Sichere und effiziente Benutzerverwaltung

Dr. Harald Meyer

Principal Architect
Novell GmbH
Zeil 79
60313 Frankfurt
Harald.Meyer@novell.com

Abstract: Ein zentrales Identitätsmanagement erleichtert die Verwaltung der IT-Zugänge unterschiedlicher Benutzergruppen innerhalb einer Organisation. Sobald jedoch auch Zugänge für Benutzer außerhalb der eigenen Organisation verwaltet werden müssen , stößt ein zentrales Konzept schnell an organisatorische Grenzen. Föderation ist ein Ansatz, um dieses Problem zu lösen, indem ein sicherer und trotzdem effizient zu verwaltender Zugang für externe Benutzer ermöglicht wird. In der Praxis haben sich mit Liberty und Shibboleth zwei leicht unterschiedliche Ansätze entwickelt, die allerdings weitgehend identische Prinzipien und Basisstandards nutzen.

1 Zentrales Identitätsmanagement

Alle IT-Systeme mit nicht-öffentlichen Inhalten benötigen einen funktionierenden Zugriffsschutz, d.h. die zuverlässige Authentisierung des Benutzers („Wer bist du?“) und darauf aufbauend die Autorisierung zur Nutzung der jeweiligen Ressourcen („Was darfst du?“).

Ein zunehmendes Problem stellt dabei die Verwaltung der Benutzerdaten dar, auf deren Basis die Authentisierung und Autorisierung erfolgt. So müssen unterschiedliche Benutzergruppen verwaltet werden wie beispielsweise Studierende, wissenschaftliche und nichtwissenschaftliche Mitarbeiter, Stipendiaten, Gasthörer, Gastwissenschaftler, Bibliotheksnutzer oder wissenschaftliche und industrielle Kooperationspartner.

Diese benötigen Zugriff auf so unterschiedliche Systeme wie interne und externe Rechnerpools, administrative Systeme, Bibliotheks-Systeme für den Zugriff auf eigene und fremde Bestände, externe Online-Datenbanken oder Projektverzeichnisse. Diese Systeme verfügen meist über jeweils eigene Benutzerverwaltungen, sodass ein Benutzer im Extremfall für jedes freigeschaltete System einen eigenen Account benötigt.

Die Verwaltung der Zugangsinformationen muss dabei sowohl effektiv als auch effizient sein.

Effektivität bedeutet in diesem Zusammenhang, dass nur tatsächlich Berechtigte Zugang erhalten - und behalten. So sollte beispielsweise der Zugang eines Studierenden zu einem Rechnerpool mit der Exmatrikulation zeitnah und zuverlässig deaktiviert werden. Gleiches gilt für den Zugang eines industriellen Kooperationspartners bei Ablauf der Kooperation.

Aus Gründen der Effizienz müssen die damit verbundenen Prozesse möglichst automatisiert werden. Dies gilt umso mehr, als gerade im Forschungs- und Bildungsbereich die Fluktuationsrate der Benutzer vergleichsweise hoch ist.

Die Lösung für die meisten dieser Fragestellungen ist ein zentrales Identitätsmanagement, bei dem Anlage und Deaktivierung von Accounts größtenteils automatisch ausgelöst werden durch Änderungen in den jeweiligen führenden Stammdatensystemen, also z.B. dem System zur Verwaltung der Studierenden. Technisch existieren dazu ausgereifte Lösungen mit umfassenden Funktionen einschließlich manueller Beantragungs- und Freigabeworkflows, Passwort-Self-Service und anderen mehr.

Eine derartige zentrale Infrastruktur für die Verwaltung der Benutzer bietet somit innerhalb einer einzelnen Organisation wie z.B. einer Universität klare Vorteile hinsichtlich erhöhter Sicherheit bei reduzierten Kosten und verbessertem Benutzerkomfort, der sich beispielsweise in einem unkomplizierten und schnellen Prozess zur Beantragung von Berechtigungen ausdrückt.

