

Autorisierung im Enterprise Federated Identity Management Standards

Christoph Mathys
christoph.mathys at hslu.ch

CC Informations und Software Sicherheit
Hochschule Luzern - Technik & Architektur

11. Juni 2008

Zusammenfassung

Federated Identity Management ist eine reifenden Technologie, die besonders im akademischen Umfeld zusehends an Bedeutung gewinnt. Sie erleichtert die Kommunikation von Identitätsdaten über Firmengrenzen hinweg durch die Definition von Standards wie beispielsweise SAML.

Das erste Kapitel beschäftigt sich mit dem Grundgedanken von Federated Identity Management. Welche Ziele werden damit verfolgt? Welche Gefahren bringt diese neue Technologie mit sich? Im zweiten Kapitel sind dann Ausprägungen dieser Technologie in Form von Protokollen das Thema.

Inhaltsverzeichnis

1	Eine Einführung in Federated Identity Management	2
1.1	Federation - Abstrakt	2
1.2	Federation - Ein Beispiel	2
1.3	Pro und Contra	3
1.4	FIM im Einsatz	3
1.4.1	Switch AAI	3
1.4.2	Boeing	3
1.4.3	American Express	3
2	Standards für FIM	4
2.1	Security Assertion Markup Language (SAML)	4
2.1.1	SAML v1.1	5
2.1.2	SAML v2.0	6
2.2	Liberty Alliance	7

Horw, 11. Juni 2008

1.2 Federation - Ein Beispiel

1 Eine Einführung in Federated Identity Management

Im Internet sind zahlreiche Accounts und Identitäten, auch digitale Identitäten genannt, schon lange die Regel und auch in Firmennetzen an der Tagesordnung. Mit klassischen, proprietären Web Single Sign On-Lösungen (basierend auf Cookies und Agents) und Directory Services (LDAP) kann der Anzahl von verschiedenen Identitäten und Loginverfahren zwar etwas Einhalt geboten werden, doch sind diese Lösungen in der Regel auf ein Netzwerk (Domain of Control) beschränkt. Zusätzlich greifen auch immer häufiger externe User auf interne Ressourcen zu und interne User brauchen Zugriff auf externe Ressourcen. Hier kommt das Federated Identity Management ins Spiel.

1.1 Federation - Abstrakt

Mit dem Begriff *Federated Identity Management* (FIM) ist eine Reihe von Standards, Technologien und Use Cases gemeint, mit denen Identitätsinformationen standardisiert zwischen eigenständigen Sicherheitsdomänen übertragen werden können. Das Ziel ist, dass Benutzer einer Domäne sicher auf Daten oder Systeme einer anderen Domäne zugreifen können, ohne dass dabei eine komplett redundante User-Administration in beiden Domänen nötig ist.

Ermöglicht werden Federations durch offene Standards und/oder offene Spezifikationen und definierte Use Cases, welche die Interoperabilität zwischen verschiedenen Partnern in diesem Szenario gewährleisten. Typische Use Cases sind das Cross Domain Web Single Sign On oder der Austausch von Benutzerattributen zwischen Domains.

Die Partner in einer Identity Federation organisieren sich in Gruppen, die Liberty Alliance nennt sie "Circle of Trust". Dabei einigen sich die Teilnehmer auf gemeinsame technische Standards und organisatorische Spielregeln zum Austausch von identitätsbezogenen Daten. Ein Benutzer kann sich nun innerhalb dieser Gruppe frei bewegen, nachdem er einmal authentisiert wurde.

Der Begriff Identity Federation ist relativ breit gefasst und entwickelt sich stets weiter. Die verschiedenen Formen von Federation sind allerdings soweit Konsistent, als dass sie immer offene Metho-

