Kommunikation in Verteilten Systemen (KiVS),
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bd. P-61, S. 65–72,2005

Federated Identity Management: Die Notwendigkeit zentraler Koordinationsdienste

Wolfgang Hommel
Munich Network Management Team
Leibniz-Rechenzentrum München
hommel@lrz.de

Helmut Reiser
Munich Network Management Team
Ludwig-Maximilians–
Universität München (LMU)
reiser@nm.ifi.lmu.de

Abstract:
Identity & Access Management (I&AM) Systeme bilden eine moderne Basis für die organisationsinterne Verwaltung von Mitarbeitern und Kunden sowie deren Zugriff auf lokale Ressourcen. Ihr Wirkungsbereich endet allerdings an den Organisationsgrenzen. Im Rahmen von B2B-Szenarien, beispielsweise beim Supply Chain Management, wächst jedoch der Bedarf, auch die Accounts und Rechte der Mitarbeiter und Kunden von Partnerunternehmen effizient verwalten zu können, d.h. diese Organisationsgrenzen zu überschreiten.
Die zentrale Idee des *Federated Identity Managements* (FIM) ist, die Partnerunternehmen als autoritative Quelle für die Identitätsinformationen zu nutzen und die damit zusammenhängenden Management–Aufgaben an diese zu delegieren.
In diesem Artikel zeigen wir, dass die drei derzeit fortgeschrittensten FIM-Ansätze – SAML, Liberty Alliance und WS-Federation – mehrere methodische und funktionale Defizite aufweisen, die einen effizienten Aufbau von FIM-Szenarien in der Praxis erschweren. Als Lösung eines Teils dieser Probleme stellen wir einen *zentralen Koordinationsdienst* für Identitätsföderationen vor, der im Rahmen unserer Forschung prototypisch implementiert wird.

1 Motivation

Die Kernaufgabe des *Identity & Access Managements* (I&AM) ist die zentrale Verwaltung von Daten über Mitarbeiter, Kunden, Partner und Gäste sowie deren Zugangsberechtigungen zu den eigenen Systemen. Die effiziente Speicherung dieser Daten wird von *Verzeichnisdiensten*, beispielsweise auf Basis von LDAP-Servern, ermöglicht. *Meta-Directories* sorgen für den Abgleich der Datenbestände zwischen verschiedensten Datenquellen und -abnehmern und so genannte *Provisioning-Systeme* übernehmen die Umsetzung von Geschäftsprozessen des Benutzer–Managements. Sie sorgen beispielsweise dafür, dass neuen Mitarbeitern automatisch und termingerecht Accounts auf allen benötigten Systemen eingerichtet und beim Ausscheiden auch wieder entzogen werden.

I&AM-Systeme konzentrieren sich auf die Beherrschung der organisationsinternen Komplexität, z.B. hinsichtlich der Anbindung von Datenquellen, die über keine standardisierten

Schnittstellen wie LDAP verfügen und in Bezug auf die Konvertierung der Daten in die von den angeschlossenen Systemen und Diensten benötigten Formate.

Letztendlich kann eine herkömmliche I&AM-Lösung aber keine Systeme außerhalb der Grenzen der sie einsetzenden Organisation abdecken. Müssen Identitäts- und Autorisierungsdaten *über Organisationsgrenzen hinweg* ausgetauscht werden, wie es zum Beispiel bei firmenübergreifenden Projekten, im Supply Chain Management oder beim Outsourcing von Diensten der Fall ist, so spricht man von *Federated Identity Management* (FIM). FIM soll gewährleisten, dass ein Parterunternehmen, das als *Service Provider* agiert, über dedizierte Protokolle Zugriff auf die unter anderem zur Authentifizierung, Autorisierung und Abrechnung notwendigen Benutzer-Daten erhält. Die Daten müssen dann nur noch vom so genannten *Identitätsprovider* gespeichert und gepflegt werden.

Mit der *Security Assertion Markup Language* [SAM], den Spezifikationen der *Liberty Alliance* [Lib] und den Entwürfen zur *Web Services Federation Language* [KN03] existieren drei fortgeschrittene Ansätze für FIM. Allerdings weisen sie einige methodische und funktionale Defizite auf, die den schnellen Aufbau und die effiziente Wartung von FIM-Systemen in der Praxis erschweren. Für einen Teil dieser Probleme schlagen wir als möglichen Lösungsansatz einen zentralen Koordinationsdienst vor.

