Identity Federation und Web Services

Karim Djelassi
Seminar Innovative Internet-Technologien und Mobilkommunikation, WS 2008/2009
Institut für Informatik, Lehrstuhl Netzarchitekturen und Netzdienste
Technische Universität München
karim@djelassi.com

ABSTRACT
Diese Ausarbeitung gibt einen Überblick über Identity Federation und Web Services und erklärt was sich hinter diesen Begriffen jeweils verbirgt. Im Anschluss werden aktuelle Identity Federation Projekte aufgezählt und klassifiziert. Die Identity Federation Projekte OASIS und Liberty Alliance werden genauer behandelt und im Detail vorgestellt. Zur Veranschaulichung wird ein Anwendungsbeispiel für Identity Federation präsentiert.

SCHLÜSSELWÖRTER
Identity federation, web service, identity federation management, digital identity, federated identity, authentication, information system, Liberty Alliance, Shibboleth, OpenID, OASIS, SAML, WSDL, SOAP

1. EINLEITUNG
Die Welt, in der wir leben, wird von einer steigenden Anzahl an Informationssystemen und Informationsservices unterstützt und ermöglicht. Dieses als „align and enable“ bekannte Prinzip beschreibt das Zusammenspiel von Informationstechnologie und Gesellschaft im Informationszeitalter [1]. Viele Menschen interagieren regelmäßig mit einer Vielzahl von unterschiedlichen Informationssystemen. Dabei kann es sich beispielsweise um Webmail-, Fotoalben-, Shopping- oder Blogging-Portale handeln. Ebenso machen webbasierte Business Applikationen einen großen Teil der regelmäßig verwendeten Informationssysteme aus.

So gut wie jede Interaktion mit einem Informationssystem erfordert eine Authentifizierung des Benutzers. Um sich gegenüber einem Informationssystem authentifizieren zu können, muss sich der Benutzer mit einem Benutzerkonto am System anmelden. Die Authentifizierung geschieht in der Regel mittels Eingabe von Benutzername und Passwort. Da der Benutzer vom System über sein Benutzerkonto identifiziert wird, spricht man auch von einer *Digital Identity* [2].

Da die meisten Menschen mit mehreren Informationssystemen interagieren, haben sie entsprechend auch mehrere Digital Identities. Aus Sicherheitsgründen sollten sich Digital Identities eines Benutzers im Bezug auf Benutzername und Passwort unterscheiden. Dennoch enthalten sie ähnliche persönliche Informationen, wie z.B. die Email-Adresse oder evtl. die Anschrift des Benutzers. Das Resultat ist eine schnell unüberschaubare Anzahl von Digital Identities, für die ein Benutzer unterschiedliche Anmeldeinformationen bereit halten muss, obwohl sie fast dieselben persönlichen Informationen enthalten.

Die aggregierte Anzahl an Digital Identities aller Benutzer in allen Informationssystemen ist dementsprechend enorm. Der Betreiber eines Informationssystems verwaltet nur die Digital Identities der Benutzer seines Systems. Sobald jedoch Informationssysteme in der Lage sein müssen sich mit anderen Informationssystemen auszutauschen müssen Digital Identities abgeglichen und synchronisiert werden können. Aufgrund der Vielfältigkeit der heute existierenden Informationssystem-Landschaft wird für jede Verbindung zweier Informationssysteme eine individuell maßgeschneiderte Softwarelösung benötigt. Diese Softwarelösungen sind in aller Regel sowohl zeit- als auch kostenintensiv [3].

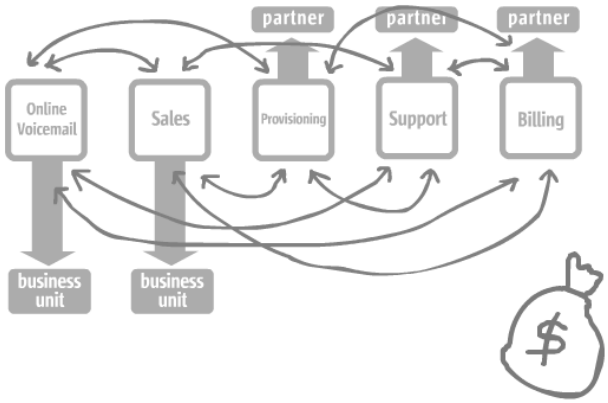

Abb. 1: Veranschaulichung der Komplexität von Informationssystem-Verbindungen [3]

Im Folgenden wird erläutert inwiefern Identity Federation und Web Services dazu beitragen können die mit Abb.1 symbolisch veranschaulichte Komplexität von Informationssystem-Verbindungen zu reduzieren.

1.1 Identity Federation
Identity Federation, auch bekannt unter der Formulierung *Federated Identity Management*, ist ein generisches Konzept, das die Angleichung und Vereinigung von Digital Identities und den in ihnen enthaltenen persönlichen Informationen beschreibt. Praktisch soll ein Benutzer nicht mehr eine Digital Identity pro Informationssystem besitzen, sondern nur noch auf wenige System-übergreifende Digital Identities angewiesen sein. Da Digital Identities durch den Prozess der Identity Federation vereinigt werden, spricht man hier auch von *Federated Identities*. Um Identity Federation global und einheitlich zu ermöglichen werden offene Standards und Spezifikationen entwickelt und benutzt [4].