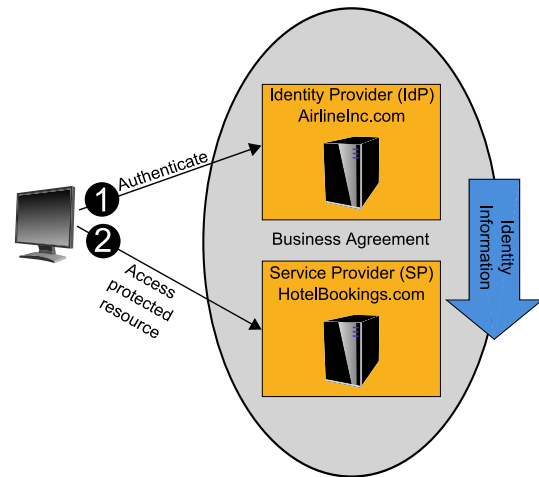


Abbildung 1: Federation anhand eines SAML Beispiels

den, oft basierend auf einem Standard, zur Übertragung von Identitätsinformationen beschreiben (Identity portability). [9]

1.2 Federation - Ein Beispiel

Zur Illustration des obigen Konzepts hier ein einfaches Beispiel aus dem SAML/Liberty-Umfeld (Abbildung 1): Ein Hotel (*hotelbookings.com*) und eine Fluggesellschaft (*airlineinc.com*) haben sich zu einem *Circle of Trust* zusammengeschlossen. Für dieses Beispiel übernimmt die Fluggesellschaft die Rolle des *Identity Providers* (IdP), das Hotel diejenige des *Service Providers* (SP). Der SP vertraut dabei der Authentisierung durch den IdP.

Ein Reisender ist auf der Site von *airlineinc.com* angemeldet und benutzt diese Ressourcen. An einem bestimmten Punkt wechselt er auf die Site von *hotelbookings.com*. Der IdP (also die Fluggesellschaft) versichert nun dem Hotel, dass sich der Benutzer bereits erfolgreich angemeldet hat. Da der SP dem IdP vertraut (Circle of Trust), muss sich der Benutzer nicht erneut anmelden. Im Fall von SAML versichert der IdP dem SP über sogenannte Assertions, dass er den User authentisiert hat. Eine solche Assertion kann zum Beispiel die folgenden Informationen enthalten: "Dieser Benutzer ist John Doe, er hat die Email-Adresse john.doe@example.com, und er wurde mithilfe eines Passwortmechanismus am 11. November um 11.11 CEST in dieses System authentisiert." Der

Horw, 11. Juni 2008

1.4 FIM im Einsatz

SP kann die Daten aus der Assertion verwenden, um zu entscheiden, ob der Zugriff erlaubt wird oder nicht.

1.3 Pro und Contra

Federated Identity Management hat, wie jede andere Technologie auch, seine Vor- und Nachteile, die im folgenden Abschnitt genauer betrachtet werden.

Zu den Vorteilen gehören vereinfachtes Passwortmanagement, einfacherer Zugriff für interne / externe Benutzer und durch Reduktion der Anzahl Accounts und Passworte eine Vereinfachung der Administration. Neben der Reduktion der Anzahl Accounts ist der Hauptnutzen für die Benutzer das weitreichende Web Single Sign On, welches mit Identity Federations einhergeht.

Das korrekte User Provisioning wird ebenfalls vereinfacht, d.h. die Accounts für einen Angestellten rechtzeitig zu erzeugen, anzupassen und zu deaktivieren. In einer einzelnen Firma schon schwierig genug, ist es über Firmengrenzen hinweg beinahe unmöglich, dieser Aufgabe fehlerfrei nachzukommen. Hier hilft Identity Federating, da jede Firma ausschliesslich die Identitäten ihrer eigenen Angestellten verwaltet muss und auch intern von der Federation gebrauch machen kann.

Das blosses Anbieten von Identity Federating kann neue Kunden bringen, sei das nun im Businessumfeld oder im Privatbereich, z.B. bei e-Commerce.

Die Nachteile ergeben sich aus den weitreichenden Zugriffsbefugnissen, die mit einer einzelnen Identität verbunden sind. Gelingt es einen Federated Accounts zu knacken oder auch nur eine Session zu übernehmen, so ist Zugriff auf sämtliche Systeme möglich, für welche die Befugnisse des Accounts ausreichen.

Ein weiterer Nachteil ist die Aufgabe von Kontrolle. Der Authentisierungsprozess wird zum Partner verlagert und steht nicht mehr unter eigener Kontrolle. Durch die engere Verbindung kann bei einem Einbruch ins Netzwerk des Partners ein grösserer Schaden für einen selber entstehen.