Im folgenden Abschnitt fassen wir die FIM-Standards anhand eines Beispiels kurz zusammen. In Abschnitt 3 demonstrieren wir, dass alle drei Ansätze derzeit unter einigen elementaren Defiziten leiden. Als vielversprechende Lösung stellen wir in Abschnitt 4 einen *zentralen Koordinationsdienst* für Identitätsföderationen vor, dessen Spezifikation und prototypische Implementierung Gegenstand unserer aktuellen Forschungen ist.

2 Existierende Ansätze für Federated Identity Management

Die nachfolgend vorgestellten Ansätze haben den Begriff *Federated Identity Management* geprägt und verfolgen das Ziel, dem Anbieter eines Dienstes *zuverlässige* Informationen über einen Benutzer verfügbar zu machen, die – der Terminologie der Liberty Alliance folgend – bei einem *Identitätsprovider* gespeichert sind.

Diese benutzerspezifischen Daten klassifizieren wir in Anlehnung an SAML grob wie folgt:

- *Identitäts- und Authentifizierungsdaten*: Der Identitätsprovider übernimmt die Authentifizierung des Benutzers und bürgt dem Service Provider gegenüber für diesen. Vertraut der Service Provider dem Identitätsprovider, so kann eine erneute Authentifizierung des Benutzers bei dessen Zugriff auf die Dienste des Service Providers entfallen – man erreicht ein organisationsübergreifendes *Single Sign-On*.
- *Autorisierungsdaten*: Sofern ein Identitätsprovider – im Sinne von *Distributed Access Control* – auf die Rechte des Benutzers beim Service Provider Einfluss hat, kann er als *Policy Decision Point* agieren. Der Identitätsprovider teilt dem Service Provider also auf Anfrage *Zugriffskontrollentscheidungen* mit, die er auf Basis der Kombination lokal gespeicherter und optional vom Service Provider übermittelter Daten und Regeln trifft.

- *Allgemeine Attributsauskünfte*: In diese Kategorie fallen alle Daten, die für den Identitätsprovider nicht mit Authentifizierungs- oder Autorisierungsinformationen behaftet sind. Sie können beim Service Provider aber wiederum für Autorisierungsentscheidungen verwendet werden oder sind anderweitig für die Erbringung der Dienstleistung notwendig. Ein Beispiel hierfür sind Informationen über die Rechnungsanschrift oder die Telefonnummer des Benutzers.

Die Funktionsweise der FIM-Ansätze wird anhand des folgenden Beispiels erläutert: Eine Firma hat ein Abkommen mit einer Mietwagengesellschaft, das den eigenen Mitarbeitern günstige Konditionen ermöglicht. Alle Mitarbeiter dürfen Kleinwagen mieten, aber nur einige ausgewählte auch Limousinen. Die Reservierung eines Wagens kann über eine Website der Mietwagengesellschaft durchgeführt werden, auf der Mitarbeiter der Firma ihre Stammdaten jedoch nie – auch bei der ersten Benutzung des Dienstes nicht – manuell angeben müssen; diese Angaben sollen vielmehr bei Bedarf automatisch übermittelt werden.

2.1 Security Assertion Markup Language (SAML)

Die *Security Assertion Markup Language (SAML)* [SAM] wird vom Security Services Technical Commitee der OASIS gepflegt, ist seit August 2003 in Version 1.1 standardisiert und definiert:

- Ein XML-basiertes Format für *Assertions*, welche die oben definierten Klassen benutzerspezifischer Daten enthalten. SAML unterscheidet zwischen *Authentication*, *Authorization* und *Attribute Assertions*. Diese Assertions werden vom Identitätsprovider an den Service Provider übermittelt. Herkunft und Integrität der Assertions werden mittels *digitaler Signaturen* sichergestellt.
- Ein *Request-Response-Protokoll*, mit dessen Hilfe beispielsweise ein Service Provider gezielt *Assertions* beim Identitätsprovider anfordern kann.
- Eine Methode, um Requests und Responses in SOAP Nachrichten zu verpacken (so genanntes *SAML Binding*).
- Diverse Varianten, um diese Nachrichten automatisiert entweder *direkt* oder *indirekt über den Benutzer*, beispielsweise HTTP-basiert mittels herkömmlicher Web-Browser, zwischen Identitätsprovider und Service Provider austauschen zu können (so genannte *SAML Profiles*).

