eduGAIN verbindet Föderationen

Torsten Kersting, Jürgen Rauschenbach

DFN-Verein
GS-Berlin
Stresemannstr. 78
10963 Berlin
kersting@dfn.de
jrau@dfn.de

Abstract: Ein Grossteil der europäischen Forschungsnetze verfügt bereits über eigene Authentifizierungs- und Autorisierungs-Infrastrukturen oder baut diese gerade auf, um so zum einen den Angehörigen dieser Netze einen komfortablen Zugang zu geschützten Ressourcen zu ermöglichen und zum anderen um Anbietern von Ressourcen eine komfortable Zugriffsverwaltung zu bieten. Innerhalb der Forschungsnetzcommunity werden diese Infrastrukturen auf nationaler Ebene in so genannten Föderationen organisiert. Im Umfeld des von der EU geförderten GN2-Projektes wurde das im folgenden beschriebene Konzept „eduGAIN" entwickelt, das bereits existierende Authentifizierungs- und Autorisierungs-Infrastrukturen der nationalen Forschungsnetze integrativ, in einer so genannten Konföderation, so organisiert, dass die Nutzer einzelner Föderationen auch Ressourcen anderer Föderationen nach vergleichbaren Regeln nutzen können.

1 Einleitung

Hochschulen und Forschungseinrichtungen verfügen über eine Vielzahl geschützter Ressourcen, auf die unter festgelegten Bedingungen zugegriffen werden darf. Zum Beispiel sollen Mitarbeiter und Studierende einer bestimmten Hochschule im Rahmen einer speziellen Lizenzvereinbarung auf Fachinformation zugreifen können oder ein eLearning-System ausschließlich von BWL-Studenten genutzt werden können.
Um den Zugriff auf diese geschützten Ressourcen für die involvierten Teilnehmer zu verbessern und zu vereinfachen, ist eine Authentifizierungs- (Wer greift zu?) und Autorisierungs- (Worauf darf er zugreifen) Infrastruktur (AAI) hilfreich. Den Nutzern soll der Zugriff unabhängig vom Ort und dem Zugriffsweg ermöglicht werden und der Zugriff auf mehrere Anbieter von Ressourcen soll möglichst nach nur einmaliger Authentifizierung erfolgen. Für die Anbieter der Ressourcen soll der Schutz vor unberechtigtem Zugriff mit möglichst geringem Aufwand realisiert werden. Für die Einrichtungen soll der berechtigte Zugriff ihrer Nutzer mit möglichst geringem Aufwand umgesetzt werden.

Grundlage für eine solche Infrastruktur ist ein Identity Management System (IDM), über das die Identitäten der Nutzer mit ihren Attributen verwaltet werden. Anhand dieser Attribute, wie z.B. der Rolle innerhalb einer Einrichtung, den besonderen Befugnissen, dem Status, fällt der an das AAI System angeschlossene Service Provider seine Autorisierungsentscheidungen. Dieses Identity Management System muss daher sehr vertrauenswürdig sein, d.h. die bereitgestellte Information muss aktuell, korrekt und sicher vor Manipulationen sein.
Eine AAI besteht üblicherweise aus drei Hauptkomponenten, dem Identity Provider, dem Service Provider und einer WAYF (Where are You From) Komponente. Der Identity Provider stellt auf Anfrage die Attribute zu bestimmten Identitäten bereit, diese bekommt er aus dem Identity Management System; der Service Provider kontrolliert den Zugriff auf Ressourcen; der WAYF dient zur Lokalisierung des zu verwendenden Identity Providers.
Um Ressourcen nicht nur innerhalb einer sondern mehrerer Einrichtungen nutzen zu können müssen die einzelnen AAI Systeme der Einrichtungen kompatibel zusammengeschlossen werden. Dieser Zusammenschluss wird als Föderation bezeichnet.
Innerhalb einer solchen Föderation, wie beispielsweise der DFN-AAI, wird die kompatible Nutzung üblicherweise durch die Einigung auf Nutzung einer einheitlichen Software realisiert, im Fall von DFN-AAI ist dies Shibboleth. Folgendes Beispiel sowie Abbildung 1 sollen dies verdeutlichen:
Ein Nutzer dessen digitale Identität bei einem Identity Provider seiner Einrichtung gespeichert ist, versucht auf Ressourcen einer anderen Einrichtung zuzugreifen (1). Der Service Provider, der diese Ressource schützt, stellt nun fest, dass der Nutzer noch nicht bekannt ist und fordert ihn auf sich zu authentifizieren. Hierzu wird er an den in einer Föderation zentralen WAYF weitergeleitet (2), diesem WAYF sind alle Teilnehmer-Organisationen der Föderation mit all ihren Service- und Identity Providern bekannt. Er wird dort aufgefordert den Identity Provider auszuwählen, bei dem seine Identität verwaltet wird, woraufhin er an genau diesen weitergeleitet wird (3). Der Nutzer meldet sich mit einem von der eigenen Einrichtung festgelegten Verfahren an, üblicherweise Nutzername und Passwort (4), und wird nach erfolgreicher Authentifizierung zurück an den Service Provider geleitet, auf dessen Ressourcen er zugreifen möchte (5). Zusammen mit der Weiterleitung an diesen Service Provider werden diverse Attribute, seine Person bestimmend, übertragen. Anhand dieser Attribute ist der Service Provider nun in der Lage eine Autorisierungsentscheidung zu fällen (6). Für weitere Grundlagen zu AAI siehe [EC07] sowie [LOP04]