1.4 FIM im Einsatz

Diverse Firmen und Institutionen setzen bereits Identity Federations ein. In diesem Kapitel werden drei Beispiele angeführt.

1.4.1 Switch AAI

Authorization and Authentication Infrastructure (AAI) ist eine durch Switch getragene Identity Federation in der Schweizer Hochschullandschaft. Sie erlaubt Studierenden, Dozierenden und Angestellten der angeschlossenen Bildungsinstitutionen den Zugriff auf alle an AAI angeschlossenen Service Provider wie z.B. E-Learning Plattformen.

Erste Untersuchungen starteten 2001. Als Technologie wurde schliesslich Mitte 2002 die Software Shibboleth gewählt, die basierend auf SAML 1.X eine Infrastruktur für Identity Federations bietet. Mitte 2005, nach einer mehr als einjährigen Pilotphase, ging die Infrastruktur schliesslich in den Produktivbetrieb über. 2006 konnten sich bereits über 130'000 Benutzer (zwei Drittel der Gesamtzahl) bei AAI authentisieren.

1.4.2 Boeing

Boeing hat auf Basis von SAML eine Identity Federation aufgebaut. Damit wurden zwei Dinge möglich:

- Die Angestellten und die pensionierten können sich in Boeing Netzwerk einloggen und haben anschliessend Zugriff auf die Informationen zu den Benefits bei jeder der verschiedenen Finanzinstitutionen.
- In einem Pilot wurde mit Southwest Airlines ebenfalls eine Federation aufgebaut, damit die Mechaniker direkt auf die Wartungshandbücher auf den Servern von Boeing zugreifen können, ohne sich am Portal anmelden zu müssen.

Für Boeing fallen damit Kosten von geschätzten \$500-\$1000 pro User pro Monat für die Passwortverwaltung weg.[5]

1.4.3 American Express

Wie viele andere Firmen auch hat American Express zahlreiche Applikationen, Systeme und Integrationen, die über die Jahre designed und deployed wurden. Mit der Zeit sind so verschiedenen "Islands of Identity" entstanden, die grössten sind IBMs RACF, GAs ACF2 und Microsofts Active Directory. Diese Inseln verursachen nicht nur für interne Applikationen einige Kosten, auch die Integration von neuen Partnersystemen ist teuer.

Horw, 11. Juni 2008

2.1 Security Assertion Markup Language (SAML)

ein Benutzer resp. eine Entität (z.B. Computer, Firma) innerhalb einer Security Domain, welche authentisiert werden kann. Es werden drei Arten von Statement in einer Assertion enthalten sein. Ein *Authentication statement* enthält Information zur Identität des Subjects, Loginzeitpunkt und Art des Logins. *Attribute statements* liefern in Form von Name-Value Paaren Details, die zum Subject gehören. Die *Authorization decision statements* geben an, dass ein Subject eine Aktion auf eine Resource anwenden darf.

Protokoll Hier werden die Protokolle definiert, mit denen Asserting und Relying Party miteinander kommunizieren. Eines der Protokolle in SAML ist das Assertion Query and Request Protocol, mit dessen Hilfe eine Relying Party bei einer Asserting Party nach Assertions fragen kann.

Bindings In Bindings wird definiert, wie SAML Protokoll Meldungen in andere Protokolle eingebunden und übertragen werden. Das SAML SOAP Binding beispielsweise gibt an, wie SAML Requests und Responses in SOAP-Meldungen übertragen werden.

Profiles In den Profilen wird definiert, wie Assertion, Protokolle und Bindings kombiniert und beschränkt werden, um einen bestimmten Use Case zu realisieren. Mit den Profilen soll erreicht werden, dass die Interoperabilität von Systemen verschiedener Hersteller möglichst gross ist.

2.1.1 SAML v1.1

SAML 1.0 wurde im November 2002 als OASIS Standard verabschiedet. Einige Monate später, im August 2003, folgte das Update auf SAML 1.1. Das Update brachte kleine Veränderungen am zugrundeliegenden XML Schema und einige Klarstellungen von Verarbeitungsregeln.

