



Fachbereich Informatik
Masterstudiengang Angewandte Informatik
Lehr- und Forschungsbereich Kommunikation und Internet
Studienfach Netzwerksicherheit B

Seminararbeit

Identity Management

Heutige IDM Systeme, Technologien und Trends

Juli 2008

Verfasser

Thomas Bottesch
Mtr-Nr: 200424896

Sebastian Feld
Mtr-Nr: 200424920

Betreuer

Prof. Dr. Norbert Pohlmann

Inhaltsverzeichnis

1	Einleitung.....	3
2	Was ist ein Identity Management System?.....	4
2.1	Was versteht man heute unter Identity Management?.....	4
2.2	Identity Management Modelle.....	5
2.2.1	Zentralisiertes IDM.....	5
2.2.2	Föderiertes IDM.....	6
2.2.3	Benutzerzentriertes IDM.....	7
3	Offene Identity Management Standards/Protokolle.....	10
3.1	SAML.....	10
3.1.1	SAML Assertions.....	10
3.1.2	SAML Protokolle.....	12
3.1.3	SAML Bindings.....	13
3.1.4	SAML Profile.....	14
3.1.5	SAML Sicherheit.....	14
3.2	Liberty Alliance.....	14
3.2.1	Zielsetzung der Liberty Alliance.....	16
3.2.2	Liberty Identity Federation Framework (ID-FF).....	16
3.2.3	Liberty Identity Web Services Framework (ID-WSF).....	17
3.2.4	Liberty Identity Services Interface Specification (ID-SIS).....	19
4	Proprietäre Identity Management Lösungen.....	20
4.1	HiPath SIdurity.....	20
4.1.1	DirX Directory Server.....	21
4.1.2	DirX Identity.....	22
4.1.3	DirX Identity Manager.....	23
4.1.4	DirX Access.....	23
4.2	Oracle Identity and Access Management Suite.....	24
4.2.1	Oracle Access Manager.....	24
4.2.2	Oracle Identity Manager.....	25
4.2.3	Oracle Identity Federation.....	25
4.2.4	Oracle Internet Directory.....	25
4.2.5	Oracle Virtual Directory.....	26
5	Fazit & Identity Management Trends.....	27
	Anhang.....	29
	Literaturverzeichnis.....	29
	Abbildungsverzeichnis.....	29

1 Einleitung

In der heutigen Zeit hat jeder Internetbenutzer, der mehrere Dienste und Anwendungen einsetzt, bereits mehrere Benutzerkonten bzw. Identitäten. Im Regelfall hat ein Benutzer pro Dienst einen Datensatz, in dem der Login-Name und das Passwort abgespeichert ist. Diese Datensätze stellen erhebliche verwaltungstechnische, kostenintensive und sicherheitsspezifische Probleme sowohl für den Anbieter, der diese Daten verwalten und schützen muss, sowie für den Benutzer, der sich zu jedem Dienst ein anderes Passwort merken muss, dar. Identity Management Systeme können die Lösung der genannten Probleme darstellen. Um einen „Identitätenkollaps“, bezogen auf zu viele Daten, Sicherheitsprobleme und hohe Kosten im Internet, zu vermeiden, bedarf es einer neuen Organisation der Nutzermerkmale und -daten, sowie neuer Identifikationslösungen. Die Basis dieser Systeme ist die Authentifizierung, das heißt, die Überprüfung einer angegebenen Identität auf Echtheit. In diesem Bereich gibt es sehr unterschiedliche Technologien und Ansätze, welche in den folgenden Kapiteln beschrieben werden.

2 Was ist ein Identity Management System?

Die oben genannten Probleme können von Identity Management (IDM) Systemen teilweise oder gar komplett gelöst werden. In IDM Systemen werden die Identitätsdaten auf eine spezielle Art und Weise konsistent gehalten, wodurch sich neue administrative Möglichkeiten bieten, um beispielsweise Prozesse zu automatisieren und somit Kosten zu sparen. Zusätzlich bieten IDM Systeme oft innovative Technologien, um eine sichere und benutzerfreundliche Authentifizierung zu ermöglichen. Innerhalb von IDM Systemen werden eine Vielzahl von verschiedenen Technologien, Protokollen und Standards verwendet, die in den folgenden Kapiteln genauer beschrieben werden.

2.1 Was versteht man heute unter Identity Management?

Spricht man heute von Identity Management bzw. IDM Systemen, so umfassen diese Begriffe eine Vielzahl von verschiedenen Teilbereichen bzw. Komponenten. Diese Komponenten sind:

Identitätsverwaltung

Identitätsdaten werden von unterschiedlichen Diensten und Anwendungen an zahlreichen Stellen gespeichert. Die große Zahl an Identitätsdaten zu einem Identitätsdatensatz zusammen zu fassen oder zumindest synchron zu halten ist eine der Hauptaufgaben eines IDM Systems und Aufgabe der Identitätsverwaltung.

Berechtigungen

Die Berechtigungskomponente eines IDM Systems hat die Aufgabe eine anwendungsübergreifende Berechtigungs- und Richtlinienverwaltung durchzuführen. Die Verwaltung und Zuordnung von Rollen, Rechten und Gruppenzugehörigkeit kann somit automatisiert durchgeführt werden.

Provisioning

Wird in einem Unternehmen ein neuer Mitarbeiter eingestellt, so ist es notwendig ihm einige E-Mailadressen, Accounts, Berechtigungen und Passwörter bereitzustellen. Dieser Vorgang wird Provisioning genannt. Die Aufgabe der Provisioning Komponente eines IDM Systems ist die Ermöglichung des

automatisierten und übergreifenden Anlegens, Ändern und Löschs von Benutzerdaten und Berechtigungen auf unterschiedlichen Systemressourcen.

Access Management

Basierend auf Benutzeridentitäten trifft diese Komponente Entscheidungen darüber, ob der Identität Zugriff auf bestimmte Ressourcen gewährt oder verweigert wird. Diese Entscheidungen werden basierend auf einer bestimmten Policy getroffen. Zusätzlich hat das Access Management noch die Aufgabe diese Zugriffsentscheidungen durchzusetzen.

Identifizierung und Authentifizierung

Die Authentifizierung stellt einen der größten Stützpfeiler des Identity Managements dar. Im Internet ist es oft notwendig die Identität eines Benutzers festzustellen, um diesem Benutzer bestimmte Ressourcen zuzuordnen. Ein Beispiel hierfür ist der kontrollierte Zugriff auf die E-Mails des Benutzers. Am Allgemein gebräuchlichsten ist die Authentifizierung mittels Benutzernamen und Passwort. Es gibt jedoch viele weitere Authentifizierungsverfahren wie z.B. die Authentifizierung mittels digitalen Zertifikaten.

2.2 Identity Management Modelle

Es gibt grob definiert drei verschiedene Modelle, nach denen heutzutage die gebräuchlichsten Identity Management Systeme aufgebaut sind. Diese Modelle sollen im Folgenden erläutert werden.

2.2.1 Zentralisiertes IDM

Beim zentralisierten Identitätsmanagement versucht man alle Identitätsinformationen an einem zentralen Platz zu speichern. Dieser Ansatz geht von einem zentralen Management aus, das eine kompletten Zugriff auf sämtliche digitalen Identitäten und Ressourcen hat.

Voraussetzung und gleichzeitig größter Kritikpunkt an diesem Modell ist die Tatsache, dass man dieser zentralen Instanz vollkommen vertrauen muss.

2.2.2 Föderiertes IDM

Bei einem föderierten IDM werden digitale Identitäten und IT-Ressourcen dezentral verwaltet. Die Zugriffe einer fremden digitalen Identität auf die Ressourcen der eigenen Unternehmung finden erst dann statt, wenn ein ausreichendes Vertrauen zu dem eigentlichen Halter der Identität besteht und das verwendete Authentikationsverfahren ausreichend für den Zugriff auf die spezielle Ressource ist.

Anhand der folgenden Abbildung wird die Authentikation in einem föderierten IDM System erläutert.