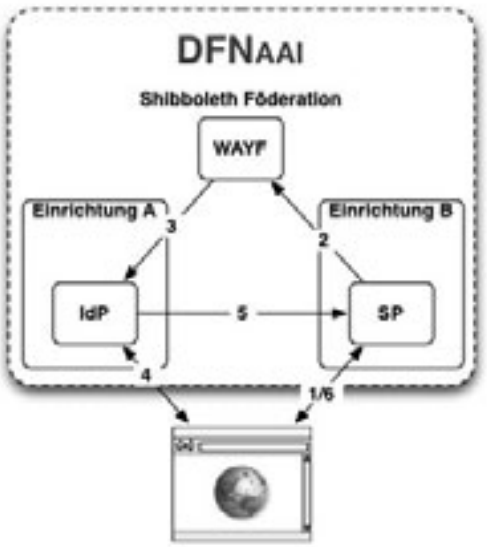

Bild 1: Föderation

Wenn auf Ressourcen außerhalb der eigenen Föderation zugegriffen werden soll, stößt das Konzept der Föderation an seine Grenzen. Der Service Provider oder der zu verwendende Identity Provider sind dem WAYF der eigenen Föderation nicht bekannt und die Software zum Aufbau der AAI innerhalb der anderen Föderation ist im allgemeinen nicht mit der Software der eigenen Föderation kompatibel. Dies kann sowohl die Art der Identitätsverwaltung, die semantische Bedeutung der Attribute als auch das verwendete Nachrichtenprotokoll betreffen.
Um derartige Grenzen zu überwinden werden in eduGAIN verschiedene Föderationen zusammengeschlossen. Dieser Zusammenschluss wird als Konföderation bezeichnet. eduGain stellt die nachfolgend beschriebenen Elemente bereit, die notwendig sind, um unterschiedliche Föderationen zu einer Konföderation zusammen zu schließen und kompatibel untereinander nutzbar zu machen.

