen Sitzungen und Workshops mit den projektbeteiligten Universitäten ein Anforderungskatalog erstellt worden. Dieser diente als Grundlage für die anschließenden technischen Umsetzungsarbeiten. Zunächst wurde in einem ersten Schritt ein Prototyp entwickelt, der die generelle technische Funktionsweise des Verfahrens demonstrierte. Darauf aufbauend wurde ein erweitertes Testsystem entwickelt und an den Standorten der projektbeteiligten Universitäten installiert, um die Betriebsfähigkeit und die Grenzen des konzipierten Verfahrens im Hinblick auf unterschiedliche Anwendungsgebiete zu verdeutlichen.

Um die Vielfalt komplexer Einsatzgebiete aufzuzeigen, auf die das Verfahren zum Zwecke der verteilte Dienstnutzung produktiv angewendet werden kann und um den Zielvorgaben des Gesamtprojekts zu entsprechen, wurden exemplarisch IT-Dienste der Bibliotheken aus der UA Ruhr ausgewählt, um in einem ersten Schritt die zuvor genannten Vorteile des Verfahrens speziell Studierenden dieser Region zugänglich zu machen. Die nachfolgenden Punkte beschreiben die Vorgehensweise und Aktivitäten innerhalb dieses Projektabschnitts:

- Beschreibung der Use-Cases für föderierte Nutzung der Bibliotheksdienste
- Festlegung und technische Spezifikation der Attributübertragung beim Dienstzugriff
- Aufbau eines Testsystems an den drei Standorten der UA Ruhr
- Beurteilung der Einhaltung datenschutzrechtlicher Vorgaben durch Einbindung des Datenschutzbeauftragten

Im letzten Projektabschnitt wurden weitere IT-Dienste analysiert, die sich für die organisationsübergreifende Nutzung anbieten. Hierbei wurde vor allem die generelle Praxistauglichkeit der ausgewählten Dienste innerhalb der Föderation geprüft sowie technische Voraussetzungen und weitere Anforderungen, die mit dem Verfahren geschaffen bzw. erfüllt werden müssen. Stellvertretend für die Klasse der Lernplattformen wurde die Lernplattform Moodle herausgegriffen und zu Testzwecken an das Verfahren angebunden.

1.3 Ausgangslage bei Bibliothekssystemen der UA Ruhr

Die bisherige Anmeldung an einer standortfremden Bibliothek innerhalb der UA-Ruhr erfolgt auf Basis der jeweils genutzten Studierendenkarten (UniCards).

Für Bochum und Dortmund werden unterschiedliche Chips zur Speicherung der Identifikation des Besitzers auf der Karte verwendet. In Duisburg-Essen dient ein auf der Karte aufgedruckter Barcode zur Identifikation des Besitzers. Dementsprechend gibt es für die verschiedenen Kartensysteme (Chip, Barcode) unterschiedliche Lesegeräte. Mehrere verschiedene Lesegeräte für die angeschlossenen Universitäten sind in den Bibliotheken jeweils bereits vorhanden und werden zur Authentifizierung eingesetzt. Das hochschulübergreifende Lesen der Kennung ist damit möglich. Zum Teil (bei den Chipkarten) wird auf diesem Wege bereits der Kartenstatus abgefragt und ggf. eine Nutzung (bei ungültigen Zertifikaten) verweigert.

In den UA-Ruhr Bibliotheken kommen unterschiedliche Bibliothekssysteme mit unterschiedlichen Anbindungen der lokalen Identitätsmanagement-Systeme (IdM-Systeme) zum Einsatz. Die UB Bochum und die UB Dortmund verwenden das Bibliothekssystem SISIS SunRise (Hersteller OCLC). In Dortmund erfolgt die Kommunikation mit dem lokalen IdM-System über einen proprietären IdM-Connector, ein Zusatzmodul des Bibliothekssystemherstellers. In der UB Duisburg-Essen kommt das System Aleph (Hersteller Ex Libris) zum Einsatz. Sowohl bei der UB Bochum als auch an der UB Duisburg-Essen werden täglich Änderungsdatensätze aus dem heimatlokalen IdM-Systemen exportiert und über eine datenbankkonforme Schnittstelle ins Bibliothekssystem importiert.

Die Struktur der eingesetzten Bibliothekssysteme erfordert es, dass für jeden Nutzer im System ein lokales Dienstkonto angelegt ist. Die Nutzerkonten werden in erster Linie für lokale Bibliotheksdienste verwendet, weiterhin jedoch auch für den Zugriff auf DigiBib einschließlich der Fernleihe des Hochschulbibliothekszentrums (hbz, Zentrale des Bibliotheksverbundes NRW).

1.4 Anforderungen für föderierte Bibliotheksnutzung

Im Gegensatz zu der Nutzung rein webbasierter Dienste, bei denen in der Regel alle Prozessschritte innerhalb der Webumgebung durchgeführt werden, finden bei Bibliothekssystemen Prozessabfolgen auch außerhalb webbasierter Anwendungen statt wie z.B. die Buchausleihe mittels Bibliotheksausweis oder die Durchführung von

Mahnverfahren. Insofern musste mit dem Einsatz des föderierten Verfahrens sichergestellt sein, dass hierüber dienst-lokale Konten in der Benutzerverwaltung des jeweiligen Bibliothekssystems initial erzeugt und auch auf einem aktuellen Stand gehalten werden.

Zur Erfüllung dieser Anforderungen wurden in der Umsetzungsphase entsprechende Funktionen und Erweiterungen mit Schnittstellen zu den jeweiligen Bibliothekssystemen programmiert.

Im Fall der TU Dortmund wurden diese Funktionen innerhalb des Serviceportals realisiert. Das Serviceportal repräsentiert einen zentralen Einstiegspunkt für alle personalisierten IT-Dienste innerhalb der Universität und ist mit effizienten Authentifizierungs- und Autorisierungsmechanismen ausgestattet, die allerdings bislang nur den Einsatz lokaler Benutzerkonten unterstützen. Daher wurden die dahinterliegenden Systeme mit selbstentwickelten Komponenten angereichert, so dass auch eine organisationsübergreifende Anmeldung und Nutzung möglich ist. Somit können auf diese Weise neben den erwähnten Bibliotheksdiensten nun auch andere Portaldienste der TU Dortmund ohne zusätzlichen technischen Anpassungsbedarf in der Subföderation angeboten werden. Mit diesem Vorgehen ist demnach auch die Anforderung umgesetzt worden, eine Infrastruktur mit einer zentralen Autorisierungsinstanz für organisationsübergreifende Nutzung von Diensten aufzubauen, die physikalisch nur an einem Standort betrieben werden bzw. verfügbar sind.

Im Gegensatz zu dieser zentralen Variante der Freigabesteuerung auf Dienste wurden bei den Projektpartnern die Autorisierung und Freigabesteuerung innerhalb der Webumgebung der Bibliothekssysteme SISS-Sunrise des Herstellers OCLC sowie Aleph von Ex-Libris verankert.

Vorteile des föderativen Verfahrens für UA Ruhr Studierende:

- Dienstnutzung der Föderationspartner über webbasierte Self-Services jederzeit und standortunabhängig möglich:
  - Registrierung am Bibliothekssystem zur Erzeugung eines lokalen Dienstkontos
  - Einsicht Bibliothekskonto: Ausleihen, Bestellungen, Gebühren
  - Einsicht Profildaten
- Vor-Ort-Nutzung: z.B. Entleihungen mit Bibliotheksausweis der Heimatuniversität

Vorteile des Verfahrens aus Verwaltungssicht:

- Keine manuelle Erfassung und Pflege von Daten
- Keine Ausweisproduktion und –ausgabe

1.5 Kritische Erfolgsfaktoren

Die organisationsübergreifende Nutzung von Diensten ist wie bereits dargestellt mit diversen Vortei len für die Angehörigen der Föderationspartner verbunden. Die Effizienz und Effektivität des dahinterliegenden Verfahrens ist letztlich an die Erfüllung unterschiedliche Anforderungen geknüpft.