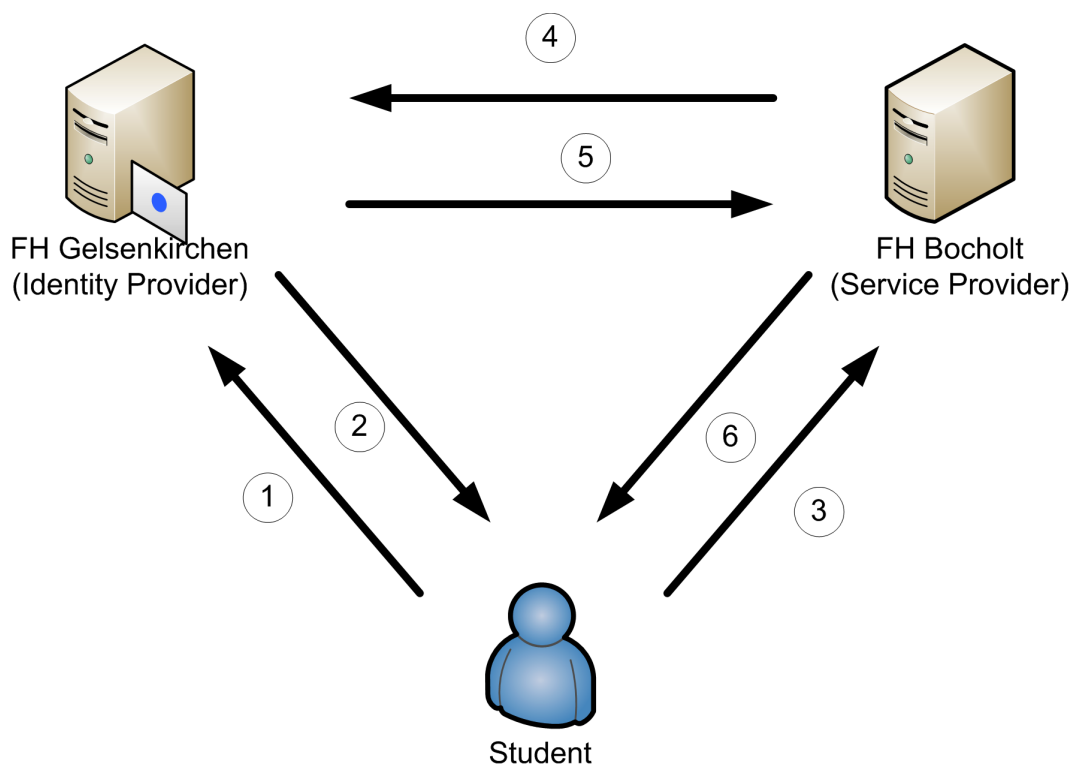


Abbildung 1: Verifikation der Identität des Studenten durch föderiertes IDM

Der Student authentifiziert sich in Schritt 1 auf der Homepage der FH Gelsenkirchen. In Schritt 2 hat FH-GE die Identität verifiziert und eine Session mit dem Studenten wird eröffnet. Nun möchte der Student sich auch einige Skripte der FH Bocholt herunterladen. In Schritt 3 versucht der Student auf die Login-Seite der FH Bocholt zu gelangen, wobei mit übertragen wird, dass er sich schon bei der FH Gelsenkirchen authentifiziert hat. Die FH Bocholt möchte dies natürlich nachprüfen und schickt eine Anfrage an die FH Gelsenkirchen, ob eine Authentifikation des Studenten durch die FH Gelsenkirchen tatsächlich

stattgefunden hat. Die FH-GE bestätigt dies in Schritt 5 und in Schritt 6 wird dem Studenten der Zugang zu den Scripten gewährt.

Um ein föderatives Identity Management zu ermöglichen ist es notwendig, Verträge zwischen allen teilnehmenden Parteien zu schließen, um so ein Vertrauensmodell zwischen Geschäftspartnern aufzubauen.

Vorteile

- Single Sign-On über Organisationsgrenzen hinweg
- Es existieren bereits gute technische Standards zur Realisierung eines föderierten IDM, bspw.: WS-*, SAML, SPML, Shibboleth und auch die Spezifikationen der Liberty Alliance
- Identitätsdaten liegen nicht mehr an einem zentralen Ort
- Gemeinsame Policies über Organisationsgrenzen hinweg können unterstützt werden

Nachteile

- Laufzeit- und Entwicklungskosten müssen von den Organisationen getragen werden
- Wie sieht es mit der Haftbarkeit aus, wenn eine Organisation für einen Bruch der Vertrauenskette verantwortlich ist?
- Großer Aufwand um Verhandlungen mit allen Organisationen zu führen und Vereinbarungen durchzusetzen

2.2.3 Benutzerzentriertes IDM

In einem benutzerzentrierten IDM System hat der Benutzer die komplette Kontrolle über seine Identitätsdaten. Er kann bestimmen wann, wo und wie viele Informationen seiner digitalen Identität er preisgeben möchte. Dies ist ein großer Schritt in die datenschutzrechtlich geforderte informationelle Selbstbestimmung. In einem benutzerzentrierten IDM Szenario gibt es grundsätzlich die drei folgenden Parteien:

- **Authoritative Party (AP)**
bürgt für bestimmte Aspekte einer Benutzeridentität, wenn gefragt
- **Relying Party (RP)**
stellt Ressourcen bereit (z.B. Zugriff auf einen geschützten Bereich), falls ein ausreichender Berechtigungsnachweis vorgelegt wird

– **Identity Agent (IA)**

ein vom Benutzer kontrollierter Agent (z.B. eine Smartcard), der für den Benutzer agiert

Im Folgenden wird die Arbeitsweise eines benutzerzentrierten IDM genauer erläutert.

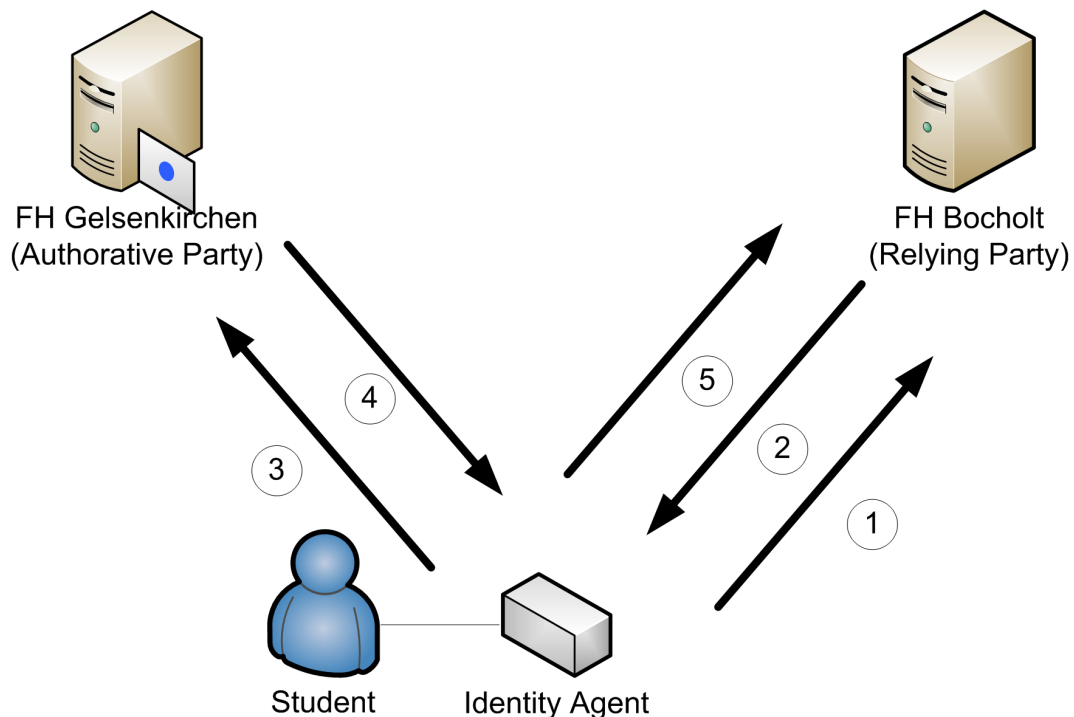


Abbildung 2: Arbeitsweise eines benutzerzentrierten IDM

Erneut möchte der Student auf die Skripte der FH Bocholt zugreifen, wozu er in Schritt 1 eine Anfrage nach den Skripten durchführt. Die FH Bocholt fragt in Schritt 2 nach einem Beweis, dass der Student an der FH GE studiert, da nur Studenten aus Recklinghausen, Gelsenkirchen und Bocholt Zugriff auf die Skripte haben sollen. In Schritt 3 fragt der IA des Studenten bei der FH GE nach einem Immatriculationsbeweis zu seinem Vornamen, Nachnamen und Geburtsdatum. Diese Identitätsdaten sind im Identity Agent gespeichert. Daraufhin erstellt die FH-GE einen nachvollziehbaren Beweis (verschlüsselt, integritätsgeschützt) und sendet diesen Beweis in Schritt 4 an den IA zurück. Der IA sendet daraufhin in Schritt 5 den Beweis an die FH Bocholt weiter und kann somit die Identität des Studenten nachvollziehen. Daraufhin hat der Student