SAML 1.1 unterstützt als einzigen Use Case das Web SSO mit zwei verschiedenen Profilen. Beide Profile sind für ein "Source-site-first" Szenario ausgelegt, d.h. der Benutzer muss sich zuerst bei der Source-Site authentisieren ehe er über Links / Redirects zur Zielsite weitergeleitet wird. Als Binding kommt bei beiden Profilen "SOAP over

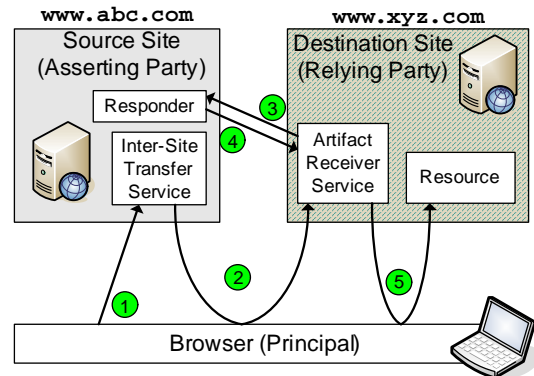


Abbildung 3: SAML 1.1 Browser Artifact Profile - Ablauf

HTTP" zum Einsatz. Das einzige definierte Protokoll ist ein einfaches Request / Response-Protokoll, mit der eine Relying Party von der Asserting Party Assertions anfordern kann.

Die beiden Profile gehen davon aus, dass ein gewöhnlicher Webbrowser benutzt wird. Sie besitzen die folgenden Eigenschaften:

Browser/Artifact Profile Das Profil verwendet ein "Pull"-Modell. Die Relying Party erhält eine Referenz zur Authentication Assertion, die Artifact genannt wird. Mit dieser Referenz kann die Relying Party die Assertion von der Asserting Party holen (pull).

Browser/POST Profile In diesem Profil wird ein "Push"-Modell zugrunde gelegt. Die Assertion wird direkt zur Relying Party gePOSTet (mit http POST).

Abbildung 3 zeigt den Nachrichtfluss bei einem Artifact Profil in einem Source-site-first Szenario. Der Principal hat bereits eine gültige Session in der Source Site *www.abc.com* (d.h. der Principal wurde bereits authentisiert).

1. Der Principal schickt einen Request zum Inter-Site Transfer Service von *www.abc.com* und gibt dabei sein gewünschtes Ziel an, welches hier *http://www.xyz.com* ist. Die URL kann folgende Form haben:

```
https://www.abc.com/  
TransferService?TARGET=<target>
```

Horw, 11. Juni 2008

2.1 Security Assertion Markup Language (SAML)

2. Der Transfer Service erzeugt eine Assertion und das Artifact für den Principal. Das Artifact ist eine Kombination aus der Source ID des SAML Responders von *www.abc.com* und einer Referenz zur Assertion, dem AssertionHandle. Der Service schickt nun dem Browser ein http-Redirect zur Adresse des Artifact Receiver Service mit dem Target und dem Artifact als Parameter. Die URL sieht dann ungefähr folgendermassen aus:

```
http://www.xyz.com/  
ArtifactConsumer?  
TARGET=<target>&  
SAMLart=<artifact>
```

3. Der Artifact Receiver Service der Destination Site extrahiert die Source ID. Das Mapping zwischen Source ID und dem Responder Service wurde bereits durch den Administrator eingerichtet (vorgängig eingerichtet Vertrauensbeziehung) und so findet der Service den SAML Responder der Source Site. Er schickt nun einen SAML Request, der das erhaltene Artifact beinhaltet, zum Responder von *www.abc.com*.
4. Der SAML Responder schickt eine SAML Response zurück, welche die Assertion enthält, welche in Schritt 2 erzeugt wurde und durch das Artifact referenziert wird.
5. Nach Erhalt einer gültigen Assertion leitet der Receiver Service den Principal wiederum mit einem Redirect weiter zum Ursprünglich angeforderten TARGET.