Die Reservierung eines Mietwagens könnte beim Einsatz von SAML wie folgt ablaufen:

1. Der Mitarbeiter, der den Mietwagen reservieren möchte, loggt sich im Intranet seiner Firma ein, wobei er anhand eines Benutzernamens identifiziert und durch Überprüfung des zugehörigen Passworts authentifiziert wird.
2. Auf einer Intranet-Seite befindet sich ein spezieller Link auf die Website der Mietwagengesellschaft, der bei SAML *Inter-Site-Transfer-Service* genannt wird.
3. Ein Aufruf dieses Links führt auf die Website des Service Providers, wobei dessen SAML Komponente beispielsweise anhand eines Parameters im verwendeten URL

(so genannter SAML *Artifact*) mitgeteilt wird, bei welchem Identitätsprovider sie Auskünfte über diesen Benutzer einholen kann.

4. Der Service Provider nimmt mit dem Identitätsprovider Kontakt auf und erfährt anhand einer *Authentication Assertion*, dass es sich tatsächlich um einen Mitarbeiter der Firma handelt, der nicht erneut authentifiziert werden muss.
   Die für die Reservierung des Mietwagens notwendigen Daten wie der Name des Mitarbeiters und die Rechnungsanschrift können in Form einer oder mehrerer *Attribute Assertions* übermittelt werden.
   Sofern der Mitarbeiter eine Limousine statt eines Kleinwagens mieten möchte, kann der Service Provider eine entsprechende *Authorization Assertion* anfordern; der Identitätsprovider antwortet entsprechend mit einer positiven oder negativen Zugriffskontrollentscheidung.

SAML bietet zusätzlich diverse Schnittstellen für eigene Erweiterungen – so genannte *SAML Extensions*. Besonders interessant ist beispielsweise die Möglichkeit zur Verknüpfung von SAML mit der eXtensible Access Control Markup Language (XACML), um eine detaillierte Modellierung von Zugriffsberechtigungen zu ermöglichen [Le04].

2.2 Liberty Alliance

Die Liberty Alliance [Lib] ist ein seit Ende 2001 existierender Zusammenschluss von mittlerweile über 150 namhaften Unternehmen. Ihr Ziel ist die Entwicklung eines Standards für den Aufbau eines Federated Identity Managements und die interoperable Implementierung darauf aufbauender Dienste.

Von der Liberty Alliance werden folgende Komponenten spezifiziert:

1. Das *Identity Federation Framework* (ID-FF) regelt den Datenaustausch zwischen Identitätsprovider und Service Provider. Ursprünglich sollte SAML als Basis für dieses Framework dienen, was aufgrund vieler Modifikationen und Erweiterungen jedoch nur noch marginal erkennbar ist. Die bei der Spezifikation von ID-FF gemachten Erfahrungen fließen aber in die Entwicklung von SAML 2.0 ein.
2. Die *Services Interface Specifications* (ID-SIS) legen im Rahmen von *Profilen* Mengen von Attributen fest, in denen Daten über die Benutzer gespeichert werden sollen. Bislang existieren Entwürfe für das *Employee Profile* und das *Personal Profile*, wobei letzteres in Business-to-Customer-Szenarien zum Einsatz kommen soll.
3. Das *Web Services Framework* (ID-WSF) spezifiziert einen *Discovery Service* und legt Mechanismen für die Kommunikation zwischen dem Benutzer und seinem Identitätsprovider fest, wobei explizit auch auf mobile Endgeräte und deren eingeschränkte Rechen- sowie Speicherkapazität und graphische Darstellungsmöglichkeiten eingegangen wird.

Ein herausragendes Merkmal der Liberty Alliance ist die Berücksichtigung und Betonung von Datenschutz-Aspekten. Im Mietwagen-Beispiel wäre also explizit vorgesehen, dass der Mitarbeiter der Übertragung seiner Daten an die Mietwagengesellschaft in geeigneter Form zustimmen können muss. Auf Basis des *Employee Profiles* könnten die an die

Mietwagengesellschaft zu übermittelnden Attribute, beispielsweise Name, Abteilung und Rechnungsanschrift, vereinbart werden.

2.3 Web Services Federation Language (WS-Federation)

Die von IBM und Microsoft entworfene *Web Services Federation Language* [KN03] ergänzt eine Serie anderer Spezifikationen zum Thema Web Services und hängt auch stark von diesen ab, beispielsweise von WS-Security [Ka02] und WS-Trust [ABB04].