Zugriff auf die Skripte der FH Bocholt.

Vorteile

- Benutzer hat die Kontrolle seiner Identitätsdaten
- Keine Verträge zwischen Organisationen notwendig
- Wird zurzeit sehr von Microsoft und anderen Herstellern gepushed

Nachteile

- Die Technologie ist relativ neu und wird weder von der Benutzern noch der IT komplett verstanden
- Wird nicht von alten Betriebssystemen unterstützt
- Benutzer muss den Umgang mit dem Identity Agent erlernen

3 Offene Identity Management Standards/Protokolle

Zentrales Thema dieser Seminararbeit ist es, ein großes Problem aktueller Identitätsmanagement Systeme aufzugreifen. Heutige IDM Systeme können kaum über Organisationsgrenzen hinweg agieren. Die Autoren dieser Seminararbeit sehen es daher als wichtig an, Technologien vorzustellen, die genau dieses Problem adressieren und eine Lösung bieten. In den folgenden zwei Kapiteln werden daher die Sprache SAML und die Liberty Alliance Spezifikation erläutert.

3.1 SAML

SAML ist eine Abkürzung für Security Assertion Markup Language. Im August 2004 verabschiedete die Standardisierungsorganisation OASIS (Organisation for the Advancement of Structured Information Standards) SAML in der Version 2.0, die immer noch dem aktuellen Stand der Technik entspricht. SAML ist eine auf XML basierende Beschreibungssprache die es ermöglicht auf standardisiertem Weg Sicherheitsinformationen für Autorisierung und Authentifizierung zwischen Anwendungen und IDM-Systemen auszutauschen.

SAML besteht aus 4 Kernkomponenten:

- Assertions
- Protokolle
- Bindings
- Profile

3.1.1 SAML Assertions

Assertions bilden den Kern von SAML und sind definiert als vertrauenswürdige Aussagen einer Asserting Party (AP) bzw. Identity Providers (IP) an eine Relying Party (RP) bzw. Service Provider (SP).

Es gibt 3 Arten von Assertions:

Authentication Assertion

Mit dieser Assertion bestätigt die AP der RP, dass ein Benutzer auf bestimmte

Ressourcen zugreifen darf.

Die Inhalte und die Funktionsweise einer Authentication Assertion werden anhand der folgenden Grafik detailliert beschrieben.

```
<saml:Assertion
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
AssertionID="VN5zxvNB+vtelx5uiOdbKHtVmH+u"
IssueInstant="2002-12-20T06:39:36Z"
Issuer="http://www.portal.com"
MajorVersion="1"
MinorVersion="0" >
  <saml:Conditions NotBefore="2002-12-20T06:39:35Z"
NotOnOrAfter="2002-12-0T06:40:06Z" >
    <saml:AudienceRestrictionCondition >
      <saml:Audience>http://www.greetings.com</saml:Audience>
    </saml:AudienceRestrictionCondition >
  </saml:Conditions >
  <saml:AuthenticationStatement AuthenticationMethod = "Password"
AuthenticationInstant="2002-12-20T06:39:36Z" >
    <saml:Subject >
      <saml:NameIdentifier>Customer'sLoginName</saml:NameIdentifier>
      <saml:SubjectConfirmation >
        <saml:ConfirmationMethod >
          urn:oasis:names:tc:SAML:1.0:cm:artifact-01
        </saml:ConfirmationMethod >
      </saml:SubjectConfirmation >
    </saml:Subject >
  </saml:AuthenticationStatement >
</saml:Assertion >
```

Abbildung 3: SAML Authentication Assertion

In Abbildung 3 ist eine in XML kodierte Authentication Assertion zu erkennen. Das Attribut IssueInstant gibt an, wann die Assertion erstellt wurde. Issuer gibt an welche Asserting Party, in diesem Fall „http://www.portal.com“, die Assertion erstellt hat. Das XML Tag saml:Conditions gibt Konditionen an, die für diese Assertion gelten. NotBefore gibt an, dass die Assertion nicht vor einem bestimmten Datum und Uhrzeit gültig ist. NotOnOrAfter gibt an, dass die Assertion nach einem bestimmten Datum/Uhrzeit nicht mehr gültig ist. Das Tag saml:AudienceRestrictionCondition beinhaltet alle Relying Partys, für die diese Assertion vorgesehen sind. In unserer Beispiellassertion gibt es lediglich die Relying Party „http://www.greetings.com“.

Wie genau sich ein „Subject“ bzw. Benutzer bei portal.com authentifiziert hat ist in dem Tag AuthenticationStatement festgehalten. AuthenticationMethod gibt an, wie sich ein Benutzer bei portal.com authentifiziert hat – in diesem Fall per Passwort. AuthenticationInstant gibt an, wann diese Authentifikation

stattgefunden hat. Das XML Tag `saml:Subject` enthält Informationen über den Benutzer in Form des `saml:NameIdentifier`, der den Loginnamen des Benutzers bei `portal.com` darstellt. Die `saml:ConfirmationMethod` gibt an, wie der Benutzer sich gegenüber `portal.com` authentifiziert hat. Die Zeile `urn:oasis:names:tc:SAML:1.0:cm:artifact-01` gibt an, dass der Benutzer sich per Browser gegenüber `portal.com` authentifiziert hat. Erhält nun `greetings.com` diese SAML Assertion, so kann basierend auf den oben genannten Informationen entschieden werden, ob die Authentifizierung mit der oben genannten `AuthenticationMethod` ausreicht oder ob eine erneute Authentifizierung für `greetings.com` notwendig ist. Es können durchaus weitere Tags und Attribute in `Authentication Assertions` auftreten.

Attribute Assertion

Eine `Attribute Assertion` bestätigt, dass einem Benutzer bestimmte statische Attribute (Rollen, Funktionen) oder dynamische Attribute (z.B. Kontostandinformationen) zugeordnet sind .

Authorisation Decision Assertion

Mit einer `Authorization Decision Assertion` wird festgelegt, ob ein Benutzer Zugriff auf eine angefragte Ressource erhält. Das bedeutet, dass die Autorisierungsentscheidung nicht von der Ressource selbst, sondern von einer vertrauenswürdigen Instanz getroffen wird.

3.1.2 SAML Protokolle

SAML Protokolle definieren die Art und Weise der Anforderung und Übermittlung von SAML Assertions. Erklärend sei hierfür die folgende Tabelle gegeben.