An seine Grenzen kommt ein zentrales Konzept jedoch dann, wenn die verwalteten Benutzer nicht mehr nur einer gemeinsamen Organisation angehören, sondern wenn eine Kooperation zwischen unterschiedlichen organisatorischen Einheiten erforderlich ist. Eine einzige zentrale Infrastruktur scheidet hier aus, da beide Partner in der Regel bereits über jeweils eigene Lösungen verfügen, die nicht konsolidiert werden können. Weitere Schwierigkeiten ergeben sich beispielsweise aus so profanen Fragestellungen wie der Systematik von Benutzernamen oder anderen eindeutigen Kennungen. Auch zeigt die Praxis, dass beispielsweise die „Heimat-Organisation“ in vielen Fällen keinen vollständigen und aktuellen Überblick darüber hat, in welchen „Gast-Organisationen“ eines ihrer Mitglieder über IT-Zugänge verfügt. So verwundert es nicht, dass gerade die Information über das Ausscheiden eines Benutzers die jeweils betroffenen „Gast-Organisationen“ in vielen Fällen entweder verspätet oder überhaupt nicht erreicht.

Aus Sicht der Benutzer kommt hinzu, dass die Beantragungsprozesse bei den „Gast-Organisationen“ jeweils dort definiert werden und der Benutzer deshalb viele unterschiedliche Beantragungsprozesse durchlaufen muss, die in einer Vielzahl von Accounts mit jeweils unterschiedlichen Benutzernamen und Passwörtern resultieren.

Ein Ansatz zur Lösung dieser Problematik wurde ursprünglich von Microsoft im Rahmen der Passport-Initiative vorgestellt und implementiert. Sie ist im Kern ebenfalls ein zentrales Konzept, bei dem eine Organisations-übergreifende Stelle (in diesem Beispiel: das Unternehmen Microsoft) einen zentralen Dienst bereitstellt, in dem die übergreifend benötigten Benutzerinformationen abgelegt werden.

Dieses Konzept gilt jedoch wegen fehlender Akzeptanz der Anwender als gescheitert. Der Hauptkritikpunkt an einem solchen Konzept war und ist, dass Benutzerinformationen und insbesondere Zugangsinformationen sensitive personenbezogene Daten darstellen, somit dem Datenschutz in besonderem Maße unterliegen und die Kontrolle über sie deshalb nicht an eine andere – d.h. externe - Organisation übertragen werden sollte.

Aus diesem Grund wurde von der IT-Industrie in Zusammenarbeit mit den Anwendern das Konzept der „Föderation" entwickelt, das ein Modell kooperierender, gleichberechtigter Partner darstellt, die ihre Eigenständigkeit behalten und keine „Souveränität" an eine zentrale Stelle abzugeben brauchen.

2 Föderation

Föderation beantwortet die Frage: „Wie kann ein zuverlässiger Zugriffschutz über Organisationsgrenzen hinweg so gestaltet werden, dass der Benutzer nur in seiner eigenen Organisation gepflegt wird und die redundante Verwaltung in allen Partnerorganisationen vermieden wird?"

In der Praxis haben sich dazu mit Liberty Alliance und Shibboleth unabhängig voneinander zwei leicht unterschiedliche Lösungsansätze entwickelt; allerdings auf Basis sehr ähnlicher Prinzipien und unter Nutzung der gleichen Basis-Standards.

2.1 Liberty Alliance

Liberty Alliance ist eine branchenübergreifende Industrie-Initiative mit derzeit (Stand: September 2006) etwa 140 Mitgliedern.

Neben IT-Herstellern (HP, IBM, Intel, Novell, Oracle, Sun, …) sind insbesondere Vertreter aus der Telekommunikation (AOL, Ericsson, France Telecom, NTT, T-Com, Telefonica, Vodafone, …), Finanzdienstleister (Fidelity Investments, American Express, Bank of America, Citigroup, …), aber auch Behörden und Forschungseinrichtungen vertreten.