In diesem Zusammenhang wurden im Projekt folgende kritische Erfolgsfaktoren für das Verfahren festgelegt. Das Verfahren soll demnach:

- einer unzweckmäßigen, redundante Haltung von Identitätsdaten vorbeugen,
- die Aufwände zur Verwaltung standortfremder Benutzerkonten verringern,
- den Zielen das Datensparsamkeit und Datentransparenz genügen,
- im Zuge der verteilten Dienstnutzung keine weiteren Identitäten erschaffen,
- die DFN-Infrastruktur und vorhandene Authentifizierungssysteme der Teilnehmer nutzen,
- keine technische Veränderung der lokalen IdM-Systeme erfordern,
- zu einer positiven Nutzer-Erfahrung beitragen,
- und darüber hinaus möglichst auf breiter Basis in der Hochschul-IT anwendbar sein (Skalierbarkeit in Ruhr-Region und NRW).

2 Beschreibung des Verfahrens und seiner Funktionsweise

Wie bereits im vorherigen Kapitel dargestellt wird mit dem Föderationskonzept die verteilte Dienstnutzung aus technischer und organisatorischer Sicht vereinfacht.

Prinzipiell wird dies erreicht, indem die für die Dienstnutzung erforderlichen Autorisierungsinformationen von der Heimateinrichtung elektronisch zum Dienstanbieter übertragen werden, sofern der betreffende Anwender der Datenweitergabe zustimmt. Das Verfahren stellt über geeignete Softwarelösungen in Form definierter Abläufe und mittels spezifizierter Schnittstellen und Protokolle eine verschlüsselte und gesicherte Übertragung zwischen dem Dienstanbieter (Serviceprovider) - z.B. dem Bibliothekssystem - und dem Identitätsprovider der Heimateinrichtung her. Aufgrund der gesicherten elektronischen Übertragung der Identitätsinformationen ist eine manuelle Erzeugung von Benutzerkonten nicht mehr notwendig.

2.1 Verteilte Benutzerverwaltung

Im Verfahren wurde vorgesehen, dass sich der Benutzer ausschließlich bei seinem Heimat-Identitätsprovider (Heimat-IdP) mit Benutzernamen und Kennwort (oder mit Chipkarte) anmeldet, da nur dort die Identitätsdaten verwaltet und geprüft werden können. Bei einer erfolgreichen Authentifizierung wird vom Heimat-IdP ein elektronischer Ausweis (elektronisch verschlüsseltes Dokument sog. e-ID) erstellt, der innerhalb der DiepRuR Föderation zur Nutzung des gemeinsamen Dienstleistungsportfolios berechtigt. Die e-ID kann nur von Dienstbetreibern (Serviceprovidern) der Föderationspartner beim Zugriff auf ihre geschützten IT-Ressourcen ausgewertet werden und erleichtert damit das Zugriffsverfahren für standortfremde Nutzer, da keine separaten Dienstkennungen bzw. Zugangsdaten erforderlich sind.

Da der Serviceprovider (SP) keine lokalen Identitäten vorhält, kann er eine Unterscheidung und Autorisierung der Benutzer beim Dienstzugriff nur über die durch den Identitätsprovider ausgestellte e-ID gemäß der darin enthaltenen Identitätsattribute vornehmen. Es handelt sich somit um ein dezentrales Verfahren zur Identitätsfeststellung, da der SP selbst keine Identitätsdaten verwaltet und speichert, sondern die Verwaltung identitätsbezogener Informationen an den zugehörigen IdP des Anwenders delegiert.

Mit der Anwendung dieses verteilten Authentifizierungs- und Autorisierungsverfahrens für die standortfremde Nutzung von Bibliotheksdiensten der UA-Ruhr werden folgende Systemrollen definiert: Die lokalen IdM-Systeme der UA-Ruhr erfüllen über ihre vorhandenen technischen Schnittstellen die Rolle sog. IdPs. Die Bibliothekssysteme repräsentieren mit ihren angebotenen Webdiensten die Rolle der SPs, die Authentifizierungs- und Provisionierungsanfragen an die IdPs delegieren und deren Rückmeldungen entgegennehmen.

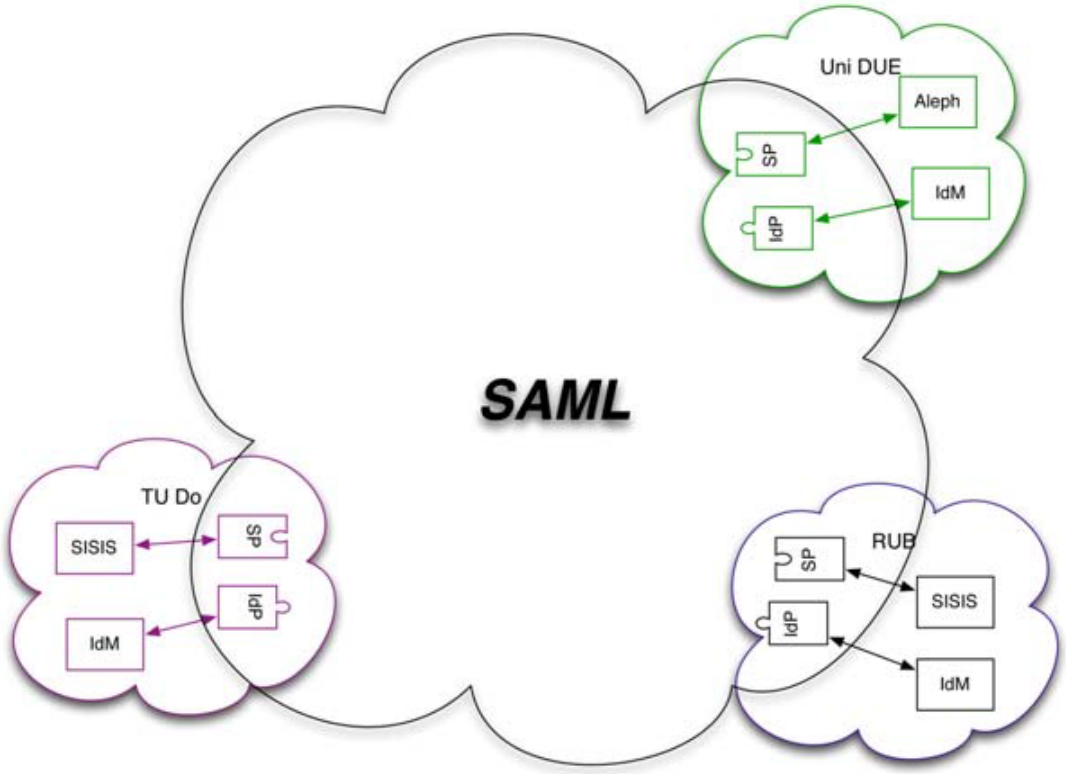

Abbildung 1: Schema der verteilten Bibliotheksnutzung innerhalb der UA-Ruhr

Für den föderierten Dienstzugriff auf Bibliothekssysteme der UA Ruhr wurden daher nachfolgende Funktionen im SP implementiert:

- Weitergabe der Authentifizierungsanfrage an den zuständigen IdP des Anwenders
- Webbasierter self-service zur Registrierung und Erzeugung neuer Benutzerkonten im Bibliothekssystem, sofern anhand der übermittelten Identitätsdaten kein zugehöriges Benutzerkonto gefunden wurde (Provisionierung durch einmaliges Registrieren unter Verwendung der übermittelten Identitätsdaten)

- Freigabe der Bibliotheksdienste falls ein gültiges Benutzerkonto im Bibliothekssystem vorhanden ist und automatische Aktualisierung der Konto- und Profildaten

2.2 Föderationsmanagement

Die Durchführung identitätsbezogener Vorgänge erfordern sowohl die Sicherheit der eingesetzten Systeme als auch die Einhaltung datenschutzrechtlicher Bestimmungen. Im Zuge der verteilten Dienstnutzung werden Authentifizierungs- und Autorisierungsvorgänge wechselseitig delegiert. Daher muss zwischen dem Dienstanbieter und dem Identitätsprovider eine entsprechende Vertrauensbeziehung auf technischer und organisatorischer Basis vorhanden sein. Durch die Interoperabilität mit dem DFN und Nutzung der DFN AAI kann diese Vertrauensbeziehung aus technischer Sicht effizient und effektiv umgesetzt werden.

Innerhalb der AAI des DFN verwalten die einzelnen Einrichtungen ihre Einträge für die betreffenden Systeme selbst. Jede Einrichtung kann genau einen IdP und mehrere SPs über sog. Entity-IDs benennen. Die Berechtigungsfreigabe von IdPs und SPs für die Teilnahme an der DiepRuR Föderation erfolgt zentral in Form einer Whitelist, die an der TU Dortmund gepflegt wird. Diese Whitelist ist über das HTTP-Protokoll vom DFN abrufbar und enthält alle Entity-IDs der berechtigten Systeme der Föderationspartner. Diesen Entitäten können die zuständigen Dienstbetreiber der jeweiligen Heimatorganisation im Web-Portal der DFN AAI die erforderliche Entity-Kategorie anschließend selbständig zuweisen. Der Eintrag für die Entity-Kategorie der DiepRuR Föderation erscheint automatisch in einer Auswahlliste.

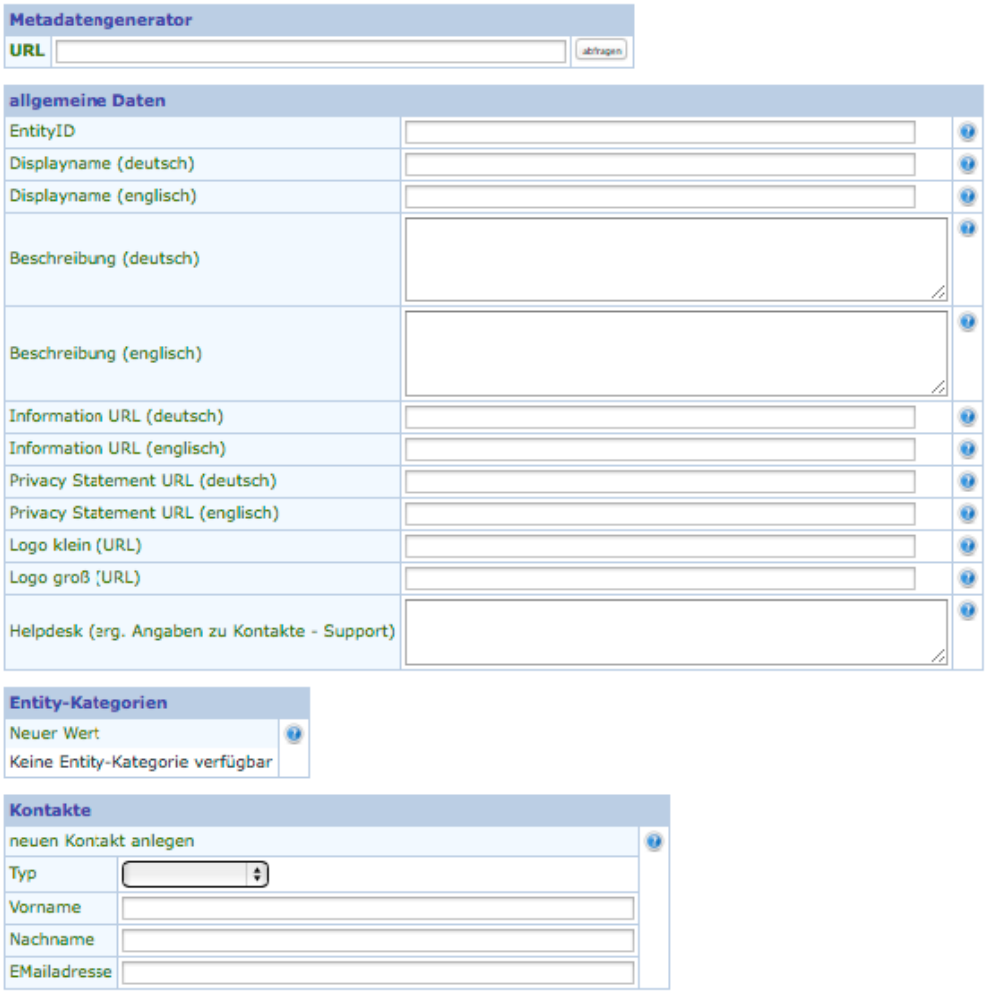

Abbildung 2: Web-Portal der DFN AAI zur Pflege der Entity-Daten

Diese Vorgehensweise sorgt dafür, dass die Systeme der Föderationspartner untereinander bekannt sind und sich gegenseitig bei der Beantwortung von Anfragen und Durchführung identitätsbezogener Vorgänge vertrauen. Somit ist die Teilnahme an der DiepRuR Föderation gleichzeitig an eine gültige Mitgliedschaft beim DFN geknüpft.

Um mit dem Verfahren eine optimale Skalierung beim Austausch von Identitätsinformationen zu gewährleisten, wurde konzeptionell auch auf die Implementierung expliziter N-zu-M Schnittstellen zwischen Dienstgebern und Dienstnehmern innerhalb der Subföderation verzichtet. Da die IdM-Systeme weiterhin autark und technisch unabhängig von den Föderationspartnern betrieben werden, wurde darauf geachtet, dass die eingesetzten Schnittstellen und Protokolle der DiepRuR Föderation resistent gegenüber technischen Änderungen und Eigenheiten dieser Systeme sind. Die wiederum erweist sich auch als Vorteil bei der Ausweitung des Verfahrens auf andere Hochschulen.