Protokolle	Beschreibung
Assertion Query und Request	Eine RP fordert bei einer AP entweder eine existierende Assertion mit Hilfe einer Assertion ID an oder bittet um eine oder mehrere Assertions – mit Hilfe von vier Abfragetypen.
Authentication Request	Ein Benutzer möchte bei einer RP authentifiziert werden. Die RP stellt dazu eine Anfrage an eine AP. Diese bestätigt der RP die Authentifizierung des anfragenden Benutzers.
Artifact Resolution	Ein RP stellt eine Anfrage an eine AP. Diese dient dazu, Referenzen auf SAML-Nachrichten aufzulösen, die beim HTTP Artifact Binding übertragen werden. Die AP gibt die SAML-Nachrichten zurück, die zu den empfangenen Referenzen (Artifacts) passen.
Name Identifier Mapping	Mit Hilfe dieses Protokolls kann eine AP aufgerufen werden, die für zwei RPs gültig ist. Diese mappt daraufhin die unterschiedlichen Name Identifier zwischen den beiden RPs.
Single Logout	Dieses Protokoll ermöglicht einen (beinahe-) simultanen Logout von Benutzern mit aktiven Sessions bei mehreren Partys.

Tabelle 1: SAML 2.0 Protokolle

3.1.3 SAML Bindings

SAML Bindings definieren den Transport von SAML Nachrichten über Standard-übertragungsprotokolle. Unterstützt werden in SAML 2.0 HTTP und SOAP. In der nachfolgenden Tabelle sind alle Bindings der Version 2.0 von SAML aufgeführt.

Bindings	Beschreibung
SAML SOAP	Transport über Webservices mit SOAP 1.1
Reverse SOAP (PAOS)	Mehrstufiger Austausch von SAML Nachrichten über SOAP 1.1
HTTP Redirect	SAML-Nachrichten werden über HTTP Redirect transportiert.
HTTP POST	SAML-Nachrichten werden base64-encoded in einem HTML-Formular abgelegt und über Onload-Submit an die RP gepostet.
HTTP Artifact	Es wird nur die Referenz (call-by-reference) auf eine SAML-Nachricht (Request oder Response) transportiert, nicht die Nachricht selbst. Dies findet Verwendung vor allem bei Smart-Clients, die keine vollständigen SAML-Nachrichten übertragen können. Die Referenz kann in einem URL-Parameter oder in einem HTML-Formular abgelegt werden, sodass die RP unabhängig vom Smart-Client bei der AP – mit Hilfe der Referenz und des SAML SOAP Bindings – die erwartete SAML-Nachricht abholen kann.
SAML URI	Es wird nur eine URI auf eine SAML Assertion übertragen. Dieses Binding ist unabhängig von SAML-Nachrichten (Request oder Response), es dient allein dazu, dass bei Anfragen an diese URI in dem Element <saml:AssertionIDRef> eine SAML Assertion zurückgegeben wird.

Tabelle 2: SAML Bindings

3.1.4 SAML Profile

SAML-Profile sind Zusammenstellungen von Bindings, Assertions und Protokollen, um spezielle Anwendungsfälle durchzuführen.

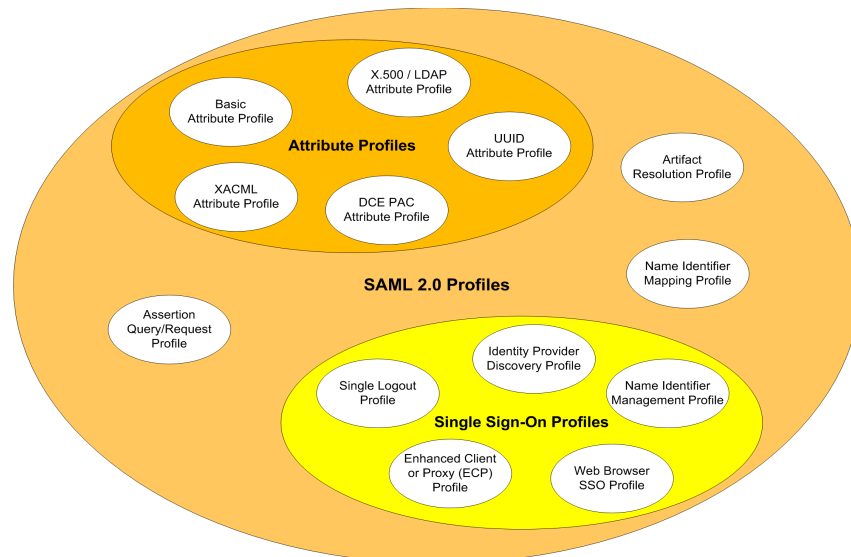


Abbildung 4: SAML 2.0 Profile

3.1.5 SAML Sicherheit

SAML 2.0 enthält keine Mechanismen um SAML Nachrichten zu verschlüsseln. SAML Assertions sind jedoch digital signierbar. Für einen sicheren verschlüsselten Austausch von SAML-Nachrichten empfiehlt die OASIS HTTP über SSL 3.0 bzw. TLS 1.0.

Zusätzlich muss ein Server nach SAML-Spezifikation seine Clients mittels X.509-Zertifikaten identifizieren.

Gelingt es einem Angreifer das SAML-Artefakt (die Referenz auf eine SAML Assertion) gemeinsam mit der URL zu rekonstruieren, so kann er sich als der entsprechende Anwender ausgeben. Um diese Gefahr möglichst gering zu halten, sollte beispielsweise die Gültigkeitszeit von SAML-Assertions, die mit den Attributen „NotBefore“ und „NotOnAfter“ festgelegt werden, möglichst gewählt werden.

3.2 Liberty Alliance

Das Liberty Alliance Projekt ist eine aus mehr als 160 Firmen bestehende Arbeitsgemeinschaft, die seit September 2001 Richtlinien und offene Standards entwickelt. Hierbei liegt der Fokus auf zwei groben Themen. Zum einen soll ein dezentrales Single Sign-On geboten werden, bei dem Pseudonyme als SSO-Identitäten eingesetzt werden, um die Privatsphäre der Benutzer zu schützen. Zum anderen wird die unternehmensübergreifende Zusammenfassung (Föderation) von Benutzerkonten reglementiert, bei der die ausdrückliche Zustimmung des Nutzers im Vordergrund steht.

Erreicht werden soll dieses Ziel durch den Aufbau von vertrauenswürdigen Verbunden von Unternehmen, den so genannten „Circle of Trust“ (CoT), um die Vertrauensbeziehungen für den Benutzer transparent im Hintergrund abwickeln zu können. Solche CoT sollen auch die Möglichkeit erhalten sich untereinander zu verbinden, wodurch vielfältige Unternehmen und Dienste dem Benutzer zur Verfügung gestellt werden können.

Die Architektur der Liberty Alliance besteht aus drei großen Komponenten (vgl. Abbildung 5), welche nach einer Schilderung der Zielsetzung der Liberty Alliance näher beleuchtet werden.