Zur Umsetzung dieses Konzepts müssen sich Informationssystem-Betreiber im Bezug auf die Authentizität ihrer individuell gesammelten Digital Identities gegenseitig vertrauen. Gleichzeitig verständigt man sich darauf, die einmalige Validierung eines Benutzers mit deiner Digital Identity unterschiedlich zu handhaben. Die Informationssystem-Betreiber gehen ein Verhältnis des gegenseitigen Vertrauens ein und vereinigen ihre Digital Identities zu Federated Identities [3]. So würden sich z.B. Universitäten darauf verständigen ihre Studenten auf unterschiedliche Art und Weise zu immatrikulieren und gleichzeitig die Authentizität eines an einer vertrauten Universität immatrikulierten Studenten akzeptieren.

Damit stellt das Konzept der Identity Federation eine vielversprechende Lösung für eine breit gefächerte Menge an Problemen dar. So können durch den richtigen Einsatz von Identity Federation Lösungen unter anderem Probleme mit der

Skalierbarkeit von Informationssystem-Verbindungen eliminiert und Produktionskosten für entsprechende Software reduziert werden. Ebenso lässt sich durch den Einsatz solcher Lösungen der Datenschutz für Benutzer erhöhen und die Benutzerfreundlichkeit umfassend verbessern [3].

1.2 Web Services

Die Entwicklung von Computern begann vor ungefähr 60 Jahren im zweiten Weltkrieg. Die damaligen Computer wurden ausschließlich für militärische Zwecke entworfen und gebaut. Eine der charakteristischsten Eigenschaften dieser Computer war, dass sie die Berechnung der ihnen gestellten Aufgaben alleine bewerkstelligen mussten. Die Evolution der isoliert arbeitenden Computer setzte sich zunächst fort und wurde letztendlich in den Siebzigerjahren durch die Entwicklung der Personal Computer (PC) beendet. Die für die damalige Zeit unglaublich leistungsfähigen Computer wurden verstärkt an immer mehr Arbeitsplätzen eingesetzt. Durch die Ausstattung vieler Mitarbeiter einer Organisation mit einem PC wurden Daten verstärkt lokal abgespeichert und Informationsstrukturen wandelten sich zu tendenziell dezentraleren Schemata [5].

An diesem Punkt der Entwicklung bekamen Netzwerke eine entscheidende Bedeutung für den Informationsaustausch – die Entwicklung der ersten verteilten Systeme begann. Diese waren innerhalb kürzester Zeit in der Lage Funktionalität für die Computer eines Netzwerkes bereitzustellen. Die Netzwerke beschränken sich jedoch in der Regel auf eine Organisation. Dies änderte sich jedoch schlagartig mit der Einführung und der rapide ansteigenden Nutzung des Internets [5].

Verteilte Systeme bekamen durch diese Entwicklung noch eine viel bedeutendere Rolle zugesprochen – eine Entwicklung, die bis heute anhält und weiterhin die Bedeutsamkeit von verteilten Systemen steigen lässt. Ebenso stiegen jedoch die Anforderungen an verteilte Systeme: Netzwerkstrukturen wuchsen, Informationsmengen nahmen zu und Informationsstrukturen wurden komplexer. Durch die Verwicklung von immer mehr Organisationen und die globale Verteilung von Informationen waren eine steigende Inkohärenz und eine daraus resultierende Inkonsistenz der Informationen unvermeidlich [5].

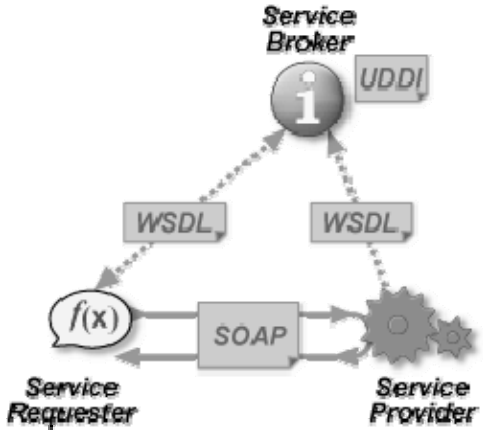

Abb. 2: Web Services Protokoll Architektur [6]

Insbesondere die konstant ansteigende Anzahl von Organisationen mit denen Informationsaustausch betrieben wurde, sorgte für eine ebenso konstant ansteigende Kostenkurve für Informationsverarbeitung und eine Vielzahl von Softwarelösungen, die aufgrund mangelnder Übertragbarkeit kaum wiederverwendbar waren [3]. Dieser Umstand machte die Entwicklung von standardisierten und somit kosteneffizienten Wegen des Informationsaustauschs dringend notwendig: *Web Services* wurden eingeführt. Diese Technologie ermöglicht es verteilten Systemen miteinander zu kommunizieren und vollautomatisch Informationen auszutauschen.

Aktuell existieren zwei maßgebliche Web Service Plattformen: J2EE von Sun Microsystems und .NET von Microsoft. Beide Plattformen beherbergen mehrere Web Service Frameworks. Obwohl die unterschiedlichen Frameworks auf unterschiedlichen Plattformen beruhen besteht dennoch Kompatibilität durch die Verwendung und Einhaltung von gemeinsamen und offenen Protokollen.