So ist es nicht verwunderlich, dass die Einsatzschwerpunkte derzeit im Behördenumfeld (z.B. US e-Authentication Program) sowie in den Branchen Telekommunikation, Finanzdienstleistungen, aber auch Reise und Touristik liegen. Weitere wichtige Nutzer stellen Industrien wie Flugzeugbau (z.B. Boeing) und die Automobilindustrie dar (z.B. General Motors), die traditionell eine sehr enge Zusammenarbeit mit einer großen Zahl unterschiedlicher Zulieferer pflegen.

Da die Liberty Alliance im Bildungswesen im Vergleich zu Shibboleth (siehe unten) nur eine vergleichsweise geringe Bedeutung besitzt, wird dieses Konzept nicht in größerem Detail beschrieben.

2.2 Shibboleth

2.2.1. Historie

Parallel zu der Entwicklung der Liberty Alliance Spezifikation und unabhängig davon erfolgte die Entwicklung und Implementierung von Shibboleth. Die Entwicklung begann im Februar 2000; mittlerweile liegt die Implementierung in der Version 1.3 vor.

Shibboleth wird unter dem „Internet2 Intellectual Property Framework[1]“ - einer Open Source Lizenz – veröffentlicht und primär im Bildungswesen eingesetzt.

Wegen der Datenschutzanforderungen im US-Bildungswesen aufgrund von FERPA (Family Educational and Privacy Act, 1974) wurde von vorneherein besonderer Wert auf den Schutz personenbezogener Daten gelegt.

Der Name „Shibboleth“ leitet sich aus dem Alten Testament (Buch der Richter, Kap. 12, Verse 5, 6) ab[2]:

> „Und die Gileaditer nahmen ein die Furt des Jordans vor Ephraim. Wenn nun sprachen die Flüchtigen Ephraims: Laß mich hinübergehen, so sprachen die Männer von Gilead zu ihm: Bist du ein Ephraiter?
>
> Wenn er dann antwortete: Nein, so hießen sie ihn sprechen: Schiboleth, so sprach er: Siboleth, und konnte es nicht recht reden. So griffen sie ihn und schlugen ihn an der Furt des Jordans, daß zu der Zeit von Ephraim fielen zweiundvierzigtausend.“

2.2.2. Funktionsweise

Nachfolgend wird die Funktionsweise von Shibboleth anhand eines typischen Einsatzszenarios dargestellt, bei der ein Benutzer auf die Website eines Kooperationspartners (des „Service Providers“ in Abb. 1) zugreift. Er selbst gehört einer anderen Organisation an, bei der er auch verwaltet wird („Identity Provider“ in Abb. 1).

---

[1] http://members.internet2.edu/intellectualproperty.html
[2] http://www.spiritproject.de/orakel/magie/lyrik/bibel/richter.htm

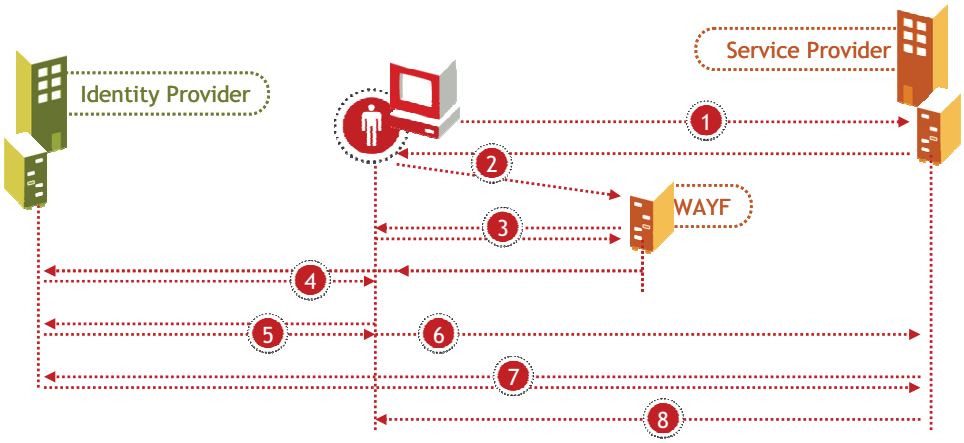

Abbildung 1: Funktionsweise von Shibboleth

1. Der Benutzer versucht, auf eine Website des Service Providers zuzugreifen.

2. Der Service Provider sendet einen Browser-Redirect auf seinen „Where Are You From“ (WAYF) Service. Dort wird dem Benutzer eine Liste der beim Service Provider registrierten Kooperationspartner angezeigt.