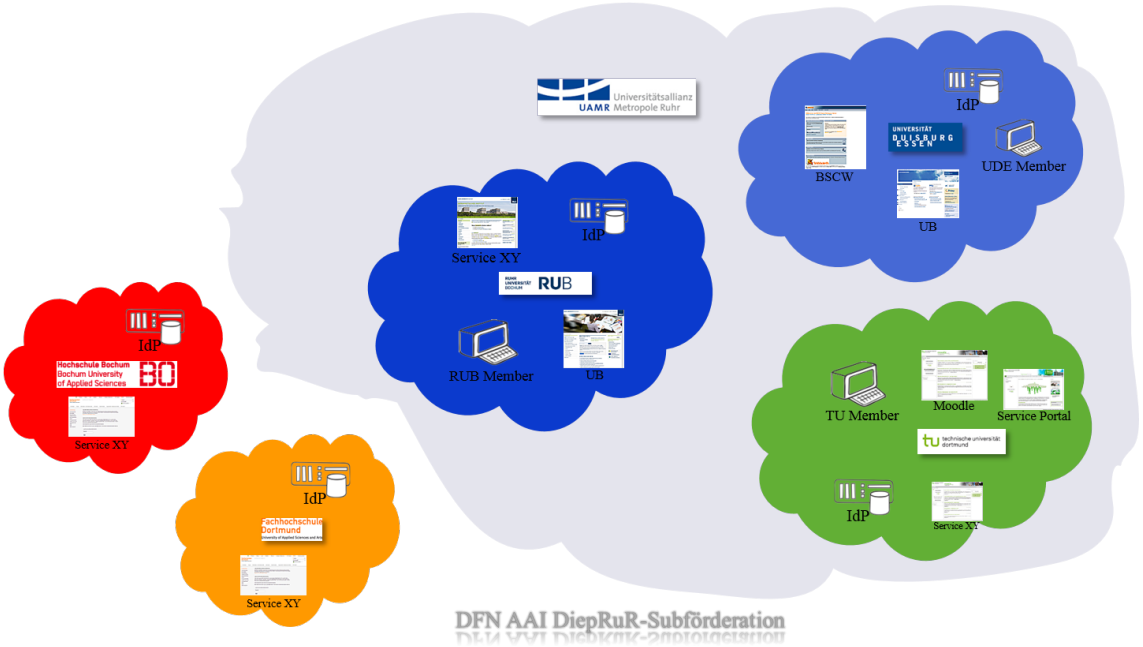

Abbildung 3: Schema der DiepRuR Föderation im Kontext der DFN AAI

Die teilnehmenden IdPs und SPs können die Metadaten entweder direkt über die DFN AAI beziehen oder über einen Discovery-Service, der für die DiepRuR Föderation zentral über den DFN bereitgestellt wird. Der Discovery-Service erfüllt im Prinzip zwei unterschiedliche Aufgaben. Einerseits kann er als Alternative zum DFN AAI Verzeichnis bei der Verteilung von Metadaten der Systeme innerhalb der Föderation genutzt werden. Andererseits nutzt der Discovery-Service Einträge aus der bereits genannten Whitelist, um bei einem föderierten Dienstzugriff die erforderlichen Authentifizierungsanfragen an den zuständigen IdP des Anwenders weiterzureichen.

2.3 Verwendete Software zum Austausch identitätsbezogener Informationen

Beim Informationsaustausch zwischen Anbietern und Nutzern von Ressourcen wird ein attributbasierter Ansatz verfolgt. Der Serviceprovider bezieht Benutzerattribute von einem Identitätsprovider aus der Heimatorganisation des Anwenders.

Der Attributaustausch erfolgt gemäß dem SAML Standard (Security Assertion Markup Language), der vom OASIS-Konsortium entwickelt worden ist, um identitätsbezogene Informationen zu beschreiben und zu übertragen. Es handelt sich um ein XML-basiertes Framework, das aus sog. SAML-Assertions, aus einem SAML-Protokoll und aus SAML-Bindings und Profilen zusammengesetzt ist. Eine SAML-Assertion enthält ein durch den Identitätsprovider ausgestellten Satz von Identitätsattributen, die an den die Authentifizierungsanfrage initiierenden SP übermittelt werden.

Die Definition der Protokolle, Spezifikationen und Assertion, die den SAML Standard beschreiben, sind ebenfalls in die vom Internet2 entwickelte Open Source Software Shibboleth eingeflossen. Demnach sind beide Definitionen quasi identisch.

Da die Shibboleth Software seitens der DFN-AAI für föderative Verfahren eingesetzt und empfohlen wird, ist SAML innerhalb des nationalen Forschungsnetzes zu einem Standard bei der Übertragung von identitätsbezogenen Informationen geworden. Neben der großen Verbreitung bietet es weiterhin den Vorteil, dass es die spezifischen Eigenheiten und Implementierungen der verwendeten IdM-Systeme vom Föderationsbetrieb entkoppelt, so dass diese sich nicht gegenseitig negativ beeinflussen. Daher wurde im Projekt während der Evaluationsphase die Entscheidung zu Gunsten von SAML getroffen.

Neben der Open-Source Variante Shibboleth existieren auch kommerzielle Produkte, die SAML zur Übertragung von Identitätsinformationen implementiert haben. Darunter auch das Produkt OpenAM, das als Nachfolger von OpenSSO (ehemals SUN) von der Firma ForgeRock weiterentwickelt wird. Innerhalb des Projekts wurden beide Produkte berücksichtigt, so dass Föderationspartner diesbezüglich eine Wahlfreiheit haben, da für beide Varianten entsprechende Referenzimplementierungen angeboten werden und die Produkte darüber hinaus aufgrund der gemeinsamen Protokollschicht untereinander kompatibel sind.

Beide Produkte bestehen jeweils aus drei Komponenten, die getrennt voneinander betrieben werden können:

- Identitätsprovider: befindet sich in der Heimateinrichtung
- Serviceprovider: befindet sich beim Dienstanbieter
- Lokalisierungsdienst oder Discovery-Service (früher WAYF – Where are you from?): wird innerhalb der DiepRuR Föderation zentral beim DFN betrieben

Funktionsweise der Komponenten:

Vorgang	Beschreibung
Authentifizierung	Ein Anwender will auf eine geschützte Anwendung zugreifen, die als wechselseitiger Dienst über die DiepRuR Föderation angeboten wird. Der Serviceprovider nimmt die Anfrage entgegen und prüft, ob der Anwender bereits authentifiziert ist. Wenn nicht, dann wird der Anwender zum Lokalisierungsdienst weitergeleitet. Der Lokalisierungsdienst bietet dem Anwender eine Auswahl von Einrichtungen an, die Föderationspartner sind. Der Anwender wählt seine Heimateinrichtung aus und wird zum Authentifizierungsserver (IdP) dieser Einrichtung weitergeleitet. Die Heimateinrichtung prüft, ob der Anwender bereits authentifiziert ist und ob der Anfrage des initiierenden Serviceproviders vertraut werden kann (Circle of Trust) . Falls der Anwender nicht authentifiziert ist und der Anfrage des Serviceproviders vertraut wird, dann wird der Anwender aufgefordert die Authentifizierung durchzuführen (z.B. Eingabe von Benutzername und Passwort oder mittels Chipkarte). Nach erfolgreicher Authentifizierung stellt der IdP der Heimateinrichtung einen digitalen Ausweis aus (e-ID mit Identitätsattributen). Sofern der Anwender der Übermittlung der e-ID an den Serviceprovider zustimmt (elektronische Feststellung der Einwilligung mittels Opt-In-Modell), dann wird er automatisch zum Serviceprovider zurückgeleitet. Der Verbindungsaufbau und Austausch der e-ID erfolgt mittels SAML.
Autorisierung	Der SP entscheidet anhand der ausgestellten e-ID, ob er der Authentifizierungsstelle (IdP) vertraut und ob der Benutzer auf das System oder die Ressource gemäß der übermittelten Identitätsattribute zugreifen darf.

2.4 Konfiguration der SAML Schicht

Im Rahmen des Projekts sind folgende Festlegungen getroffen worden, um die Interoperabilität der SAML-Schicht zu gewährleisten:

SAML Element	Festlegungen
Unterstützte Protokolle	AuthN Request, SSO, SLO, IdP Disco
Unterstütztes Login Profile	Web Browser SSO
Unterstütztes Binding	HTTP POST (empfohlen); HTTP Redirect
Initiator	SP
Unterstütztes Logout Profile	Web Browser SLO
Authentication Context	Password Protected Transport
Name-ID-Format	urn:oasis:names:tc:SAML:2.0:nameid-format:transient
AuthN-Requests	signed
Post-Responses	signed
Logout Requests	signed
Logout Responses	signed

Jede Einrichtung die im Rahmen von DiepRuR Dienste anbieten möchte oder die ihren Nutzern die vorhandenen DiepRuR-Dienste zur Verfügung stellen will, muss die eigene(n) SAML Komponente(n) in dieser Konfiguration zur Verfügung stellen.