Wie in Abb.2 dargestellt handelt es sich bei den essentiellen Protokollen um die *Web Service Description Language (WSDL)* und das *Simple Object Access Protocol (SOAP)*. Wie der Name vermuten lässt wird WSDL für die Beschreibung von Web Services verwendet. Mit Hilfe einer WSDL Beschreibung ist es einem Benutzer oder einem Computer möglich festzustellen wo ein spezieller Web Service zu finden ist und in welcher Art und Weise die Interaktion mit diesem erfolgen muss. Im Wiederspruch zu seinem Namen handelt es sich bei SOAP nicht mehr um ein einfaches Protokoll. Mit der Zeit wurde es zu einem komplexen und sehr vielseitigen Protokoll, welches zum Versenden und Empfangen von Web Service Nachrichten verwendet wird. Die an einen Web Service versendeten Nachrichten enthalten in der Regel Meta-Informationen, welche die vom Benutzer benötigten Informationen beschreiben. Die im Gegenzug von einem Web Service versendeten und vom Benutzer empfangenen Nachrichten enthalten in der Regel die angefragten Informationen. Beide Protokolle, WSDL und SOAP, basieren auf XML [6].

Mit Bezug auf Identity Federation stellen Web Services die nötigen Plattformen und Frameworks bereit, in deren Umgebung die Entwicklung und der Einsatz von Identity Federation Systemen ermöglicht werden. Es ist von entscheidender Bedeutung, dass alle verwendeten Protokolle frei verfügbar sind und offenen Standards genügen damit uneingeschränkte Kompatibilität zu jeder Zeit garantiert werden kann.

2. PROJEKTE

Mittlerweile existiert eine beträchtliche Anzahl an Identity Federation Projekten, deren Entwicklungsstände sich teilweise der Markreife nähern. Einige wenige Projekte und eine Auswahl von am jeweiligen Projekt beteiligten Unternehmen haben bereits damit begonnen Identity Federation in Form von Pilotprojekten aktiv einzusetzen. Nahezu marktreife Identity Federation Projekte zeichnen sich unter anderem dadurch aus, dass neben Standards und Spezifikationen auch fertig implementierte Software erhältlich ist. Diese Basissoftware implementiert den Teil der Standards und Spezifikationen, der für alle Verwender identisch ist. So können sie von Unternehmen bei minimalem Zeit- und Kostenaufwand aufgegriffen, erweitert und an die eigenen Bedürfnisse angepasst werden [7].

Zu den am mit weitesten fortgeschrittenen Organisationen zählen unter anderem *Liberty Alliance*, *Internet2* und die *Organization for the Advancement of Structured Information Standards (OASIS)* mit ihren Projektgruppen *Liberty Federation*, *Shibboleth* und dem *Security Services Technical Committee (SSTC)*. Speziell diese drei Projektgruppen konnten die Entwicklung ihrer Identity Federation Projekte durch enge Kooperation schnell voran treiben und bilden mittlerweile die Speerspitze auf dem Gebiet der Identity Federation [8].

Bereits kurz nach dem Start von Shibboleth im Jahr 2000, dicht gefolgt von Liberty Federation und SSTC im Jahr 2001, begann die Kooperation zwischen den Projektgruppen. Wie in Abb. 3 erkennbar fand der erste Austausch zwischen Liberty Federation und SSTC nach knapp 22 Monaten Projektarbeit im November 2002 mit dem Release des *SAML V1.0* Standard statt. Die Veröffentlichung dieses Standards nahm Einfluss auf die in der

frühen *Phase 1* befindliche Liberty Federation. Im Januar 2003 konnte die erste Liberty Federation Spezifikation veröffentlicht werden: *ID-FF V1.1*. Diese wurde dicht gefolgt von den im Juli bzw. August 2003 veröffentlichten ersten Shibboleth Spezifikationen: *Shib 1.0 bzw. 1.1*. Beide Spezifikationen basierten auf dem SAML V1.0 Standard.

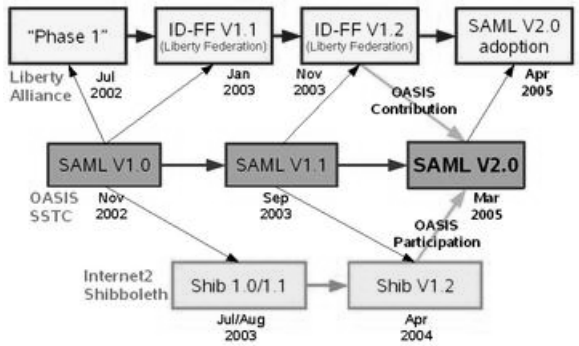

Abb. 3: Kooperation zwischen Liberty Alliance, Shibboleth und OASIS [15]

Basierend auf der im September 2003 folgenden SAML V1.1 Spezifikation wurden die Spezifikationen *ID-FF V1.2* und *Shib 1.2* entwickelt. Die elementaren Aspekte beider Spezifikationen konnten in den im März 2005 veröffentlichten *SAML V2.0* eingebracht werden. Die aktuelle Version der Shibboleth Spezifikation ist die im März 2008 veröffentlichte *Shib V2.0*, welche [9]. Für Liberty Federation stellt die ID-FF V1.2 Spezifikation seit 2003 weiterhin den aktuellen Stand dar. Dieser wurde allerdings um eine ganze Reihe von zusätzlichen Spezifikationen ergänzt, wodurch die Abdeckung verschiedenster Bedürfnisse unterschiedlicher Branchen im Bezug auf Identity Federation gewährleistet wird [10].