WS-Federation tauschte Nachrichten zwischen Identitätsprovider und Service Provider ursprünglich nicht in Form von Assertions aus, sondern erinnerte mehr an *Kerberos*: Dem Benutzer werden von seinem Identitätsprovider spezielle, digital signierte Zertifikate ausgestellt, die als *Secure Tokens* bezeichnet werden und ausgewählte Attribute (so genannte *Claims*) des Benutzers enthalten. Ein Token kann dann einem Service Provider vorgelegt werden, um Zugriff auf die gewünschten Ressourcen zu erhalten. Wenn ein Dienst Daten benötigt, die nicht im Token enthalten sind, beispielsweise eine Aussage über die Berechtigung zur Reservierung einer Limousine, so muss dem Benutzer von seinem Identitätsprovider ein neues Token ausgestellt werden. Die WS-Spezifikationen definieren den SAML Profiles ähnliche Protokolltechniken zur automatischen Anforderung neuer Tokens.

Erfreulicherweise erfolgten mittlerweile Erweiterungen, um auch *SAML Assertions* im Rahmen von WS-Federation verwenden zu können. Die Chancen auf interoperable Implementierungen von SAML, Liberty Alliance und WS-Federation steigen damit deutlich. Allerdings gibt es bislang nur für SAML vollständige Implementierungen, unter anderem auch als Open Source Software.

3 Defizite und Schwächen existierender Ansätze

Aufgrund der breiten Akzeptanz, die SAML gefunden hat, nähern sich alle FIM Ansätze mehr und mehr diesem Standard an. Allerdings teilen sie sich nicht nur Vor-, sondern auch diverse Nachteile.

Im Folgenden werden die fünf wichtigsten Nachteile vorgestellt, die den Aufbau und den laufenden Betrieb von Identitätsföderationen in der Praxis deutlich erschweren. In Abschnitt 4 zeigen wir mögliche Lösungswege für einen Teil dieser Probleme.

1. *Syntax und Semantik von Attributen*: Alle Ansätze bieten zwar die flexible Möglichkeit, beliebige Daten über einen Benutzer in Form von Attributen, d.h. Tupeln (Attributsname; Attributswert), auszutauschen. Sowohl hinsichtlich der Namensgebung als auch der Spezifikation von Syntax und Semantik der Attributswerte werden aber weder Richtlinien vorgegeben noch formale Methoden zur Verfügung gestellt. Einzig die Liberty Alliance definiert mit dem *Employee* und dem *Personal Profile* zwei Instanzen von Attributsdefinitionen; ihnen ist aber ihr Entwurfscharakter noch deutlich anzusehen und sie werden voraussichtlich – ähnlich diversen weit verbreiteten LDAP-Objektklassen – auch langfristig keinen universellen Verwendbarkeitsgrad

erreichen bzw. ohne anwendungsspezifische Ergänzungen auskommen. Es fehlt also eine Unterstützung für die Erarbeitung eines föderationsweiten Datenschemas.