2 Architektur

Zielstellung bei der Entwicklung von eduGAIN war es, eine Architektur zu schaffen, die es gestattet, die Interoperabiliät zwischen bereits bestehenden als auch zukünftigen AAIs zu unterstützen ohne dass Eingriffe in diese nötig sind. Die Architektur besteht im Wesentlichen aus einem WFAYF (Which Federation Are You From), einem Metadaten Service sowie diverse Bridging Elemente. Beim WFAYF handelt es sich um eine Erweiterung des WAYF Konzeptes der Föderation, mit dem Unterschied, dass statt des Identity Providers, die Föderation in der dieser beheimatet ist ausgewählt wird und das die Informationen über alle teilnehmenden Entitäten nicht mehr von diesem selber sondern vom Metadaten Service verwaltet werden. Die Bridging Elemente bilden die Protokolle und die den Identity Providern zu Grunde liegenden Attributsschemata auf ein Konföderationsformat ab. Da dies für die Föderationen völlig transparent geschieht, sind keinerlei Eingriffe in diesen notwendig um an der Konföderation teilzunehmen. Folgendes Beispiel sowie Abbildung 2 sollen den geänderten Ablauf im Gegensatz zur Föderation verdeutlichen:
Im ersten Schritt versucht ein Nutzer mit seinem Browser auf eine Ressource außerhalb seiner eigenen Föderation zuzugreifen. Ein deutscher Student, dessen Heiminstitution an DFN-AAI angeschlossen ist, versucht beispielsweise auf ein spanisches, per PAPI (eine AAI Entwicklung aus Spanien) geschütztes, Wiki zuzugreifen (1). Da der spanische Service Provider über keine Authentifizierungsinformationen des Nutzers verfügt, der Nutzer somit also nicht bereits authentifiziert ist, wird dieser an den WAYF Service der PAPI Föderation weitergeleitet (2). Hier kann er nun auswählen, dass der Identity Provider, den er zur Authentifizierung benutzen möchte, aus einer anderen Föderation stammt und er per eduGAIN authentifiziert werden möchte. Daraufhin wird er an den WFAYF Service weitergeleitet, der im Remote Bridging Element beheimatet ist und wählt dort die Föderation aus in der sein Identity Provider beheimatet ist(3), dieser Schritt soll in einer späteren Entwicklungsstufe durch eine Abfrage des WFAYF beim Metadataservice (4) automatisiert ablaufen. Das Bridging Element nimmt die Auswahl der Föderation entgegen und bildet die lokalen Protokolle auf das eduGAIN Protokoll ab. Der Nutzer wird in an das Home Bridging Element weitergeleitet, wo das eduGAIN Protokoll wiederum in das lokale AAI Protokoll übersetzt wird (5), dieser Schritt erfolgt völlig transparent für den Nutzer. Nachdem dieser vom Home Bridging Element an den WAYF seiner Föderation weitergeleitet wurde (6), muss er nur noch seinen Identity Provider innerhalb der eigenen Föderation auswählen und kann sich nach einer Weiterleitung an diesen (7) dort authentifizieren (8). Je nach verwendeter AAI wird nun beispielsweise lediglich ein so genanntes Handle, das ist eine anonymisierte Referenz auf den Nutzer anhand derer weitere Attribute abgefragt werden können, oder bereits eine komplette Liste von Attributen an den spanischen Service Provider übertragen. Diese laufen dabei ebenfalls über die beiden involvierten Bridging Elemente und werden dort entsprechend abgebildet (lokal - eduGAIN - lokal) (9, 10 und 11). Der Service Provider kann im letzten Schritt entscheiden, ob die erhaltenen Attribute ausreichen, um den Nutzer zu authentifizieren und autorisieren, und somit den Zugriff zu gewähren oder zu verweigern (12).

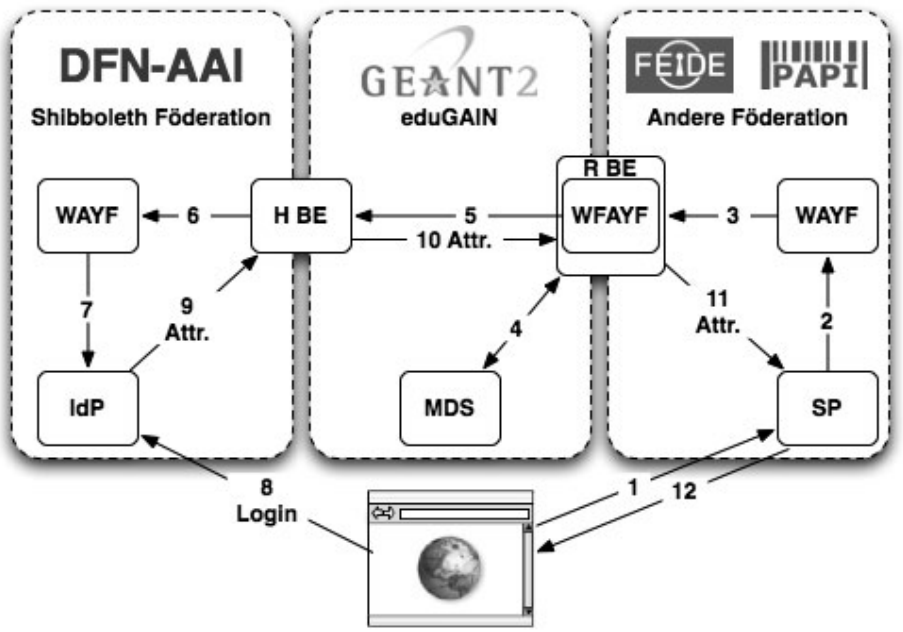

Bild 2: Konföderation (Ablauf der Authentifizierungs- und Autorisierungsschritte)

Nachfolgend werden die einzelnen Komponenten dieser Infrastruktur genauer erläutert:

2.1 Bridging Elemente

Die Bridging Elemente sind immer in die AAI-Systeme der teilnehmenden Föderationen integriert und dienen dazu, die Protokolle und Attributsschemata der lokalen Föderation auf das eduGAIN Format abzubilden. Daher ist für jede an eduGAIN angeschlossene AAI ein eigenes Bridging Element nötig. Aktuell sind diese für folgende AAI-Systeme vorhanden: Shibboleth, A-Select, PAPI und simpleSAMLphp. Da alle verwendeten Protokolle und Attributsschemata offen liegen, ist es durchaus möglich, ein eigenes Bridging Element zu entwickeln, um eine AAI in eduGAIN zu integrieren, die aktuell noch nicht unterstützt wird. Weiterhin publizieren und aktualisieren die Bridging Elemente die Metadaten der Föderation beim Metadata Service. Um eine unrechtmäßige Manipulation der Metadaten zu verhindern, müssen sich die Bridging Elemente gegenüber dem Metadata Service mit Zertifikaten ausweisen. Dieses Zertifikate werden von der zu diesem Zweck gegründeten eduGAIN CA (s.u.) ausgestellt.

2.2 WFAYF

Der WFAYF ist eigentlich ein Provisorium im aktuellen Entwicklungsstand von eduGAIN und kein Bestandteil der finalen Architektur. Er greift, wie bereits erwähnt, das Konzept des WAYF aus der Föderation auf mit dem Unterschied dass statt des Identity Providers selber, die Föderation ausgewählt wird in der dieser beheimatet ist. Diese Auswahl soll in einem späteren Entwicklungsstadium von den Bridging Elementen automatisiert vorgenommen werden, die dazu auf die Metadaten des Metadata Service zurück greifen, daher ist der WFAYF aktuell auch funktional in die Bridging Elemente integriert.

2.3 Metadata Service

Der Metadata Service verwaltet an zentraler Stelle in der Konföderation die Metadaten aller teilnehmenden Föderationen. Diese Metadaten beschreiben alle existierenden AAI Komponenten der Teilnehmer, wie Identity Provider, Service Provider, eingesetzte WAYFs und zugehörige Zertifikate. Jede Föderation ist selber für die Aktualität und Korrektheit dieser Daten verantwortlich. Um dies komfortabel zu gewährleisten können, werden die Metadaten von autorisierten Bridging Elementen automatisiert beim Metadata Service publiziert.
Die Metadaten werden hauptsächlich benötigt, damit sich kommunizierende Komponenten eindeutig Identifizieren können.

2.4 Protokoll

Sämtliche Kommunikation zwischen eduGAIN-Komponenten wird über einen sicheren Kanal mit gegenseitiger Authentifizierung auf der Basis von Zertifikaten durchgeführt. Die Zertifikate werden unter Verwendung der Komponenten-Identifikatoren gebildet, die in einem einheitlichen Namensraum (urn:geant:edugain) erfasst sind. Auf diese Weise ist jede Komponente der Infrastruktur nach dem Empfang einer Anfrage oder Antwort in der Lage, zum einen die Gültigkeit des Zertifikats zu überprüfen, die von der Gegenstelle präsentiert wurde (Vertrauenskette, Widerrufliste, etc) und zum anderen kann anhand der Werte in diesen Zertifikaten entschieden werden ob die Gegenstelle für die beabsichtigte Interaktion akzeptabel ist.
Um Authentifizierungs- und Autorisierungsinteraktionen auszuführen ist die Security Assertion Mark-up Language (SAML) in Kombination mit dem Transport über einen abgesicherten Kanal weit verbreitet und enthält bereits große Teile der erforderlichen Funktionalität [SAML20]. Daher bestehen die Nachrichten, die in eduGAIN ausgetauscht werden, zu großen Teilen aus Variationen von SAML Nachrichten.

2.5 Attributsschema

eduGAIN verwendet die Attributsschemata eduPerson [EDUCAUSE] sowie SCHAC [SCHAC], d.h. alle innerhalb von Föderationen verwendeten Attributsschemata, wie beispielsweise swissEduPerson in der SWiTCH-AAI, werden auf diese abgebildet sobald Föderationsgrenzen überschritten werden.