3. Der Benutzer wählt seine eigene „Heimat-Organisation“, d.h. den Identity Provider aus und übermittelt diese Information an den WAYF-Service.

4. Der Benutzer wird vom WAYF-Service über einen Browser-Redirect auf die Anmeldeseite des in Schritt 3 ausgewählten zuständigen Identity Providers geleitet.

5. Der Benutzer meldet sich beim Identity Provider mit Benutzername / Passwort an. Dies ist möglich, da er dort bekannt ist und dort auch seine Zugangsdaten verwaltet werden.

6. Der Identity Provider prüft die Zugangsdaten und leitet den Benutzer bei einem erfolgreichen Login über einen Browser-Redirect auf die ursprünglich angefragte Seite beim Service Provider weiter. Dabei fügt der Identity Provider eine sog. Security Assertion in den Request ein, anhand dessen der Service Provider erkennt, dass dieser Benutzer soeben erfolgreich beim Identity Provider authentisiert wurde.

7. Der Service Provider kann optional beim Identity Provider noch weitere Informationen über den Benutzer einholen, aufgrund derer der Service Provider entscheiden kann, ob der Zugriff gewährt werden soll („Attribute Request“). So kann der Service Provider beispielsweise für den Zugriff auf ein Projektverzeichnis abfragen, ob der Benutzer tatsächlich ein Projektmitglied ist. Im Allgemeinen kann der Benutzer dabei vorab festlegen, welche Informationen der Identity Provider tatsächlich bereitstellt. Es liegt allerdings in der Entscheidungsfreiheit des Service Providers, ob er die übergebenen Informationen als ausreichend für den Zugriff erachtet.

8. Basierend auf der im Schritt 6 übertragenen Security Assertion und gegebenenfalls der im Schritt 7 angefragten Zusatzinformationen gewährt der Service Provider Zugriff auf die gewünschte Ressource.

2.2.3. Vorteile

Anhand dieses typischen Einsatzbeispiels lassen sich die wesentlichen Vorteile von Föderation generell und insbesondere von Shibboleth identifizieren:

1. Kein oder zumindest sehr geringer Aufwand für die Verwaltung externer Benutzer für den Service Provider: Im Normalfall ist der Benutzer beim Service Provider namentlich gar nicht bekannt, sondern nur seine Organisationszugehörigkeit („Where are you from?“).

2. Guter Schutz personenbezogener Daten, da sie die „Heimat-Organisation“, d.h. den Identity Provider nicht verlassen müssen.

3. Hoher Benutzerkomfort durch lokale, d.h. einfache und schnelle Prozesse für die Beantragung von Zugriffen sowie durch Web Single Sign On auch über die externen Partnerdomänen hinweg.

4. Dennoch hohe Sicherheit für den Service Provider durch Authentisierung, Autorisierung und Auditfähigkeit: Abhängig von der konkreten Implementierung kann der Identity Provider beispielsweise eine eindeutige Kennung für einen Benutzer vergeben, die an den Service Provider übermittelt wird. Wichtig ist, dass nur der Identity Provider, nicht aber der Service Provider aus dieser Kennung die tatsächliche Identität des Benutzers ermitteln kann. Bei begründeten Ausnahmefällen wie etwa einem Fehlverhalten des Benutzers kann dann der Service Provider vom Identity Provider anhand dieser Kennung die tatsächliche Identität des Benutzers über ein separates Verfahren anfordern.

2.2.4. Voraussetzungen

Die Voraussetzungen für den Einsatz von Föderation lassen sich auf zwei Kernelemente reduzieren: Vertrauen und Interoperabilität.