2. *Datenschutz (Privacy):* Aus Gründen des Datenschutzes ist es oftmals erforderlich, dass Benutzer explizit darüber entscheiden können müssen, welche über sie gespeicherten Daten welchem Service Provider zur Verfügung gestellt werden dürfen. Die Notwendigkeit so genannter *Attribute Release Policies (ARPs)* ist zwar bekannt, mit Ausnahme des auf SAML basierenden Projekts Shibboleth [Shi], das seit Version 1.2 rudimentäre provider-weite und benutzer-spezifische ARPs in einem proprietären Format bietet, existieren jedoch noch keine konkreten Spezifikationen. Teilfragestellungen betreffen die eindeutige, fälschungssichere *Identifikation von Service Providern*, geeignete formale Sprachen zur *Spezifikation* von ARPs sowie Möglichkeiten zu deren Abbildung – beispielsweise auf Directory Server Access–Control–Lists (ACLs) – um eine *Integration* von FIM-Komponenten in bestehende I&AM-Lösungen zu erreichen.
3. *Gesamt-Sicherheitsarchitektur*: Obwohl Maßnahmen für die *sichere Kommunikation* zwischen je zwei Endpunkten festgelegt werden, fehlt eine umfassende Betrachtung der *Sicherheit der gesamten Identitäts-Föderation*, die nichts anderes als ein verteiltes System autonomer, kooperierender Teilnehmer ist. Hier fehlen insbesondere Mechanismen zur provider-übergreifenden *Korrelation sicherheitsrelevanter Ereignisse*.
4. Beschränkung auf *Web basierte Dienste*: Die beschriebenen FIM-Ansätze sind auf die organisationsübergreifende Verwendung von Web Services ausgelegt und stellen umfangreiche Bemühungen an, um eine transparente Verwendbarkeit mit herkömmlichen Web Browsern zu gewährleisten. Die Anwendung der FIM-Techniken auf Dienste, die nicht web-basiert zur Verfügung stehen, beispielsweise die Provisionierung von Datenbanksystemen, Großrechnern und lokalen Rechnerpools, bleibt jedoch offen. Da viele Dienste auch langfristig nicht als Web Services realisiert werden können, müssen zusätzliche Methoden zur Datenakquisition eingesetzt werden, wodurch sich die Gesamtkomplexität weiter erhöht.
5. *Persistente Datenhaltung*: Zwar erhalten Service Provider unmittelbar bei der Verwendung des von ihnen angebotenen Dienstes die jeweils aktuellen Daten über den Benutzer. Änderungen an diesen Daten werden ihnen jedoch immer nur bei der nächsten Benutzung des Dienstes mitgeteilt. *Regelmäßige* oder *ereignisgesteuerte Datenabgleiche*, wie sie im Identity Management eingesetzt werden, sind ebenso wenig vorgesehen wie beispielsweise aus verteilten Dateisystemen bekannte *Cache-Invalidierungs-Techniken*. Möchte ein Service Provider über Veränderungen auf dem Laufenden gehalten werden, müssen wiederum zusätzliche Verfahren eingesetzt werden.

Die beschriebenen Nachteile haben in der Praxis zwei gravierende Konsequenzen: Einerseits gestaltet sich der Aufbau von größeren Identitätsföderationen äußert mühsam, andererseits kann auf Basis dieser Techniken nur ein Teil der angebotenen Dienste auf FIM umgestellt werden. Insbesondere wird auch die Integration in bestehende I&AM-Lösungen nur unzureichend unterstützt.

4 Zentraler Koordinationsdienst für Identitäts-Föderationen

In diesem Abschnitt präsentieren wir einen Ansatz, der zumindest Teile der oben erwähnten Defizite kompensiert und dabei kompatibel zum de facto Standard SAML bleibt. Er basiert auf einer Erweiterung von Identitäts-Föderationen um einen *zentralen Koordinationsdienst*, der den initialen Implementierungsaufwand verringert und die Skalierbarkeit verbessert. Die *Autarkie* der einzelnen Föderationsteilnehmer und die *dezentrale Verwaltung der Nutzdaten* bleiben dabei vollständig erhalten.

Aus technischer Sicht beginnt der Aufbau einer Föderation mit der Spezifikation des einzusetzenden Datenschemas. Dabei müssen die n Teilnehmer entweder eine gemeinsame Attributsmenge festlegen (d.h. Name, Syntax und Semantik jedes Attributs) oder jeder Teilnehmer muss die von den $n - 1$ anderen Teilnehmern verwendeten Schemata kennen, was einem Aufwand von $O(n^2)$ gleichkommt und in der Praxis *manuell* nicht mehr mit akzeptablem Aufwand wartbar ist.

Die Spezifikation eines gemeinsamen Daten-Schemas gestaltet sich unserer Erfahrung nach bereits bei nur wenigen Teilnehmern aus organisatorischen und unternehmenspolitischen Gründen oftmals schwierig, wodurch der Aufbau von Identitäts-Föderationen auch in technischer Hinsicht erschwert wird. Um provider-spezifische Erweiterungen nutzen zu können, ist darüber hinaus die paarweise Kenntnis der Schemata häufig sowieso nötig.

Unser zentraler Koordinationsdienst übernimmt Zusammenstellung und Verteilung eines *föderationsweiten Regelwerks* zur Konvertierung von Attributen zwischen je zwei Teilnehmern. Der Aufbau wird dadurch erleichtert, dass in der Praxis die meisten Attribute, die überhaupt konvertiert werden müssen, nur diskrete Werte aus einer kleinen Wertemenge annehmen. Der manuelle Aufwand zur Erstellung sämtlicher Konversionsregeln reduziert sich dadurch auf ein Minimum, dass die Regeln transitiv angewandt werden können: Wenn Regeln für die Konvertierung zwischen den Providern A und B existieren, dargestellt als $A \leftrightarrow B$, und auch Regeln für $B \leftrightarrow C$ vorhanden sind, so beschränkt sich die Erstellung von $A \leftrightarrow C$ auf eventuell vorhandene zusätzliche Attribute, die A und C miteinander, aber nicht mit B austauschen wollen.