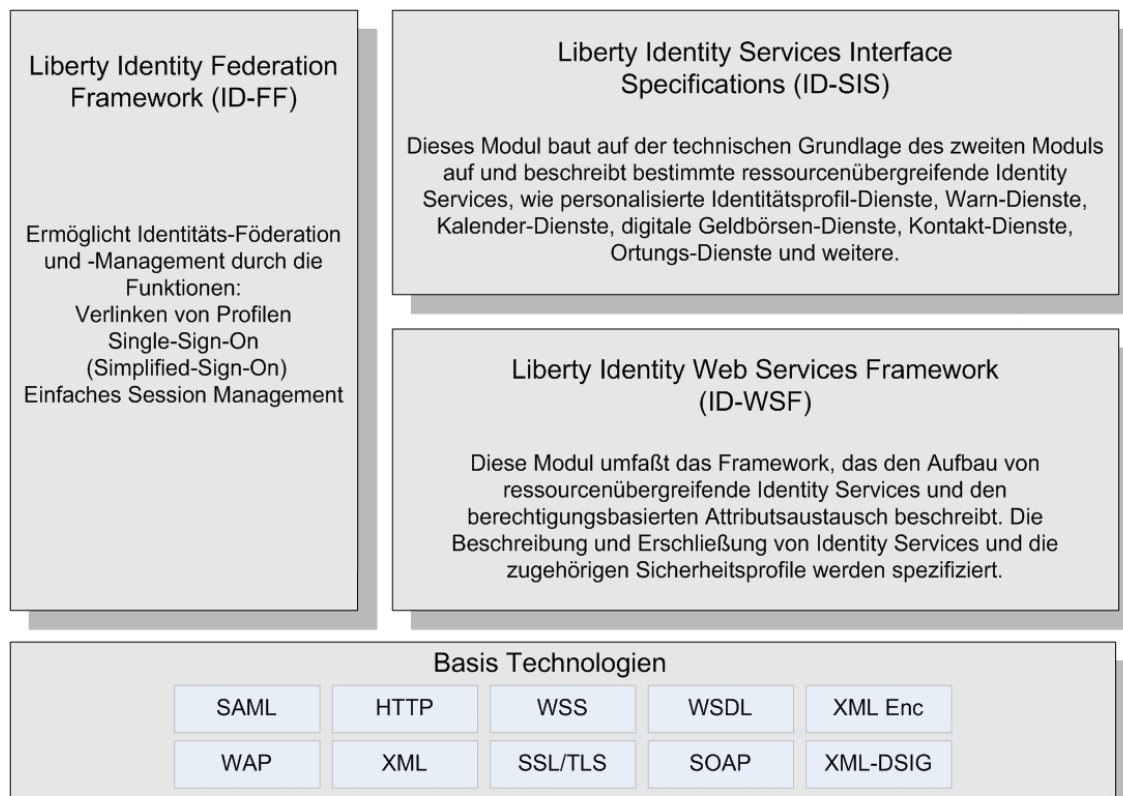


Abbildung 5: Die dreigeteilte Architektur der Liberty Alliance mit den von ihr benutzten Basis Technologien

3.2.1 Zielsetzung der Liberty Alliance

Die Liberty Alliance hat sich die folgenden Ziele gesetzt:

- Erstellung einer Spezifikation für föderierte Identitäten und identitätsbasierte Web Services, die auf offenen Spezifikationen basiert.
- Suchen nach Lösungen zum Schutz vor Identitätsdiebstahl
- Bereitstellung einer Interoperabilitäts-Test Infrastruktur zum Testen neuer Produkte, die auf den Liberty Alliance Produkten basieren
- Anbieten einer Zertifizierung für Produkte, welche die Liberty Spezifikationen benutzen
- Öffnung für Kooperationen mit anderen Standards, Unternehmen und der Regierung
- Aufklärung der Benutzer über Identitäts- und Datenschutzprobleme

3.2.2 Liberty Identity Federation Framework (ID-FF)

Wie bereits angesprochen wurde, liegt das Konzept der Liberty Alliance in der Föderation und Verwaltung von Identitäten. Es soll die Verknüpfung von verschiedenen Benutzerdaten innerhalb einer Gruppe von Unternehmen, dem Circle of Trust, kontrolliert ermöglicht werden. Hierfür bietet das Framework ID-FF die Grundlagen.

Ein grundsätzliches Verfahren für den Zusammenschluss von Identitäten ist die Benutzung von „Federated Name Identifier“. Die Idee hierbei ist, dass eine Föderation von Informationen ohne die Preisgabe der gesamten Identitätsdaten ermöglicht werden soll. Ein Wetterdienst soll beispielsweise in der Lage sein den aktuellen Aufenthaltsorts eines Benutzers zu erfahren, ohne dessen Vor- und Nachnamen zu kennen.

Technologisch gesehen liegt diesem Framework SAML 2.0 (vgl. Kapitel 3.1) zugrunde. Aufgrund dessen bietet die Liberty Alliance auch verschiedene Protokolle, Profile und Bindings. Durch Kombination des ID-FF und SAML wird die Möglichkeit eines Single Sign-On innerhalb einer föderierten Identität geboten. Hat ein Benutzer also mehrere Accounts und schließt er diese zu einer Föderation zusammen, so muss er sich lediglich einmal in dieser Föderation anmelden und hat Zugriff auf alle Dienste sämtlicher Teilnehmer der Föderation.

Entsprechend ist es auch notwendig die Session bei einem Logout mit allen Teilnehmern der Föderation zu beenden. Dies wird durch ein „Global Single Logout“ ermöglicht, das alle Teilnehmer über die Beendigung der Session informiert.

3.2.3 Liberty Identity Web Services Framework (ID-WSF)

Das Framework ID-WSF beschreibt die technischen Grundlagen zur Erstellung von interoperablen, identitätsbasierten Web Services. Die Spezifikationen der Interoperabilität ermöglicht Web Services miteinander zu kommunizieren, sowie sich gegenseitig zu authentifizieren. Es soll möglich sein Informationen zu einer bestimmten Personen innerhalb eines Circle of Trusts ausfindig zu machen und einzuholen. Das Einholen der Informationen wird ebenfalls im Framework ID-WSF beschrieben. So wird definiert, dass eine ausdrückliche Erlaubnis vorliegen muss, bevor Benutzerinformationen weitergegeben werden können.

Technisch gesehen identifizieren sich nicht mehr Personen, sondern so genannte „Principals“. Dies sind die zu authentifizieren Größen, können also Personen, aber auch Web Services sein. Kommuniziert wird hier mittels SOAP-Nachrichten in Kombination mit SAML.

Anwendungsbeispiel ID-FF und ID-WSF

Zunächst ein paar Definitionen:

Web Service Provider (WSP)

Ein WSP bietet identitätsbasierte Web Services an.

Web Service Client (WSC)

Der WSC (Principal) ruft einen identitätsbasierten Web Service beim WSP auf.

Discovery Service (DS)

Ein DS ist ein Verzeichnisdienst, in dem WSPs ihre Web Services registrieren können. Zudem werden hier Web Services vom WSC registriert, die er für andere Web Services zur Nutzung frei gibt.

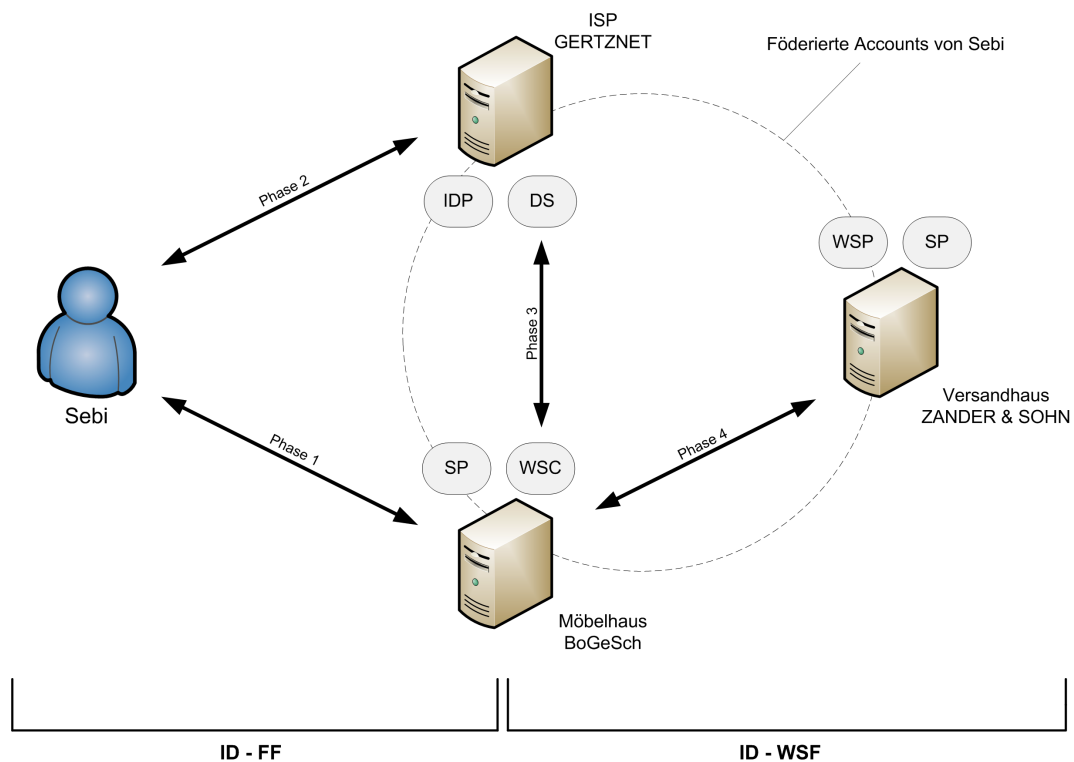


Abbildung 6: Benutzer Sebi möchte über seine föderierten Accounts ein Wasserbett bestellen

Benutzer Sebi besitzt drei Accounts. Ein Account existiert beim Internet Service Provider GERTZNET, ein weiterer beim Möbelhaus BoGeSch und der letzte Account befindet sich beim Versandhaus ZANDER & SOHN. Der ISP GERTZNET ist in diesem Szenario der Identity Service Provider (IDP) und stellt gleichzeitig auch einen Discovery Service (DS) bereit.