2.5 Art der übertragenen Daten und deren Verwendung

Die konkreten Daten, die mittels SAML attributbasiert übertragen werden, bilden den Ausgangspunkt für ein einheitliches Informationsmodell. Je nach Dienstzugriff werden unterschiedliche Attribute für die Freigabesteuerung benötigt. In einem gemeinsamen Workshop, an dem die jeweiligen Dienstbetreiber der UA Ruhr Universitäten aus verschiedenen Bereichen geladen waren, wurde an einer einheitlichen Attributspezifikation für das DiepRuR Verfahren gearbeitet. Es wurden die nachfolgenden Attribute identifiziert und spezifiziert, die für die Autorisierung und Anwendungsunterstützung mindestens erforderlich sind.

A - Authentifizierung

Zur Authentifizierung am Heimat-IdP werden vom Anwender folgende Daten eingegeben:

- Nutzername/Anmeldename des Benutzeraccounts beim Heimat-IdP
- Passwort des Benutzeraccounts beim Heimat-IdP

B - Kernsatz: Grundlegende Attribute für Autorisierungsvorgänge an standortfremden Diensten

Mit dem Kernsatz werden die nachfolgenden Standardattribute beschrieben, die für die Kommunikation zwischen IdP und SP zwingend vorgesehen werden, um den Zugriff auf standortfremde Dienste innerhalb der Subföderation zu steuern:

- Kennung der Heimateinrichtung des Anwender: Das kann z.B. der Realm für die EduROAM Kennung sein, oder die ID des Statistischen Landesamtes für die Heimat-Universität.
- Status bzw. Rolle des Anwenders bei der Heimateinrichtung: Hier wäre grundsätzlich für zugriffsbeschränkte Dienste zu unterscheiden, ob es sich bei einem Anwenders um einen Student, Mitarbeiter, einen Hochschulangehörigen, etc. handelt, da lokale Rollen- und Rechtemodelle danach ausgerichtet sind.

Zur Verwendung geschützter webbasierter Ressourcen werden seitens der Dienstanbieter weitere Attribute benötigt, um einen personalisierten Zugriff auf das jeweilige Dienstangebot zu gewährleisten. Diese Attribute gelten sowohl für Heimatuser als auch standortfremde Anwender. Hierbei handelt es sich um:

- Name des Anwenders
- Vorname des Anwenders
- zugewiesene Mailadresse von der Heimateinrichtung: z.B. vorname.name@tu-dortmund.de

C - anwendungsunterstützende Attribute für Bibliothekssysteme

Für das Anlegen und Verwalten von Benutzerkonten innerhalb der Bibliothekssysteme werden zusätzliche personenbezogene Attribute vom Identitätsprovider angefordert (systemtechnische Notwendigkeit). Diese Attribute besitzen innerhalb der DiepRuR Subföderation einen optionalen Charakter, da sie nur im Rahmen der wechselseitigen Bibliotheksnutzung angefordert und daher ausschließlich für diesen Dienst genutzt werden.

- Geschlecht: in den derzeitigen Bibliothekssystemen ist die Angabe des Geschlechts für die Anlage eines Benutzerkontos notwendig
- Geburtsdatum: das Geburtsdatum ist zur Prüfung einer bestehenden Minderjährigkeit notwendig.
- private Adresse des Anwenders: wird im Rahmen von Mahnverfahren genutzt
- Kartennummer des Bibliotheksausweises: wird bei der Buchausleihe an der Theke verwendet
- persistente Nutzerkennung: ist für den Zugriff auf webbasierte Dienste der Bibliothekssysteme zur Feststellung des zugehörigen Benutzerkontos notwendig, da die Kartennummer des Anwenders im Zeitablauf nicht persistent ist

2.6 SAML Attribute für Nutzung der Bibliotheksdienste

Für die Nutzung der Bibliotheks-Dienste innerhalb von DiepRuR sind die folgenden Attribute definiert1:

Attr. Friendly Name	**Name**	**Format**
dateOfBirth	rn:oid: 1.3.6.1.4.1.25178.1.2.3	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
mail	urn:oid: 0.9.2342.19200300.100. 1.3	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
sn	urn:oid:2.5.4.4	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
cardID	cardID	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
eduPersonScopedAffiliation	urn:oid: 1.3.6.1.4.1.5923.1.1.1.9	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
O	urn:oid:2.5.4.10	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
l	l	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
givenName	urn:oid:2.5.4.42	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
postalCode	urn:oid:2.5.4.17	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
gender	urn:oid: 1.3.6.1.4.1.25178.1.2.2	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
postalAddress	urn:oid: 0.9.2342.19200300.100. 1.39	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri
permID	permID	urn:oasis:names:tc:SAML: 2.0:attrn ame-format:uri

Diese Attribute werden der IdP Komponente aus dem jeweiligen IdM-System der Einrichtung zur Verfügung gestellt. Die Attribute werden nicht im SP gespeichert, sondern ausschließlich zur initialen Erzeugung von Bibliothekskonten und deren Aktualisierung verwendet.

Für das Verhalten der SPs auf fehlende Attribute gibt es keine allgemeine Festlegung auf der SAML-Schicht. Die Reaktion des SP auf fehlende Attribute wurde jeweils lokal entschieden und dementsprechend implementiert. Können oder sollen Attribute nicht Verfügung gestellt werden, kann die föderierte Dienstnutzung nur eingeschränkt oder gar nichtmöglich sein.

Können oder sollen Attribute nicht zur Verfügung gestellt werden, dann kann die föderierte Dienstnutzung nur eingeschränkt oder gar nichtmöglich sein.

3 Anwendung des Verfahrens für die verteilte Bibliotheksnutzung in der UA Ruhr

In diesem Abschnitt wird kurz die Funktionsweise und Betriebsfähigkeit des Verfahrens dargestellt, das für die verteilte Bibliotheksnutzung prototypisch angewendet worden ist. Hierzu wurde wie bereits in den vorangegangenen Kapiteln dargestellt, ein Testsystem aufgebaut, dass sich aus den typischen SAML-fähigen Komponenten zusammensetzt, die an den projektbeteiligten Universitäten installiert bzw. für die Föderationsteilnahme angepasst worden sind.

3.1 Konfiguration des Service Providers an der TU Dortmund

Aufgrund der unterschiedlichen technischen und organisatorischen Rahmenbedingungen, welche sich an der UA Ruhr schon alleine dadurch ausdrücken lassen, dass zwei verschiedene Bibliothekssysteme eingesetzt werden (SISS Sunrise von OCLC und Aleph von Ex-Libris), wurde das Szenario zur Kontoerzeugung auch auf unterschiedliche Art und Weise implementiert. Grundsätzlich erfolgt der Zugriff auf eine geschützte Ressource immer über einen SP. Der SP prüft, ob beim Dienstzugriff ein gültiges Session-Cookie mit einer SAML Assertion vorhanden ist. Falls kein Cookie vorhanden ist, dann wird eine Authentifizierungsanfrage an den Heimat-IdP via Discovery-Service eingeleitet. Nach einer erfolgreichen Authentifizierung sendet der Heimat-IdP seine Antwort in Form einer SAML-Assertion über das vom SP ausgestellte Session-Cookie an den SP zurück. Gemäß der im Verfahren für eine föderative Bibliotheksnutzung spezifizierten Regeln führt der SP die Autorisierung durch. Am Beispiel der TU Dortmund werden Bibliotheksdienste integriert über das Service-Portals neben Universitätsangehörigen auch Föderationsnutzern von DiepRuR zur Verfügung gestellt, wobei folgende Anwendungsfälle als Self-Services umgesetzt worden sind:

- Registrierungsschritt: Neuerstellung von Benutzerkonten im Dortmunder Bibliothekssystem für autorisierte Föderationsnutzer anhand der gelieferten SAML-Attribute

- automatischer Abgleich und ggf. Aktualisierung bereits vorhandener Kontodaten bei jeder Wieder-Anmeldung und autorisierter Nutzung der webbasierten Bibliotheksdienste
- Zugriff auf die mit dem Bibliothekskonto verknüpften Informationen wie Ausleihen, Bestellungen, Gebühren, Profildaten, etc.