SAML V2.0 stellt bis zum heutigen Tag die unumstrittene Basis für Identity Federation Projekte und Spezifikationen dar und wurde von einer Vielzahl von Identity Federation Projektgruppen aufgegriffen. Welche Rolle SAML V2.0 spielt und in welchem Zusammenhang es mit Liberty Federation steht im wird im Folgenden genauer erläutert.

3. OASIS

OASIS ist ein gemeinnütziges Konsortium, das die Entwicklung und Verbreitung von offenen Standards für die globale Informationsgesellschaft voran treibt. Das Konsortium wurde im Jahr 1993 von einer kleinen Anzahl von Unternehmen gegründet, die es sich zum Ziel gesetzt hatten die Kompatibilität zwischen ihren Produkten zu gewährleisten. Mittlerweile besteht das Konsortium aus über 5.000 Mitgliedern, die über 600 Unternehmen aus unterschiedlichen Ländern der ganzen Welt repräsentieren [11].

OASIS fordert aktiv dazu auf sich an der Mitgestaltung von offenen Standards zu beteiligen. Mitglied werden kann jeder, vom Selbständigen über kleine Unternehmen bis hin zum internationalen Konzern. Der jährliche Mitgliedsbeitrag liegt je nach Art der Mitgliedschaft und Unternehmensform des Mitglieds bei 300 bis 50.000 Dollar [12].

Strukturell gliedert sich OASIS in das *Board of Directors*, das *Tech Advisory Board* und diverse *Technical Committees*. Die Boards werden im Zwei-Jahres Intervall mit Mitgliedern besetzt, welche wiederum von Mitgliedern gewählt wurden. Die Teilnahme an beliebigen Technical Committees steht jedem Mitglied frei [11].

3.1 SSTC

Das *Security Services Technical Committee (SSTC)* ist eines der angesprochenen Technical Committees. Es wurde im November 2000 ins Leben gerufen, worauf hin im Januar 2001 das erste Treffen der SSTC-Mitglieder stattfand und die Aufgabe des Komitees definiert wurde. Aufgabe des SSTC ist es ein auf XML basierendes Framework, welches die Erstellung und den Austausch von Authentifizierungs- und Autorisations-Informationen ermöglicht, zu definieren, zu erweitern und zu pflegen. Zentrales Objekt dieser Bemühungen ist seit jeher die Entwicklung des SAML Standards. [13]

3.2 SAML

Die *Security Assertion Markup Language (SAML)*, welche aktuell in der Version 2.0 vorliegt, ist dazu bestimmt die Erstellung und den Austausch von Authentifizierungs- und Autorisations-Informationen zu ermöglichen.

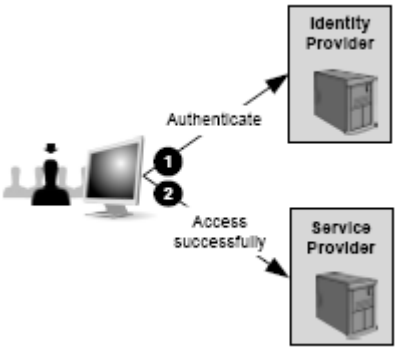

Abb. 4: Single Sign-On Authentifizierungsprozess, ausgelöst vom Identity Provider [16]

In Anspielung auf das bekannte Sprichwort „think globally, act locally“ wird dieses im Sinne der Identity Federation genau umgekehrt zu „think locally, act globally“ [14]. Dieses lässt sich durch das für den Endbenutzer wichtigste Feature der Identity Federation, den Single Sign-On, näher erläutern. Wie in Abb.4 ersichtlich authentifiziert sich der Benutzer bei seinem Identity Provider, dem Anbieter, der die Digital Identity des Benutzers verwaltet, dem der Benutzer nahe steht und Vertrauen schenkt – „think locally“. Mithilfe dieser Authentifizierung ist der Benutzer in der Lage auf Service Provider zuzugreifen. Bei Service Providern handelt es sich um Anbieter eines speziellen Angebots, jedoch muss für den Zugriff zunächst die Authentizität des Benutzers gewährleistet werden. Mittels der vom Identity Provider bestätigten Authentizität des Benutzers kann dieser wiederum auf die Angebote verschiedenster Service Provider weltweit zugreifen – „think globally“.

Eine weitere Art der Realisierung des Single Sign-On wird in Abb.5 dargestellt. Im Falle des Nichtvorhandenseins der Authentifizierung des Benutzers wird dieser an seinen Identity Provider weitergeleitet. Dort muss sich der Benutzer zunächst authentifizieren und kann im Anschluss zum Angebot des Service Providers zurückkehren [16].