Die oben genannten drei Accounts hat Sebi föderiert und möchte nun ein Wasserbett bei BoGeSCH bestellen.

Zunächst loggt sich Sebi in Phase 1 beim Möbelhaus ein. Das Möbelhaus BoGeSch erkennt, dass Sebi's Identity Service Provider der ISP GERTZNET ist. Das Möbelhaus leitet Sebi nun in Phase 2 zu seinem IDP um, damit dieser sich bei seinem ISP anmeldet. Der IDP sendet Sebi nun ein Artefakt, das der Benutzer an das Möbelhaus, welches in diesem Fall als Service Provider (SP) fungiert, weiterleitet. Durch dieses Artefakt ist es dem Möbelhaus nun möglich nachzuvollziehen, dass der Benutzer sich erfolgreich in seiner Föderation angemeldet hat. Damit ist der Single Sign-On komplett. Als nächstes benötigt

BoGeSch die Adresse von Sebi. Hierzu fragt BoGeSch mit dem bereits bekannten Artefakt beim Discovery Service an, ob es einen Teilnehmer der Föderation von Sebi gibt, der dessen Adresse kennt (Phase 3). GERTZNET meldet, dass Sebi das Versandhaus ZANDER & SOHN zur Bereitstellung der Adressdaten definiert hat und übermittelt sogleich die notwendigen Daten, um eine solche Anfrage stellen zu können. Mit diesen Credentials kann das Möbelhaus nun in Phase 4 eine identitätsbasierte Anfrage an Z & S schicken. In diesem letzten Dialog fungiert BoGeSch nun als Web Service Client und Z & S als Web Service Provider. Z & S liefert letztendlich die Adresse an BoGeSch und das Wasserbett kann verschickt werden.

3.2.4 Liberty Identity Services Interface Specification (ID-SIS)

Die Service Interface Specification setzt auf die bereits angesprochenen Frameworks ID-FF und ID-WSF auf. Mit dem ID-SIS soll grob gesprochen eine Schnittstelle definiert werden, welche die Anbindung von erweiterten und vernetzten Diensten möglich macht. Es wird spezifiziert, wie unterschiedliche Identitätsinformationen standardisiert ausgetauscht werden sollen.

Zurzeit bietet das ID-SIS Spezifikationen für Dienste der folgenden Bereiche:

- Directory Access Protocol
- Content SMS/MMS
- Personal Profile Service
- Employee Profile Service
- Contact Book Service
- Geolocation Service
- Presence Service

Als ein Beispiel sei der Geolocation Service heraus gegriffen. Der Principal bestimmt einen Web Service Provider und registriert ihn beim Discovery Service als eine Art Informant für dessen Geoinformationen. Möchte nun ein weiterer Web Service Geoinformationen über den Principal erhalten, so kann dieser standardisiert mittels des Geolocation Service über den DS diese Informationen erhalten.

4 Proprietäre Identity Management Lösungen

Im Zuge dieser Arbeit soll nicht nur ein Überblick über die offenen Standards und Technologien von IDM Systemen gegeben werden, sondern auch eine, wenn auch kurze, Einsicht in bestehende, proprietäre Lösungen. Es existiert eine Vielzahl an Implementierungen, wobei in dieser Arbeit nur zwei solcher Frameworks exemplarisch dargestellt werden sollen. Es handelt sich um die IDM Lösungen von Siemens und von Oracle.

4.1 HiPath Scurity

Die erste vorzustellende Identity Management Lösung ist das Framework „HiPath Scurity“. Es wird vom Bereich Identity & Access Management der Consultingeinheit der Siemens Enterprise Communications GmbH & Co. KG entwickelt und betreut. Das Framework setzt seinen Schwerpunkt auf den Schutz von Ressourcen sowohl innerhalb des einsetzenden Unternehmens als auch firmenübergreifend.

Siemens HiPath Scurity setzt sich aus den folgenden Komponenten zusammen (vgl. dazu auch Abbildung 7):

- DirX Directory Server
- DirX Identity
- DirX Identity Manager
- DirX Access

Des weiteren bietet Siemens ein passendes Smart Card-Portfolio an, welches von der Karteninfrastruktur und den erforderlichen Lesegeräten bis hin zu einer engen Integration mit den HiPath Scurity Solutions geht. Im Zuge dieser Arbeit wird hierauf nicht weiter eingegangen.

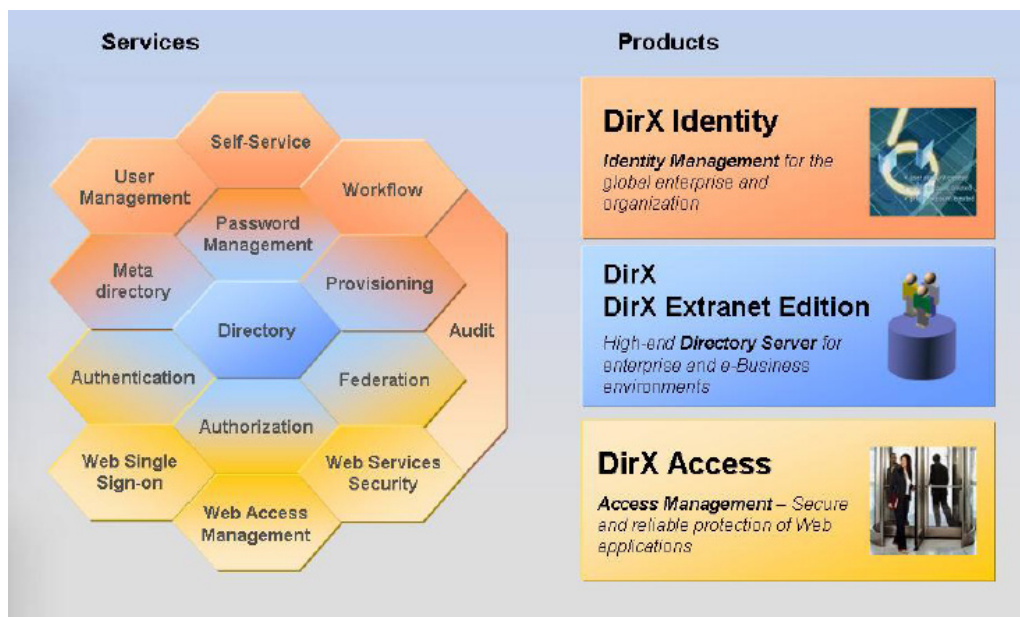


Abbildung 7: Die Komponenten des Frameworks HiPath Scurity und ihre Aufgaben

4.1.1 DirX Directory Server

Das Kernstück dieses IDM Systems bildet ein Verzeichnisdienst (engl. „directory service“), der als zentrales Metadirectory eingesetzt werden kann und eine zentrale Sammlung von Daten verschiedenster Art ermöglicht. Es können Informationen über Identitäten wie bspw. Personen, Organisationen oder Netzwerkkomponenten gespeichert werden. Diese Informationen wiederum können aus E-Mail-Adressen, Personaldaten, Zertifikate einer PKI oder weiterem bestehen.