Das Bibliothekssystem der TU Dortmund basiert auf dem Produkt SISIS SunRise der Firma OCLC. Durch die Integration der Selbstbedienungsfunktionen in das Service-Portal der TU Dortmund, können Bibliotheksdienste über eine lokale Session im Single-Sign-On (SSO) erreicht werden. Das SSO an der TU Dortmund basiert auf dem Produkt OpenAM des Herstellers ForgeRock. Dieses Produkt kann einerseits lokale SSO-Sessions verwalten, andererseits in einer SAML-Föderation auch als Service-Provider agieren. Dabei kann es lokale Session auf Basis von SAML Assertions erzeugen.

Im lokalen SSO der TU Dortmund werden die angebundenen Anwendungen typischerweise entweder per Policy-Agent oder mit Hilfe von REST-Schnittstellen geschützt, um Sessions zu verifizieren und bei Bedarf mit Attributen aus dem lokalen IdM für eine anwendungsunterstützende Autorisierung anzureichern. Die Sessions für das Service-Portal werden mittels J2EE Policy Agent geschützt.

Das Produkt OpenAM unterscheidet dabei grundsätzlich zwischen sog. Profil-Attributen und Session-Attributen. Die Profil-Attribute sind im Gegensatz zu Session-Attributen im Zeitablauf nicht änderbar. Profil-Attribute kommen notwendigerweise aus dem lokalen IdM-System der TU Dortmund, das zur Authentifizierung bei der Nutzung lokaler Dienste eingesetzt wird.

Da bei der SAML-basierten Authentifizierung nicht das lokale IdM-System der TU Dortmund befragt wird, müssen konsequenterweise Session-Attribute eingesetzt werden. Daher muss für die föderative Dienstnutzung eine separate Authentifizierungskonfiguration im OpenAM erstellt werden.

Falls ein Zugriff eines Nutzers der TU Dortmund auf das Service-Portals der TU Dortmund via SAML und nicht via SSO-Session stattfindet, dann müssen per LDAP-Anfrage die vorhandenen Attribute aus dem IdM ausgelesen werden. Die Attribute der SAML-Assertions, die vom Heimat-IdP ausgestellt werden sind für die Autorisierung lokaler Nutzer nicht hinreichend.

3.2 Konfiguration des Identity Providers an der TU Dortmund

Der Identityprovider der TU Dortmund basiert aktuell auf dem Produkt des Shibboleth Konsortiums. Dieser IdP ist in den Metadaten der DFN AAI gelistet. Zur Authentisierung nutzt der IdP das IdM der TU Dortmund. Da das Produkt OpenAM auch als SAML-fähiger IdP agieren kann, wird der Shibboleth-basierte IdP mittelfristig durch das Produkt OpenAM in dieser Rolle ersetzt. Hierzu mussten zwei Erweiterungen für den OpenAM entwickelt werden:

1. Wenn ein Anwender im Rahmen der DFN AAI das erste mal einen externen Dienst nutzen möchte und dabei Daten von seiner Heimateinrichtung zum SP übertragen werden, dann wird hierfür seine Zustimmung webbasiert abgefragt und in einer

Datenbank hinterlegt. Dazu nutzt die TU Dortmund das uApprove Plugin für das Shibboleth Produkt. Dieses Plugin wurde im Rahmen dieses Projekts auf das Produkt OpenAM portiert, wobei die Datenbank-Struktur erhalten werden konnte.

2. Weiterhin ist es in einigen Fällen notwendig, die Attributwerte die der IdP aus dem IdM erhält, zu manipulieren bevor sie in eine SAML Assertion geschrieben werden. Dies umfasst:
    - die Filterung der Attributwerte
      z.B. sollen nur Email Adressen aus bestimmten Domains per SAML übermittelt werden, auch wenn aus Kompatibilitätsgründen andere Domains mitgepflegt werden müssen
    - die Erweiterung der Attributwerte um feste Strings:
      beispielsweise wird das Attribute eduPersonAffiliation um den Einrichtungsnamen erweitert; aus “student“ wird damit “student@TU-Dortmund“
    - konstante Strings als Wert:
      z.B. wird der Name der Einrichtung als fester String in einigen Fällen in der SAML erwartet, obwohl er so nicht im LDAP hinterlegt ist

Um diese Funktionalität nachzubilden, wurde der OpenAM so erweitert, dass die Attribute durch serverseitige Skripte entsprechend angepasst werden. Dazu wird die Javascript-Umgebung der JVM genutzt. Die Skripte können für jeden SP einzeln festgelegt werden.

3.3 Vorbereitungsschritte für die Teststellung

Der Vorbereitungsschritt für die Teststellung des Verfahrens, bei der UA Ruhr Studierende der Universitäten Duisburg-Essen und Bochum die Bibliotheksdienste der TU Dortmund nutzen können, umfasste folgende, einmalige Vorbereitungsschritte, die auch für andere Dienste wiederverwendet werden können:

- Konfiguration der SAML-Schicht an allen beteiligten UA-Ruhr IdPs gemäß Attributspezifikation
- Installation des uApprove Plugins bei IdPs: Mit diesem Modul wird die Zustimmung des Anwenders für die Weitergabe seiner Identitätsdaten vom IdP an SP erfragt und dauerhaft gespeichert
- Aufbau einer Subföderation innerhalb der DFN AAI
- Aufbau eines Discovery-Service
- Konfiguration des OpenAM als SAML SP: Erweiterung des SSO der TU Dortmund um SAML-initiierte Sessions
- Verwendung der XSLNP-Schnittstelle beim Zugriff auf das Bibliothekssystem SISIS-Sunrise über eine von der TU Dortmund programmierte Webanwendung, die im Service-Portal implementiert worden ist

3.4 Zugriff auf Webdienste des Bibliothekssystems der TU Dortmund

Wie bereits dargestellt, erfolgt der Zugriff auf die Dienstes des Bibliothekssystems der TU Dortmund über das Service-Portal. Sofern der Anwender auf die geschützten Dienste des Portals zugreifen möchte, dann prüft das Login-Modul des Portals, ob eine gültige SSO-Session vorhanden ist. Existiert keine solche Session, dann findet der Anwender einen Login-Button vor.