2.5 eduGAIN CA

In den meisten teilnehmenden Forschungsnetzen existieren bereits eigene Certificate Authorities (CAs), diese verwenden fast alle unterschiedliche Wurzelzertifikate. Damit die Vertrauenskette der verwendeten Zertifikate zu einem einzigen Wurzelzertifikat zurück verfolgt werden kann und um auch den Forschungsnetzen ohne eigene CA eine Teilnahme zu ermöglichen, wird innerhalb von eduGAIN eine eigene CA aufgebaut. Diese soll die Wurzelverzeichnisse der NREN CAs signieren können um so parallel zu diesen zu existieren oder selber Zertifikate ausstellen können. Die Certificate Authority befindet sich zur Zeit im Aufbau und wird vom spanischen Forschungsnetz betrieben, Zertifikate können bereits zu Testzwecken über ein Webfrontend[1] beantragt werden

2.6 Policy

Um die Verhältnisse zwischen den teilnehmenden Identity- und Service Providern auf eine sichere rechtliche Basis zu stellen wird in naher Zukunft eine eduGAIN Policy entwickelt werden. Für die Identity Provider geht es dabei um den Umgang mit den nutzerbezogenen Daten, für die Service Provider sind lizenzrechtliche Fragen von belang.

3 Pilotinstallation

Das Projekt betreibt aktuell eine Pilotinstallation, welche bereits mehrere Föderationen verbindet. Angeschlossen sind die AAI-Systeme folgender Forschungsnetze: per Shibboleth DFN, SWITCH, HUNGARNET und GRNET, per simpleSAMLphp UNINETT und RESTENA, über A-Select SURFnet, RedIRIS durch PAPI, und CARNet mit einer auf Radius basierenden Eigenentwicklung. Damit ist das oben beschriebene Szenario bereits umsetzbar.
Eine Teilnahme weiterer AAI-Systeme aus Forschungsnetzen am Testbed ist jederzeit problemlos möglich, Bridging Elemente für alle genannten AAIs sind auf den entsprechenden Software-Servern des Projektes erhältlich.
Um die Infrastruktur zu verwalten und erweitern, ist eine enge Zusammenarbeit mit den anderen Teilnehmern sehr erwünscht. eduGAIN ist ein Gemeinschaftsprojekt und auf breite Unterstützung angewiesen. Sämtliche Dokumentation und Software ist auf dem eduGAIN Wiki zu finden [JRA5WIKI].

[1] http://pki.edugain.org/

Ein zentraler gemeinsamer Géant Identity Provider (GIdP) wurde im eduGAIN Verbund geschaffen, um Nutzern, die in ihrer Heimateinrichtung noch keine etablierte AAI haben, die Nutzung entsprechend geschützter Ressourcen zu ermöglichen. Jeder GÉANT2-Mitarbeiter kann über den GIdP-Administrator in der Umgebung seines Forschungsnetzes eine digitale Identität beantragen, um ohne große Verzögerung eduGAIN nutzen zu können. Der GIdP wurde bereits erfolgreich getestet und wird demnächst offiziell in Produktion gehen, es wird davon ausgegangen, dass er als Interimslösung überflüssig wird, sobald alle Forschungsnetze mit eduGAIN verbunden sind und forschungsnetzweite AAI Lösungen eine ausreichende Durchdringung erreicht haben.

Literaturverzeichnis

[AAI] Authentication and Authorisation Infrastructure (AAI), http://de.wikipedia.org/wiki/Authentication_and_Authorization_Infrastructure

[DJ5.2.2,2] Geant2 Authorisation and Authentication Infrastructure (AAI) Architecture – second edition, http://www.dante.net/upload/pdf/GN2-07-024-DJ5-2-2-2-GEANT2_AAI_Architecture_And_Design.pdf

[DJ5.2.3,2] Best Practice Guide – AAI Cookbook – Second Edition, http://www.dante.net/upload/pdf/GN2-07-023v4-DJ5-2-3_2_Best_Practice_Guide-AAI_Cookbook-Second_Edition.pdf

[EC07] C. Eckert, IT-Sicherheit – Konzepte, Verfahren, Protokolle; Oldenburg, 2007 ISBN-10: 3486582704, ISBN-13: 978-3486582703

[EDUCAUSE] The EDUCAUSE/Internet2 eduPerson task force, http://www.educause.edu/eduperson/

[JRA5WIKI] JRA5 Wiki zur Zusammenarbeit aller Geant2 JRA5 Teilnehmer http://www.rediris.es/jra5wiki/

[LOP04] J. Lopez, R. Oppliger, and G. Pernul, "Authentication and Authorization Infrastructures (AAIs): A Comparative Survey," Computers & Security, vol. 23, pp.578-590, Elsevier, October 2004.

[SAML20] S. Cantor et al. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0 OASIS Standard, März 2005 http://doc.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SCHAC] J Masa (Editor). SCHAC Attribute Definitions for Individual Data, Mai 2006 http://www.terena.nl/activities/tf-emc/docs/schac/schac-schema-IAD-rel1.pdf