Der Directory Server ist zusammen mit DirX Identity (vgl. Kapitel 4.1.2) in der Lage Benutzerinformationen aus verschiedenen bestehenden Systemen zusammenzuführen (Konsolidierung), einen konsistenten Zustand der verschiedenen Daten herzustellen (Synchronisierung) sowie eine möglichst gleichartige Struktur herzustellen (Homogenisierung). Das Produkt dieses Prozesses ist die Bereitstellung einer zentralen und eindeutigen Identität für die Benutzer, ganz gleich ob sie unternehmensintern oder -fremd sind. Zudem können Änderungen nun zentral erfasst und an alle angeschlossenen Systeme verteilt werden.

Technisch gesehen ist der DirX Directory Server eine vollständige

Implementierung des Directory Access Protocol (DAP) aus dem X.500 Standard, welcher den Entwurf eines globalen Verzeichnisdienstes beschreibt und den Rahmen für dessen Konzeption bildet. Des Weiteren ist eine Konformität mit dem Lightweight Directory Access Protocol (LDAP) sowie der Directory Service Markup Language (DSML) gegeben.

4.1.2 DirX Identity

Identity Management befasst sich im Kern mit der Erzeugung und Pflege von Identitäten sowie der Verwaltung von Berechtigungen, Richtlinien, Benutzern und Zugriffen. Die HiPath Security Komponente DirX Identity ist genau hierfür zuständig und benutzt den in Kapitel 4.1.1 besprochenen Directory Server DirX zur Speicherung der Informationen.

Als Basis für die Verwaltung dienen Begriffe wie Zuständigkeiten, Regeln, Policies oder Rollen im Unternehmen. Zusammengefasst spricht man hier von einer rollenbasierten Provisionierung, also einer Zuordnung von Benutzern zu Gruppen und Rollen in Zielsystemen. Über diese Gruppen und Rollen erhalten die Benutzer nun Rechte zur Nutzung von Applikationen oder Diensten. Die Provisionierung stellt also die Möglichkeit dar, Zugriffe für geforderte Ressourcen zu geben, zu überwachen, aber auch zu nehmen.

Sämtlicher Informationsfluss zwischen den verschiedenen am System angeschlossenen Verzeichnisdiensten oder anderen Systemen läuft über DirX Identity. Es können Workflows erstellt werden, die beschreiben, welche Menge an Informationen von welchen Systemen gelesen und an welche Zielsystemen gesendet werden dürfen. Im Umfang des Frameworks HiPath Security ist zudem der DirX Identity Manager, ein komplexes Werkzeug mit grafischer Oberfläche, welches die Administration des Servers unterstützen soll (vgl. Kapitel 4.1.3).

DirX Identity benutzt eine offene Schnittstelle basierend auf der Service Provisioning Markup Language (SPML), einem Standard für den Austausch von Provisionierungsinformationen zwischen verschiedenen Systemen. SPML basiert auf der DSML, welche bereits in Kapitel 4.1.1 angesprochen wurde. Zudem unterstützt es das Protokoll LDAP Data Interchange Format (LDIF) zur Darstellung von Informationen aus einem LDAP-Verzeichnis sowie die XML-Spezifikation Web Services Description Language (WSDL) zum Austausch von

Nachrichten.

4.1.3 DirX Identity Manager

Wie bereits erwähnt dient der DirX Identity Manager als eine grafische Oberfläche zur Erstellung und Verwaltung von Gruppen, Rollen, Privilegien und Workflows. Zudem existiert ein Wizard, der automatisiert bei der Realisierung von kleineren Aufgaben hilft, ohne die Kenntnis der zugrunde liegenden Technologien vorauszusetzen. Bei speziellen Anpassungen oder größeren Aufgaben ist jedoch die Kenntnis der Technologien und des IDM Systems unvermeidlich.

Die technische Grundlage für den DirX Identity Manager bildet ein Java Swing Programm. Die in dem Programm darzustellenden Objekte werden in XML-Dateien hinterlegt und anschließend in Java Beans umgewandelt.

4.1.4 DirX Access

Während sich die zuvor erläuterten Komponenten auf das Identity Management konzentrieren, liegt der Fokus vom DirX Access beim Access Management. Dazu gehört die Überprüfung der Identitäten (Authentication/Authentifizierung) sowie die Vergabe und Umsetzung der Zugriffsrechte (Authorization/Zugriffskontrolle).

In einem ersten Schritt ist es notwendig, einen unternehmensinternen oder -externen Benutzer, der auf Unternehmensressourcen zugreifen will, eindeutig zu identifizieren. DirX Access bietet die Möglichkeit eines flexiblen Access Managements, denn sowohl Benutzername und Passwort, als auch Smart Cards mit Zertifikaten werden unterstützt.

In einem zweiten Schritt muss sichergestellt werden, dass ein authentifizierter Benutzer nur Zugriff auf die Ressourcen erhält, für die er berechtigt ist. Dies wird über definierte Regeln entschieden, wobei das zentrale Verzeichnis sowie die Rolleninformationen hinzugezogen werden.

Weitere Funktionalitäten des DirX Access ist die so genannte Anwenderselbstbedienung sowie der delegierte Administrationsdienst. Dies bedeutet, dass ein Benutzer in der Lage ist Rechte der eigenen Person zu

deligieren, sodass andere Mitarbeiter Assistenzfunktionen übernehmen können.

Zusammenfassend stellt die Komponente DirX Access eine zentrale Autorisierung von Zugriffen bereit und erlaubt zudem ein unternehmensweites und -übergreifendes Single Sign-On für Webanwendungen.

4.2 Oracle Identity and Access Management Suite

Eine weitere proprietäre Identity Management-Lösung ist die „Identity and Access Management Suite“ von Oracle. Hierunter verbirgt sich eine Zusammenfassung von Einzellösungen aus dem Hause Oracle, welche ebenfalls den Schutz von heterogenen IT-Umgebungen gewährleisten soll.

Oracle Identity and Access Management Suite setzt sich aus den folgenden, auch als Standalone-Produkte zu betreibenden Komponenten zusammen:

- Oracle Access Manager
- Oracle Identity Manager
- Oracle Identity Federation
- Oracle Internet Directory
- Oracle Virtual Directory

4.2.1 Oracle Access Manager

Die Komponente Oracle Access Manager kombiniert Identitätsmanagement mit Zugriffskontrolle, sodass eine zentralisierte Authentifizierung, eine regelbasierte Autorisierung sowie ein Auditing bereitgestellt werden kann. Ferner können, ähnlich wie beim IDM-Framework von Siemens (vgl. Kapitel 4.1), Administrationsdienste delegiert und Workflows erstellt werden. Durch die Unterstützung von unterschiedlichen Authentifizierungsmechanismen wie Benutzername und Passwort, X.509-Zertifikate oder Smart Cards wird eine breit gefächerte Single Sign-On-Lösung bereitgestellt.

Technischer Hintergrund des Oracle Access Managers ist das Protokoll LDAP, das Active Directory Service Interface (ADSI) zur Anbindung von Microsofts Active Directory sowie das XML-Schema Extensible Access Control Markup Language (XACML), welches die Darstellung und Verarbeitung von Autorisierungs-Policies standardisiert.

4.2.2 Oracle Identity Manager

Der Identity Manager dient zum Hinzufügen, Ändern, Löschen und Provisionieren von Identitäten innerhalb des Systems. Der auf J2EE basierende Identity Manager verwaltet nicht nur den kompletten Lebenszyklus einer Identität, sondern bietet auch Auditing und Compliance Monitoring, also das Überwachen der Einhaltung von Verhaltensmaßnahmen und Richtlinien.

Durch ein eingebautes Framework zur Erstellung von Konnektoren wird die Kommunikation über Standardprotokolle wie HTTP, SMTP oder FTP ermöglicht. Des Weiteren werden Nachrichtenformate wie CSV, SPML 2.0 oder LDIF unterstützt.

4.2.3 Oracle Identity Federation

Die Komponente Oracle Identity Federation bietet die Infrastruktur, um Identitäten mitsamt ihren Berechtigungen sicher in einer bestimmten Domäne zu verteilen. Diese Domäne kann sowohl ein Unternehmen allein als auch ein Verbund von Unternehmen sein. Hierdurch wird ein unternehmensübergreifendes Single Sign-On ermöglicht, sowie die Integration von unternehmensfremden Identitäten, ohne diesen Datenstamm verwalten zu müssen.