Abbildung 4: Erstzugriff auf das Service-Portal ohne Login-Session

Über diesen Login-Button gelangt der Anwender zu der Web-Oberfläche des zentralen SSO-Dienstes der TU Dortmund, der drei unterschiedliche Login-Methoden bereithält:

- TU-Angehörige haben die Möglichkeit sich entweder durch die Eingabe ihrer Uni-Account Daten anzumelden oder mittels ihrer UniCard und der darauf gespeicherten Zertifikate. In beiden Fällen werden die entsprechenden Profil-Attribute für die Autorisierung vom lokalen IdM System geliefert
- Angehörige von Hochschulen, die der DiepRuR Föderation beigetreten sind, autorisieren sich über die Option “Login mit Föderation“

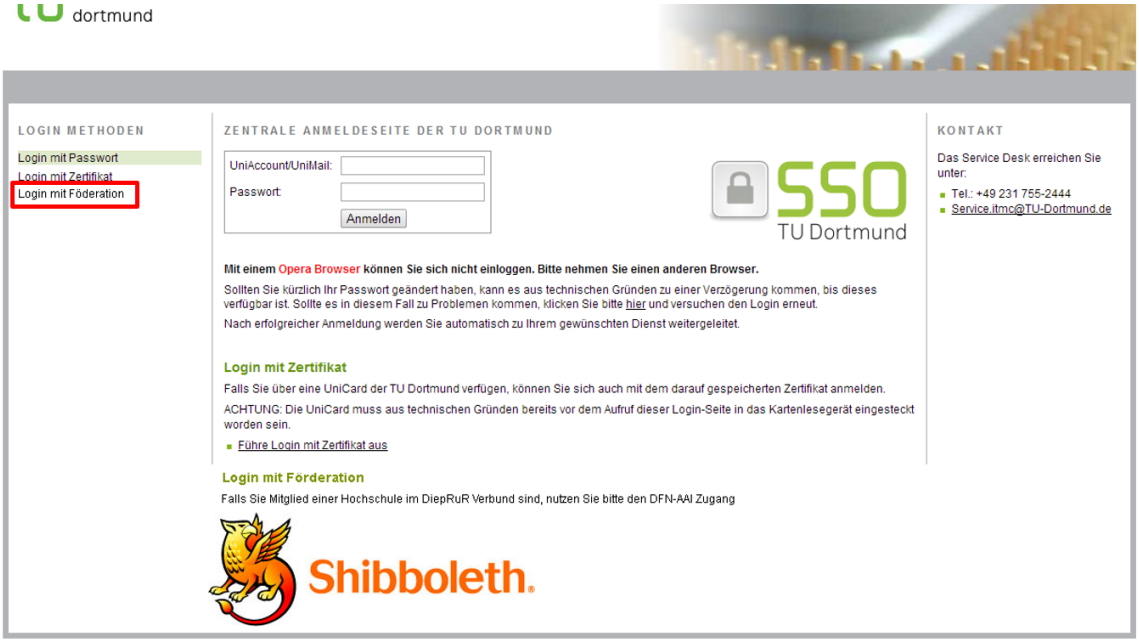

Abbildung 5: Weboberfläche des SSO-Dienstes (gleichzeitig auch Service-Provider) an der TU Dortmund

Bei der Auswahl der Option “Login mit Föderation“ gelangt der Anwender zum Dicovery-Service der DiepRuR Föderation, der über die DFN AAI zentral betrieben wird. Der Dienst beinhaltet eine Liste mit allen IdPs, die der Föderation angehören.

Abbildung 6: Weboberfläche des Discovery-Service mit Auswahlliste der Heimatorganisationen

Aus dieser Liste wählt der Anwender seine Heimatorganisation aus und wird anschließend zu dem für ihn zuständigen Identity Provider weitergeleitet. Der Discovery-Service beinhaltet nur Weiterleitungsadressen der IdPs teilnehmender Föderationspartner, die u.a. in der Whitelist gepflegt werden. Als Beispiel dient hier die Authentifizierung am IdP der Ruhr-Universität Bochum:

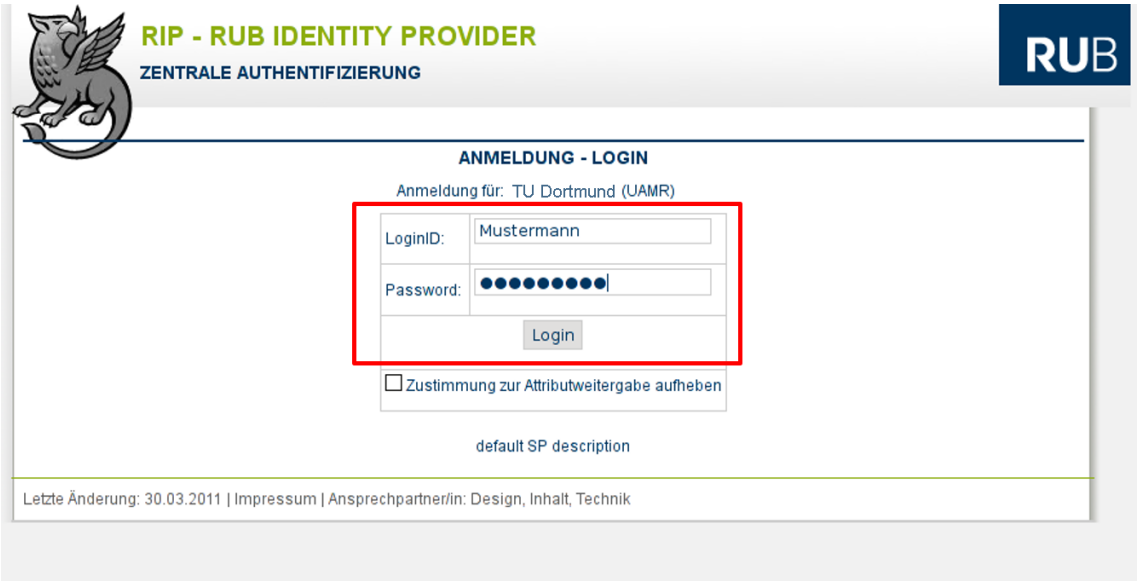

Abbildung 7: Login-Maske des Identity-Providers an der Ruhr-Universität Bochum

Nach einer erfolgreichen Authentifizierung wird zunächst die Einwilligung des Benutzers für die Datenweitergabe an den SP mittels uApprove-Plugin eingeholt.

Wie hierbei auf dem Schaubild zu erkennen ist, wird bei diesem Vorgang der User nicht nur über die anstehende Übertragung von Identitätsdaten in Kenntnis gesetzt, sondern er bekommt auch die Daten angezeigt, die der IdP seiner Heimateinrichtung für ihn aktuell bereitstellt und an den entsprechenden ServiceProvider (bei Zustimmung des Users) überträgt.

Abbildung 8: Weboberfläche des uApprove-Plugins für Zustimmungsverfahren bei der Datenweitergabe am Bochumer IdP

Auch hier bekommt der Anwender im Vorfeld die Möglichkeit den Vorgang entweder abzubrechen sofern er mit der Übermittlung nicht einverstanden ist oder aber der Übertragung dauerhaft zuzustimmen, wodurch diese Abfrage nicht jedes Mal beim Zugriff auf das Service-Portal der TU Dortmund erforderlich wird. Bis zu diesem Zeitpunkt des Zustimmungsverfahrens sind noch keine Identitätsdaten vom IdP an den SP übertragen worden.

Falls der Benutzer der Datenweitergabe an den SP zustimmt, erfolgt im nächsten Schritt eine automatische Weiterleitung wieder zurück zum SP der TU Dortmund. Wie bereits dargestellt, ist der SP im zentralen SSO-Dienst (OpenAM) der TU Dortmund implementiert. Dieser Prüft nun die gelieferten SAML-Assertions und erzeugt anschließend eine Session mit Weiterleitung zum Service-Portal.

Im Service-Portal wird gemäß der in der Session enthaltenen Attribute der Autorisierungsschritt durchgeführt. Dabei wird gleichzeitig geprüft, ob im Bibliothekssystem ein entsprechendes Benutzerkonto vorhanden ist.