Ferner ist die *zuverlässige Identifikation* von Föderations-Teilnehmern Aufgabe des Koordinationsdienstes: Die Zugehörigkeit eines Providers zu einer Identitäts-Föderation ist die Basis für seine Vertrauenswürdigkeit. Die Funktionalität, autoritative Aussagen über die Mitgliedschaft einzelner Provider in der Föderation auf Abruf zur Verfügung zu stellen, könnte beispielsweise von bereits vorhandenen Discovery Services oder im Rahmen einer für die föderationsinterne Public Key Infrastruktur (PKI) zuständigen Zertifizierungsautorität bereitgestellt werden. Hierdurch lassen sich insbesondere die derzeit notwendigen PKI-spezifischen Operationen wie die jeweils paarweise gegenseitige Validierung der Gültigkeit von Provider-Zertifikaten auf ein Minimum reduzieren.

Schließlich sorgt die Koordinationskomponente auch für Korrelation und Propagierung sicherheitsrelevanter Ereignisse, beispielsweise bei gezielten Angriffen auf Benutzer, einzelne Provider oder die Föderation als Ganzes, und Unterstützung entsprechender Eskalationsmechanismen. Durch diese holistische Betrachtungsweise lässt sich das Sicherheitsniveau innerhalb der Föderation deutlich erhöhen.

Unsere aktuellen Aufgaben umfassen die Spezifikation und anschließende prototypische

Implementierung sowohl der beschriebenen zentralen Koordinationskomponente als auch derjenigen providerseitigen Module, die zur Nutzung dieses Dienstes benötigt werden.

5 Weitere Forschungsfragestellungen

Neben dem Aufbau von Identitäts-Föderationen spielt deren laufender Betrieb sowie die Einbettung in die bestehende, jeweils organisationsinterne Software-Infrastruktur eine wesentliche Rolle. Dies umfasst insbesondere die Anbindung von Systemen, die über keine FIM-Schnittstelle verfügen, aber beispielsweise mit in Form von SAML Assertions übermittelten Benutzer-Stammdaten gespeist werden könnten.

Während derzeit I&AM und FIM voneinander isoliert behandelt werden und sich in beiden Bereichen völlig unterschiedliche Techniken entwickeln, muss unserer Überzeugung nach Konvergenz unter Ausnutzung der sich dabei ergebenden Synergieeffekte angestrebt werden. Unsere Arbeit konzentriert sich deshalb auf die Integration von FIM in vorhandene I&AM-Architekturen unter Wahrung der Kompatibilität zu Industrie-Standards, insbesondere SAML.

Danksagung:
Die Autoren danken den Mitgliedern des Münchener Netzwerk-Management Teams (MNM Team) für hilfreiche Diskussionen und wertvolle Kommentare zu früheren Versionen dieses Artikels. Das MNM Team ist eine Forschungsgruppe der Münchener Universitäten und des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften unter der Leitung von Prof. Dr. Heinz-Gerd Hegering.

Literatur

[ABB04] Anderson, S., Bohren, J., und Boubez, T. Web Services Trust Language (WS-Trust). ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf. 2004.

[Ka02] Kaler, C. Web Services Security specification. http://www-106.ibm.com/developerworks/webservices/library/ws-secure/. 2002.

[KN03] Kaler, C. und Nadalin, A. Web Services Federation Language specification. http://www-106.ibm.com/developerworks/webservices/library/ws-fed/. 2003.

[Le04] Lepro, R. Cardea: Dynamic Access Control in Distributed Systems. http://www.nas.nasa.gov/Research/Reports/Techreports/2003/nas-03-020-abstract.html. 2004.

[Lib] Liberty Alliance Homepage. http://project-liberty.org/.

[Ope] Open Source SAML Implementierung in C++ und Java. http://www.opensaml.org/.

[SAM] Security Assertion Markup Language V1.1 Standard Specification. http://www.oasis-open.org/committees/download.php/3400/oasis-sstc-saml-1.1-pdf-xsd.zip.

[Shi] Homepage des Shibboleth Projekts. http://shibboleth.internet2.edu/.