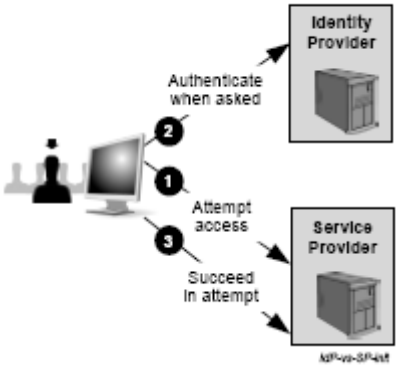

Abb. 5: Single Sign-On Authentifizierungsprozess, ausgelöst vom Service Provider [16]

Zu den Stärken von SAML zählt vor allem die starke Anpassbarkeit bei gleichzeitiger Wahrung der Kompatibilität zum eigenen Standard. Auf diese Weise ist es SAML möglich den unterschiedlichsten Anforderungen von Unternehmen zu Rechnung zu tragen und somit als unbestrittener Basisstandard für Identity Federation zu gelten. Ebenfalls Resultat des sehr allgemein gehaltenen Standards ist die Plattformunabhängigkeit, was wiederum zur weiteren Verbreitung und Adaption von SAML beiträgt. Aus Sicht eines Unternehmens betrachtet bietet SAML sehr großes Potential für Zeit- und Kostenersparnisse – Kosten die sonst durch die Entwicklung von komplett individuell erstellter Software verursacht worden wären. Aus Sicht des Endbenutzers ist die stark erhöhte Benutzerfreundlichkeit durch den Single Sign-On direkt spürbar. Die auf den ersten Blick nicht ganz offensichtliche Verbesserung von Sicherheit und Privatsphäre für den Endbenutzer durch insgesamt weniger und gleichzeitig leichter kontrollierbare Federated Identities zählt ebenfalls zu den zentralen Stärken von SAML [14].

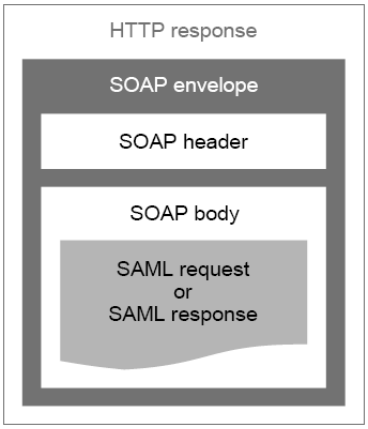

Abb. 6: Strukturelle Einbettung einer SAML Nachricht in SOAP und http [16]

Ebenso gliedert sich SAML in die bestehende Landschaft aus Standards und Spezifikationen nahtlos ein. Abb.6 zeigt eine in eine SOAP Nachricht eingebettete SAML Nachricht. SOAP wird im Zusammenhang mit Web Services verwendet. Es bietet sich an SAML und Identity Federation insgesamt in Verbindung mit Web Services zu nutzen. Sowohl Identity Federation mit SAML als auch Web Services mit SOAP sind stark durch Standards und Spezifikationen geprägte Technologien. Auf diese Weise können vollständig automatisierte Prozesse über System- und Unternehmensgrenzen hinweg auf einer gemeinsamen Basis existieren und funktionieren [16].

4. LIBERTY ALLIANCE

Die Liberty Alliance Projektgruppe arbeitet an der Entwicklung von Identity Federation Spezifikationen, Protokollen und Applikationen. Die leitende Vision der Liberty Alliance ist eine auf offenen Standards basierende und vernetzte Welt zu ermöglichen in der Kunden, Bürger, Unternehmen und Regierungen Onlinetransaktionen leichter als bisher ausführen können wobei die Privatsphäre und die Sicherheit von persönlichen Informationen dauerhaft geschützt bleibt [17]. Diese Vision soll dadurch erreicht werden, dass alle erarbeiteten Spezifikationen, Protokolle und Applikationen frei verfügbar gemacht werden und von jedem, der Liberty Federation für verwenden möchte, aufgegriffen und adaptiert werden können.

4.1 Projektmitglieder

Die Liberty Alliance wurde im Jahr 2001 von 30 führenden Organisationen aus den Bereichen IT, Finanzwesen, Telekommunikation, Medien, Produktion, Regierung und Bildung gegründet. Die Organisationen entstammen unterschiedlichen Teilen dieses Planeten und bieten so eine gute Repräsentation verschiedener Kulturen. Insbesondere die umfassende Repräsentation unterschiedlicher Kulturen im Projekt ist ein wichtiger Aspekt bei Entwicklung von global anwendbaren Standards für Identity Federation. Die aktuelle Anzahl der Liberty Alliance Mitglieder beläuft sich mittlerweile auf 150 bedeutende Organisationen [18].

Strukturell sind die Mitglieder in mehrere Stufen unterteilt, welche jeweils einen anderen Grad der Beteiligung aber auch des Einflusses repräsentieren. An der Spitze der Hierarchie stehen die Organisationen, die dem Management Board angehören. Beispiele für diese Mitgliedschaftsstufe sind AOL, Intel, Sun und Oracle. Dennoch sind auch bei Mitgliedschaftsstufen mit weniger Beteiligung und Einfluss bedeutende Unternehmen wie z.B. IBM, HP, Nokia, Adobe und Paypal zu finden [19].