Da die beteiligten Föderationspartner in der Regel eigenständige Organisationen mit eigener IT-Hoheit darstellen, muss die Interoperabilität der unterschiedlichen Implementierungen gewährleistet sein.

Durch die Lizensierung unter einer Open Source Lizenz sowie der Existenz einer eigenen Referenzimplementierung ist die Interoperabilität zwischen verschiedenen Shibboleth-Installationen weitgehend gewährleistet, wenn sie auch im Einzelfall grundsätzlich getestet und verifiziert werden muss. Allerdings ist aufgrund der Historie die Herstellerunterstützung derzeit noch geringer als im Falle der Liberty Alliance.

Die zweite Voraussetzung – Vertrauen – muss zwischen den Kooperationspartnern vorab geschaffen werden. Konkret muss der Service Provider auf die Qualität der Benutzerverwaltung des Identity Providers vertrauen, da der Service Provider selbst nicht mehr kontrolliert, dass beispielsweise die Zugangsrechte ausgeschiedener Benutzer zeitnah und zuverlässig entzogen werden.

Auf Seiten des Identity Providers setzt dies in der Regel eine funktionierende Infrastruktur für das Management von Identitäten voraus. Da eine Organisation innerhalb einer Föderation in der Regel sowohl die Rolle eines Identity Providers als auch gleichzeitig eines Service Providers darstellt, bedeutet dies, dass die Partner vor der Teilnahme an einer Föderation zunächst ihre jeweiligen Hausaufgaben hinsichtlich des Identitätsmanagements erledigen müssen.

2.3 Zusammenhang zwischen Liberty Alliance und Shibboleth

Wie bereits eingangs beschrieben, adressieren Liberty Alliance und Shibboleth beide die gleiche Fragestellung, nämlich die zuverlässige Authentisierung und Authorisierung von Web-Zugriffen über Domänengrenzen hinweg, ohne dass der Benutzer in allen Domänen redundant verwaltet werden muss.

Sie nutzen dazu insbesondere in den aktuellen bzw. bevorstehenden Versionen identische Basisstandards (http(s), XML, SAML[3]).

Aufgrund der unterschiedlichen Historie legen beide allerdings leicht unterschiedliche Schwerpunkte. Das Konzept von Shibboleth lässt sich zusammenfassen mit: „Ich weiß, woher du kommst.“, während Liberty zusammengefasst werden konnte mit: „Ich weiß, wer du bist.“

Insbesondere die Einführung von SAML V2.0 bewirkt allerdings eine zunehmende Konvergenz zwischen beiden Ansätzen, da viele der vormals getrennten Detailspezifikationen nunmehr durch SAML V2.0 abgedeckt und damit vereinheitlicht werden.

---

[3] Security Assertion Markup Language

Dies betrifft insbesondere auch das sog. „Attribute Sharing“, das es einem Benutzer erlaubt, die an den Service Provider übertragenen persönlichen Informationen innerhalb eines voreingestellter Rahmens zu begrenzen. Dieser Mechanismus wurde ursprünglich nur von Shibboleth unterstützt, steht mit SAML V2.0 nun allerdings auch in Liberty zur Verfügung.

Basisfunktionen wie die reine Authentisierung sollten aufgrund der gleichen Basisstandards interoperabel sein, wenngleich Praxistests auch noch ausstehen (Stand: Juni 2006).

Im Detail bestehen allerdings immer noch kleinere Unterschiede im Kommunikationsprotokoll zwischen Identity Provider und Service Provider, sodass die Interoperabilität für weitergehende Funktionen wie beipielsweise die Abfrage zusätzlicher Informationen („Attribute Request“) noch nicht gegeben ist.

Die Beziehung zwischen Liberty Alliance und Shibboleth wird deshalb am besten durch eine „friedliche Koexistenz“ beschrieben. Dies zeigt sich auch darin, dass Internet2 - das Standardisierungsgremium für Shibboleth – nunmehr auch Mitglied der Liberty Alliance ist.