Falls noch kein Benutzerkonto vorhanden ist, dann wird dem Benutzer über einen Self-Service die Erzeugung eines Kontos ermöglicht. Hierzu wird in der Navigation auch ein entsprechender Menüeintrag angeboten.

Dieser Self-Service zeigt dem Anwender zunächst alle Identitätsattribute an, die zu diesem Zeitpunkt im Service-Portal über die gültige Session vorliegen und auf deren Grundlage das Benutzerkonto erzeugt werden kann. Für die Erzeugung des Benutzerkontos muss die Datenschutzerklärung der TU Dortmund sowie die Nutzungsbedingungen der Bibliothek akzeptiert werden.

Abbildung 9: Self-Service zum Erzeugen eines neuen Benutzerkontos im Service-Portal der TU Dortmund

Bestätigt der Anwender diese Erklärungen, dann wird ein entsprechendes Benutzerkonto im Bibliothekssystem der TU Dortmund erzeugt. Im Anschluss daran kann der Dienst der Bibliothek auch sofort webbasiert genutzt werden bzw. Bücher können über den eigenen Universitätsausweis entliehen werden.

Nach der Kontoerzeugung können die Webdienste der Bibliothek im Service-Portal in Anspruch genommen werden, um beispielsweise eigene Profil- und Vorgangsdaten oder den aktuellen Gebührenstand anzuzeigen.

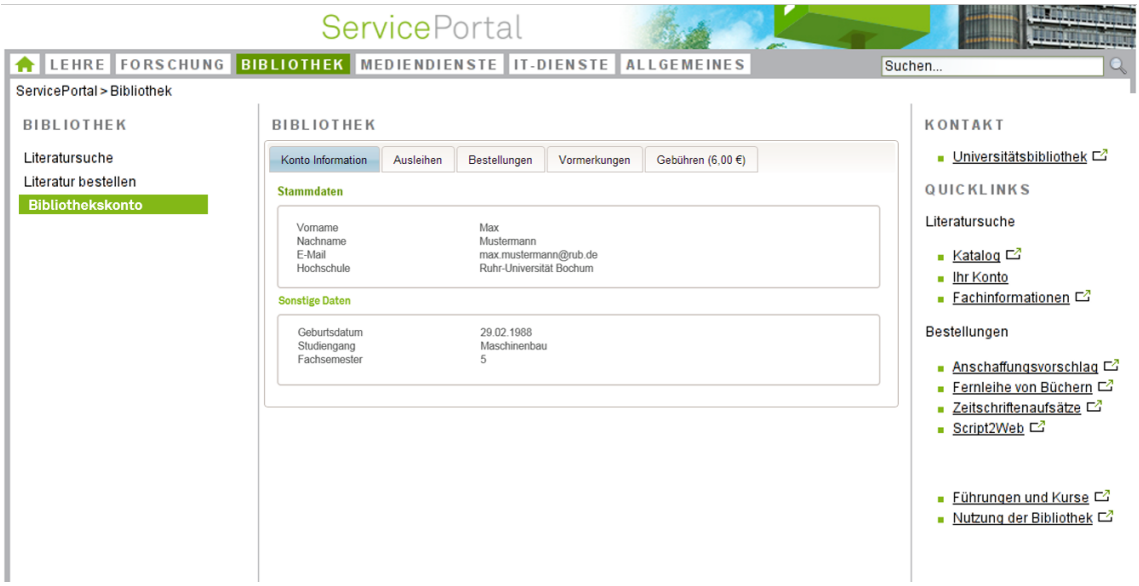

Abbildung 10 a: Anzeige von Profildaten zum via SAML verknüpften Benutzerkonto im Dortmunder Bibliothekssystem

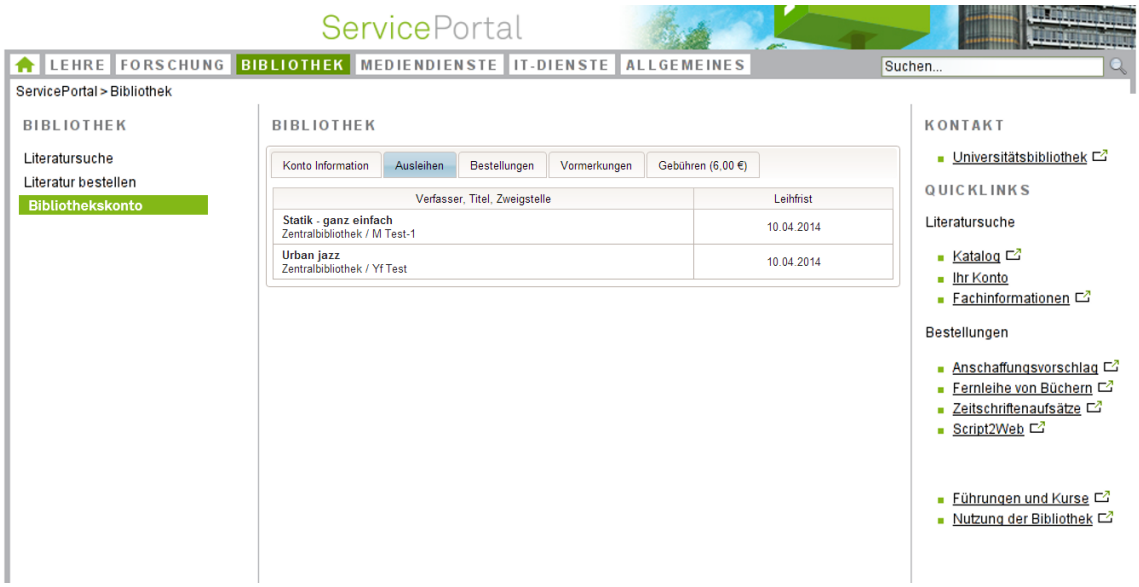

Abbildung 10 b: Auszug aktueller Vorgangsdaten eines Benutzerkontos aus dem Dortmunder Bibliothekssystem

4 Fazit

Mit diesem Projekt wurde ein entscheidender Beitrag dazu geliefert, eine SAML-basierte Föderation in der Ruhr-Region aufzubauen, die eine organisationsübergreifende Nutzung von webbasierten Diensten einfach und effektiv ermöglicht. Im Rahmen dieses Projekts sind unterschiedliche Implementierungsvarianten geschaffen worden, die sowohl OpenAM

als auch Shibboleth-basierte Systeme unterstützen. Ein entsprechender Mechanismus zur Steuerung der Vertrauensbeziehung zwischen Identitäts- und Serviceprovidern bei der Durchführung identitätsbezogener Vorgänge ist ebenfalls implementiert worden.

Weiterhin wurden auch technische Möglichkeiten hervorgehoben, die beim DiepRuR Verfahren zum Zweck der Einhaltung datenschutzrechtlicher Bestimmungen implementiert worden sind, so dass die gewählte Technologie als datenschutzfreundlich eingestuft werden kann.

Die Einfachheit des Verfahrens und seiner Anwendung auf bereits vorhandene Systeme zeigt, wie klein die Hürde für einen Föderationsbeitritt ausfällt. Daher wird das Interesse von anderen Hochschulen aus der Ruhr-Region bzw. Nordrheinwestfalens der Föderation mit eigenen Diensten beizutreten begrüßt, um das Dienstleistungsportfolio auf Grundlage dieser Föderation stetig auszuweiten.

Weitere Materialien

PowerPoint zum Thema „DiepRuR - ein Kooperationsprojekt der Hochschulen in der Ruhr-Region“ im Rahmen der CampusSource Tagung am 10.04.2014 an der FernUniversität in Hagen.