4.2 Liberty Federation

Die Gründung der Liberty Alliance fand zunächst ausschließlich vor dem Hintergrund der gemeinsamen Entwicklung von Identity Federation Spezifikationen statt. Das erste und zunächst einzige Projekt war somit die Liberty Federation.

Mit dem Fortschritt der Liberty Federation ergaben sich Ansatzpunkte für Erweiterungen und weitere Aspekte die näherer Betrachtung bedurften. Es kam zur Gründung diverser Strategic Initiatives innerhalb der Liberty Alliance, welche alle auf der Liberty Federation basierten [20].

Ein weiteres Projekt, das sich umfassend auf alle Strategic Initiatives bezieht, ist die Liberty Interoperable. Im Rahmen dieses Projekts werden Testszenarien für Liberty Federation entwickelt und angewendet. Aufgabe ist es Unternehmen, die einen Test ihrer Liberty Federation Lösung wünschen zu prüfen um die Kompatibilität mit den Standards und Spezifikationen zu garantieren. Bei einem erfolgreich absolvierten Test erhält das Unternehmen ein Zertifikat, das die Standard-Konformität dokumentiert. Sollte ein Unternehmen mit seiner Liberty Federation Lösung den Test nicht bestehen werden detailierte Hinweise und Testergebnisse bereitgestellt um Schwächen und Fehler der Implementierung zu beseitigen [21].

Mit diesem Testprogramm ist die Liberty Alliance bisher alleiniger Vorreiter und macht einen wichtigen Schritt in Richtung Vertrauensbildung zwischen Unternehmen. Auf diese Weise können Unternehmen, die den Test erfolgreich absolviert haben und das Zertifikat vorweisen können, davon ausgehen dass zumindest auf Ebene der unterschiedlichen Implementierungen

und im Bezug auf deren Kompatibilität die Wahrscheinlichkeit für Probleme sehr gering ist.

4.3 Liberty Web Services

Bei den Liberty Web Services handelt es sich um eine Strategic Initiative der Liberty Alliance. Basierend auf der ID-FF V1.2 Spezifikation der Liberty Federation und dem SAML V2.0 Standard existieren die Spezifikationen *Identity Web Services Framework ID-WSF V2.0* und *Identity Service Interface Specifications ID-SIS V1.0* im Liberty Web Services Projekt. Zusammen ermöglichen beide Technologien die Entwicklung von Identity-sensitiven Web Services [22].

Sinn und Zweck von Identity-sensitiven Web Services ist die Ermöglichung völlig neuer und stark automatisierter Anwendungen im Web. Durch die Liberty Web Services werden Wege eröffnet, die die Vergabe von Zugriffsrechten auf persönliche Informationen eines Benutzers ermöglichen. Ziel ist es den automatischen Informationsaustausch zwischen Service Providern zu realisieren um so das Service Angebot für den Benutzer zu bereichern. Die Herausforderung ist zunächst die Auffindung von Informationen mittels eines *Discovery Service (DS)* überhaupt erst zu ermöglichen und im Anschluss einen standardisierten Informationsaustausch zu gewährleisten [23].

In diesem Zusammenhang wird der Informationen zur Verfügung stellende Service Provider als *Web Service Provider (WSP)* bezeichnet. Der Informationen konsumierende Service Provider wird entsprechend als *Web Service Consumer bezeichnet (WSC)*. Abb.7 zeigt in diesem Zusammenhang die abstrahierte Liberty Federation im Vergleich mit den detailierten Liberty Web Services. *Authentication Service (AS)*, *Single Sign-On Service (SSOS)*, *Identity Mapping Service (IMS)* und Discovery Service (DS) stellen die detailieren Funktionalitäten des abstrahierten *Identity Providers (IdP)* dar [23].

Ein beispielhaftes Szenario ist die vollautomatische Buchung eines Bahntickets. Statt einer klassischen Online-Buchung durch den Benutzer, für die eine manuelle Auswertung von Terminkalender, möglichen Zugverbindungen, entsprechenden Preisen und eventuellen Sonderangeboten nötig wäre, soll die Buchung vollständig vom Buchungssystem erledigt werden. Um das Zeitfenster für die Zugfahrt feststellen zu können benötigt das Buchungssystem Zugriff auf den Terminkalender des Benutzers. Mittels eines Discovery Service kann das Buchungssystem feststellen welcher Service Provider den Terminkalender des Benutzers verwaltet. Sofern der Benutzer den eingeschränkten Zugriff auf den Terminkalender durch das Buchungssystem gestattet hat kann das Buchungssystem die für die Buchung des Bahntickets relevanten Informationen vollautomatisch abrufen. Entsprechend wird das Buchungssystem dazu in die Lage versetzt ein Ticket für eine in den Terminkalender passende Zugverbindung zu buchen.