Es werden folgende Protokolle unterstützt:

- OASIS SAML 2.0 (1.0 & 1.1)
- Liberty Alliance ID-FF 1.1 & 1.2
- WS-Federation

4.2.4 Oracle Internet Directory

Der zentrale Identitätenspeicher der Oracle Identity and Access Management Suite ist in dieser Komponente zu finden. Zusammen mit dem Produkt Oracle Directory Synchronization ist der Verzeichnisdienst in der Lage, weitere Verzeichnisse zu integrieren. Es steht somit ein Metadirectory zur Verfügung.

Das Oracle Internet Directory hat als Basis das bereits mehrfach angesprochene Protokoll LDAP in der Version 2 und 3 unter sich.

4.2.5 Oracle Virtual Directory

In Kombination mit der Komponente Virtual Directory ist das Oracle Internet Directory in der Lage, Identitäten aus verschiedenen Verzeichnisdiensten virtuell zu kombinieren und einer weiteren Applikation als eine Datenquelle zu präsentieren. Es können also verschiedene LDAP- und XML-Sichtweisen auf Identitätsinformationen herzustellen, ohne die zugrunde liegenden Daten zu synchronisieren oder zu bewegen.

Realisiert wird diese Fähigkeit mittels LDAP in der Version 3 sowie DSML Version 2.

5 Fazit & Identity Management Trends

Abschließend soll in dieser Arbeit ein Gefühl dafür gegeben werden, in welche Richtung sich das große Gebiet des Identity Managements bewegt. Dazu wurden die folgenden drei großen Konferenzen beleuchtet, die als Schwerpunkt Identitäten haben:

- Net-ID 2006, Berlin
- Net-ID 2007, Berlin
- European Identity Conference 2008, München

Kategorisiert man die auf den Konferenzen gehaltenen Vorträge, so erkennt man diverse Trends. So behandeln im Jahre 2006 und 2007 die Mehrzahl der Vorträge das föderierte Identitätenmanagement sowie Themen rund um eHealth, ePass, eGovernment oder eID-Cards, stets im länderübergreifenden Kontext. Ebenfalls viele Vorträge wurden über benutzerzentriertes Identitätenmanagement gehalten, womit zwei der drei grundlegenden IDM Modelle (vgl. Kapitel 2.2) behandelt wurden.

Benutzerzentriertes IDM wird ebenfalls im Jahre 2008 angesprochen, aber der Trend in diesem Jahr geht mehr in die Richtung von Themen wie Risk Management bzw. Compliance Profiling. Es wird die Erweiterung bestehender IDM-Systeme in Bezug auf Überwachung und Monitoring angesprochen, um beispielsweise internen Datenklau zu erkennen oder um sicherzustellen, ob jeder Benutzer noch die richtigen Rechte besitzt. Es werden Verfahren vorgeschlagen, die das IDM System mit dem Human Resource Management System (HRMS) kombiniert, um Personen, die aus dem Unternehmen ausgeschiedenen sind, die Privilegien zu nehmen.

Ebenfalls in diesen Bereich fällt die Wartung und Pflege von IDM Systemen. Innerhalb von Unternehmen wird oft erkannt, dass eine Diskrepanz zwischen den realen Geschäftsprozessen und deren Abbild im IDM System herrscht. Dies kann sowohl die Effizienz des IDM Systems als auch die Sicherheit mindern, denn durch diese Unstimmigkeiten können Geisterrollen oder -identitäten entstehen.

Eine grundsätzliche Diskussion, welche über den gesamten betrachteten Zeitraum geführt wurde, behandelt die Frage, wie viel Anonymität, Vertrauen und

Kontrolle beim Umgang mit Identitäten von notwendig oder sinnvoll ist.

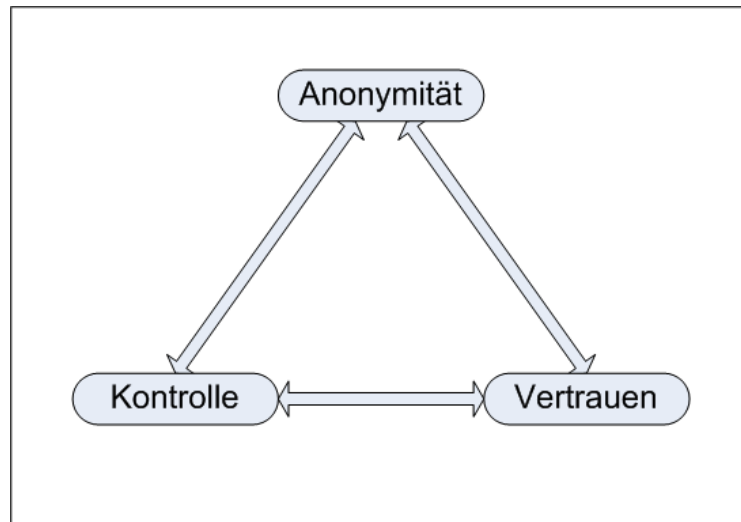


Abbildung 8: Der gegenseitige Einfluss von Anonymität, Vertrauen und Kontrolle

Stellt man beispielsweise einen hohen Anspruch auf Anonymität, so ist die Kontrolle kaum gegeben, auch kann schlecht Vertrauen entstehen (vgl. Abbildung 8). Wenn andererseits die Sicherheit bzw. Kontrolle im Vordergrund steht, so kann nicht auf Vertrauen gesetzt werden und Anonymität ist auch nicht gegeben. Eine universell richtige Herangehensweise ist derzeit nicht vorhanden und so werden die Diskussionen stets weitergeführt.

Das wohl umstrittenste Thema der letzten drei Jahre ist die Biometrie in Verbindung mit Identitäten. Es werden unterschiedliche Verfahren vorgestellt, um Personen anhand von biometrischen Merkmalen zu erkennen. Zudem werden Anwendungsfälle präsentiert, bei denen eine solche Authentifizierung von Personen vorstellbar ist. Während Befürworter beispielsweise die Fälschungssicherheit von biometrisch unterstützten Pässen begrüßen, sehen Kritiker massive Probleme beim Datenschutz. Es wird zum Beispiel befürchtet, dass das unbefugte Auslesen der Daten nicht gewährleistet werden kann und die Kritiker verweisen auf mögliche Straftaten, die anschließend folgen können.

Anhang

Abbildungsverzeichnis

Abbildung 1: Verifikation der Identität des Studenten durch föderiertes IDM	6
Abbildung 2: Arbeitsweise eines benutzerzentrierten IDM	8
Abbildung 3: SAML Authentication Assertion	11
Abbildung 4: SAML 2.0 Profile	14
Abbildung 5: Die dreigeteilte Architektur der Liberty Alliance mit den von ihr benutzten Basis Technologien	15
Abbildung 6: Benutzer Sebi möchte über seine föderierten Accounts ein Wasserbett bestellen	18
Abbildung 7: Die Komponenten des Frameworks HiPath SIdurity und ihre Aufgaben	21
Abbildung 8: Der gegenseitige Einfluss von Anonymität, Vertrauen und Kontrolle	28

Tabellenverzeichnis

Tabelle 1: SAML 2.0 Protokolle	13
Tabelle 2: SAML Bindings	13

Abkürzungsverzeichnis

Abkürzung	Erläuterung
AP	Authoritative Party
ADSI	Active Directory Service Interface
DAP	Directory Access Protocol
DSML	Directory Service Markup Language
IA	Identity Agent
IDM	Identity Management
IP	Identity Provider
ID-FF	Liberty Identity Federation Framework
ID-WSF	Liberty Identity Web Services Framework
ID-SIS	Liberty Identity Services Interface Specification
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
OASIS	Organisation for the Advancement of Structured Information Standards
RP	Relying Party

Abkürzung	Erläuterung
SAML	Security Assertion Markup Language
SP	Service Provider
SPML	Service Provisioning Markup Language
WSDL	Web Service Description Language
XACML	XML-Schema Extensible Access Control Markup Language
XML	Extensible Markup Language