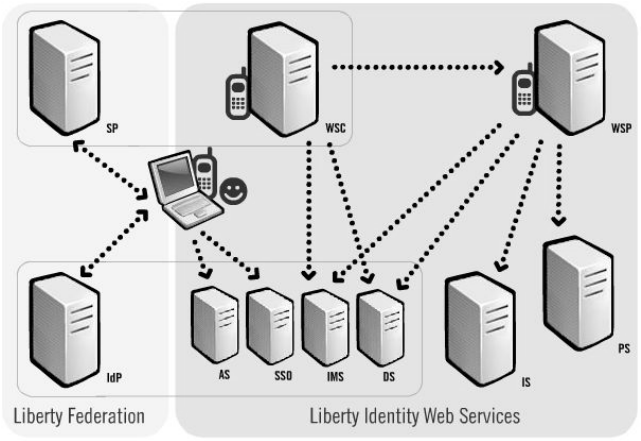

Abb. 7: Liberty Federation und Liberty Web Services im Vergleich [24]

Die Bestrebungen seitens Liberty Alliance gehen in die Richtung immer mehr Ressourcenarten zu standardisieren. Genau so wie sich der Terminkalender eines Benutzers für einen anderen Service Provider als nützlich erweisen kann sind ähnliche Applikationen mit Fotoalben, Sozialen Beziehungen, Favoriten, Blogg-Beträgen etc. denkbar. Liberty Web Services ermöglichen Applikationen, die heute noch unmöglich sind.

5. ANWENDUNGSBEISPIEL

Zur Veranschaulichung des Einsatzes von Identity Federation wird die Netzausweis Implementierung der Deutschen Telekom als Anwendungsbeispiel herangezogen. Das Netzausweis Projekt basiert auf den Standards SAML und Liberty Federation. Es erreichte im Jahr 2005 die Marktreife und wurde sofort eingeführt. In das Projekt involviert waren zunächst die drei Sparten des Deutsche Telekom Konzerns: T-Home, T-Mobile und T-Systems. Ziel war die Vereinigung der Benutzerkonten der Kunden. Dieser Schritt war sowohl für die Deutsche Telekom selbst, jedoch auch für den Kunden aufgrund bereits in dieser Ausarbeitung genannten Beweggründen von Vorteil [25].

Obwohl es sich bei den Sparten der Deutschen Telekom um Teile desselben Konzerns handelt waren aufgrund der jeweiligen Größe die Unterschiede im Bezug auf die Informationssystem-Landschaft enorm. Somit stand die Deutsche Telekom vor derselben Problemstellung wie mehrere unabhängige Unternehmen, die auf Informationsaustausch angewiesen sind. Im Zuge der erfolgreichen Markteinführung konnten weitere Unternehmen für den Netzausweis gewonnen und an das Identity Federation Netzwerk der Deutschen Telekom angebunden werden. Angetrieben durch die steigende Anzahl an Partnerunternehmen wurde das Netzausweis Projekt verlängert und um Multi-Protokoll Funktionalität erweitert. Neben den bereits implementierten Standards SAML und Liberty Federation wurden auch die Protokolle von OpenID und Microsoft Cardspace integriert [25].

Für die erfolgreiche Implementierung und Einführung des Netzausweises wurde die Deutsche Telekom mit dem IDDY Award 2006 ausgezeichnet. Inspiriert durch die Multi-Protokoll Erweiterung des Netzausweises wurde die Deutschen Telekom ein weiteres Mal ausgezeichnet, dieses Mal mit dem IDDY Award 2008 [25]. Der Netzausweis ist somit der reale Beweis dafür, dass Liberty Federation Lösungen umsetzbar sind und sich bereits in der Praxis bewährt haben.

6. ZUSAMMENFASSUNG UND AUSBLICK

Identity Federation gehört zu den wegweisenden Technologien des 21. Jahrhunderts. Mit der stetig steigenden Anzahl an Service Providern im Internet und der ebenso rasant steigenden Anzahl an

Benutzern dieser Services wird Identity Federation ein absolut notwendiges Mittel darstellen um die entstehende Komplexität zu bewältigen und kontrollierbar zu machen.

Bereits heute sind Bemühungen die Benutzerfreundlichkeit von Service Angeboten zu erhöhen auf der Tagesordnung. Nicht zuletzt kann die immer tiefergreifende und umfassendere Vernetzung von Service Angeboten durch Single Sign-Ons oder zumindest den Einsatz von gemeinsamen genutzten Digital Identity Datenbanken für verwandte Service Angebote die Komplexität für den Endbenutzer stark reduzieren. Als aktuelle Beispiele sind Windows Live ID von Microsoft, Apple ID von Apple oder myTUM von der TU München zu nennen, welche bereits innerhalb dieser großen Organisationen für eine bemerkenswerte Komplexitätsreduzierung sorgen.

Der nächste Schritt wird sein über Unternehmensgrenzen hinweg die unzähligen Digital Identities in wenige Federated Identities zusammenzuführen und zu bündeln. Aktuelle Ansätze wie die von OASIS oder Liberty Alliance stehen stellvertretend für diese Bewegung und haben darüber hinaus große Aussichten auf Erfolg. Nicht zuletzt lassen sich diese guten Erfolgsaussichten durch die vielversprechenden bis sehr erfolgreichen Pilotprojekte und die Geschlossenheit der maßgeblich an der Entwicklung beteiligten Unternehmen begründen.

Man hat offensichtlich aus Fehlern der Vergangenheit gelernt. Noch heute bekommt man die redundante Entwicklung verschiedener HTML Standards von diversen Unternehmen zu spüren. Anstatt dieselbe Technologie an verschiedenen Stellen redundant und getrennt voneinander weiterzuentwickeln war es beim Großprojekt Identity Federation offenbar möglich sich mit dem Großteil der maßgeblichen Unternehmen und somit auch mit der direkten Konkurrenz zusammenzufinden und an einer gemeinsamen Lösung zu arbeiten. Selbst getrennt voneinander operierende Projektgruppen waren und sind in der Lage aktiv Informationen auszutauschen und sicherzustellen, dass die Entwicklungen nicht in völlig unterschiedliche Richtungen laufen und stattdessen auf derselben Basis aufbauen.

Gemessen an den vielversprechenden Pilotprojekten der aktuellen Tage und den ersten im Business-2-Business Sektor produktiv genutzten Identity Federation Lösungen, speziell im Bereich Outsourcing und Supply Chain Management, kann die vollständige Marktreife nicht mehr allzu lange auf sich warten lassen. In dem Moment der Markreife wird Federated Identity auch Einzug erhalten bei Service Providern deren Angebote sich an private Endbenutzer richten. Letztendlich möchte der Großteil der privaten Endbenutzer von IT und Service Angeboten möglichst unkompliziert benutzen. Es wird immer mehr darauf ankommen Technologien intuitiv zugänglich und bedienbar für jedermann zu machen. Die enorme Steigerung der Benutzerfreundlichkeit durch Identity Federation ist nicht die Lösung aller Probleme, dennoch wird sie die IT ein Stück näher an die reale Welt heran führen und besser in den Alltag der Menschen integrieren.

7. ABBILDUNGEN

8. QUELLEN

[1] Krcmar, H., Informationsmanagement, Springer

[2] „Identity and Access Management", Allan Milgate, http://identityaccessman.blogspot.com/, 29.1.2009

[3] „Federated Identity Management", Sun Microsystems, http://www.sun.com/software/media/flash/demo_federation/index.html, 29.1.2009

[4] „Federated Identity", Wikipedia Foundation, http://en.wikipedia.org/wiki/Federated_identity, 29.1.2009

[5] Eberhart, A. and Fischer, S., Web Services: Grundlagen und praktische Umsetzung in J2EE und .NET, Hanser

[6] „Web Service", Wikipedia Foundation, http://en.wikipedia.org/wiki/Web_service, 29.1.2009

[7] „Identity Federation Multi-Protocol Solutions", Symlabs, http://symlabs.com/solutions/identity-federation, 29.1.2009

[8] „Whats Federated Identity Management?", David F. Carr, http://www.eweek.com/c/a/Channel/Whats-Federated-Identity-Management/, 29.1.2009

[9] „Shibboleth 2 Available", Internet2, http://shibboleth.internet2.edu/shib-v2.0.html, 29.1.2009

[10] „Liberty Alliance Complete Specifications ZIP Package", Liberty Alliance, http://www.projectliberty.org/resource_center/specifications/liberty_alliance_complete_specifications_zip_package_21_november_2008, 29.1.2009

[11] „OASIS – Who we are", OASIS, http://www.oasis-open.org/who/, 29.1.2009

[12] „Categories and Dues", OASIS, http://www.oasis-open.org/join/categories.php, 29.1.2009

[13] „OASIS Security Services TC", OASIS, http://www.oasis-open.org/committees/security/charter.php, 8.1.2009

[14] „SAML V2.0 Executive Overview", OASIS, http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf, 8.1.2009

[15] „Liberty Federation Strategic Initiative ", Liberty Alliance, http://www.projectliberty.org/liberty/strategic_initiatives/federation, 29.1.2009

[16] „ SAML V2.0 Technical Overview ", OASIS, http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf, 8.1.2009

[17] „About", Liberty Alliance, http://www.projectliberty.org/liberty/about, 29.1.2009

[18] „History", Liberty Alliance, http://www.projectliberty.org/liberty/about/history, 29.1.2009

[19] „Current Members", Liberty Alliance, http://www.projectliberty.org/liberty/membership/current_members, 29.1.2009

[20] „Strategic Initiatives“, Liberty Alliance, http://www.projectliberty.org/liberty/strategic_initiatives, 29.1.2009

[21] „Liberty Interoperable“, Liberty Alliance, http://www.projectliberty.org/liberty/liberty_interoperable, 29.1.2009

[22] „Liberty Web Services“, Liberty Alliance, http://www.projectliberty.org/liberty/strategic_initiatives/web_services, 29.1.2009

[23] „Liberty Alliance Web Services Framework: A Technical Overview“, Liberty Alliance, http://www.projectliberty.org/liberty/content/download/4120/27687/file/idwsf-intro-v1.0.pdf, 29.1.2009

[24] „Liberty Alliance“, Wikipedia Foundation, http://en.wikipedia.org/wiki/Liberty_alliance, 29.1.2009

[25] „Case Study: Deutsche Telekom lowers implementation barriers for online IP based services“, Liberty Alliance, http://www.projectliberty.org/liberty/content/download/4421/29639/file/Deutsche%20FINAL9.08.pdf, 8.1.2009