2.1.2 SAML v2.0

Das Liberty Alliance Project, ein Konsortium aus Firmen, Non-Profit- und Regierungsorganisationen, hat nach der Standardisierung von SAML 1.0 eine Extension dafür definiert, das Identity Federation Framework, kurz ID-FF. Später wurde ID-FF an OASIS übergeben und floss in SAML 2.0 ein. Auch vom Projekt Shibboleth, eine Opensource FIM-Lösung von Internet2, erhielt OASIS Input für SAML 2.0. Im März 2005 schliesslich wurde der Standard verabschiedet. SAML 2.0 hat sehr viele Veränderungen gegenüber SAML 1.1 erfahren und ist nicht abwärtskompatibel.

SAML 2.0 definiert eine Reihe von Rollen, die ein System haben kann. Eine *Rolle* definiert, welche SAML Services und Protokolle ein System benutzt und welche Art Assertions erzeugt resp. benötigt werden. Beispiele für Rollen sind *Identity Provider* (IdP), *Service Provider* (SP) oder *Attribute Authority*.

Gegenüber seinem Vorgänger hat SAML 2.0 erhebliche Erweiterungen erfahren. Es gibt eine ganze Reihe von weiteren Protokollen, Bindings und Profilen. Zu den wesentlichen Neuerungen zählen unter anderem die folgenden Features:

- *Metadaten* erlauben, die Konfigurationdaten zwischen verschiedenen SAML-Parties auszutauschen. Die Konfiguration erfasst dabei Bereiche wie die unterstützten Protokolle, zugeordnete Rollen, Keys zum verschlüsseln und signieren von Messages, usw. Das Format dieser Metadaten ist in einem eigenen XML-Format definiert.
- Damit ein Assertion Consumer weiss, wie "sicher" eine Assertion ist gibt es den *Authentication Context*, der beschreibt, wie der Principal authentisiert wurde. Diese Information kann beispielsweise enthalten, wie der User anfänglich identifiziert wurde (z.B. persönlich, online), wie die Kompromittierung der Credentials verhindert wird (z.B. Häufigkeit der Credentialerneuerung, clientseitige Schlüsselerzeugung) oder mit welchem Mechanismus ein User authentisiert wurde (z.B. Passwort, SSL Zertifikat).
- Eine wichtige Neuerung ist die Unterstützung von *Pseudonymen*, mit deren Hilfe ein Principal durch eine zufällige Zeichenfolge bei einem SP repräsentiert wird. Ein Pseudonym wird vom IdP für einen einzelnen SP erzeugt, wobei zwischen *persistenten* und *transienten* Pseudonymen unterschieden wird. Ein transientes Pseudonym identifiziert den Principal nur für diese Session, danach wird es verworfen. Bei einem persistenten Pseudonym merkt sich der IdP, welches Pseudonym der Principal für welchen SP erhält. Ebenso merkt sich der SP, welches Pseudonym welchem seiner lokalen Benutzer entspricht. Dadurch lässt sich der Datenschutz verbessern, da der Principal nicht durch einen globalen Namen zu

Horw, 11. Juni 2008
2.2 Liberty Alliance

identifizieren ist, sondern bei jedem SP einen eigenen Identifikation besitzt. Es ist somit nicht möglich, von der Identität auf SP A auf die Identität auf SP B zu schliessen. Falls genau das allerdings gewünscht wird, also dass mehrere SP den Principal unter dem gleichen Pseudonym kennen, ist dies mit sogenannten *Affiliations* ebenfalls möglich.

- Zahlreiche Online-Dienste verwalten eigene Identitäten. SAML 2.0 erlaubt, lokale Identitäten dynamisch zu einer Federated Identity hinzuzufügen. Die Provider der verschiedenen Services müssen dazu ein entsprechendes Abkommen haben. Das Verknüpfen vom lokalen Account mit dem Federated Account wird auch als *Account Linking* bezeichnet. Das Mittel dazu sind die oben beschriebenen Pseudonyme.
- SAML 2.0 verfügt über Funktionen zum Session Management, konkret das *Single Logout Protocol*. Damit ist es möglich, SSO Session bei verschiedenen SPs praktisch gleichzeitig zu terminieren.
- In Deployments mit mehreren IdPs muss der SP eine Möglichkeit haben um herauszufinden, welchen IdP ein Principal benutzt. Das ist mit dem *Identity Provider Discovery Profile* möglich.
- SAML 2.0 erlaubt, gewisse Teile von Attribute Statements, Name Identifiers oder ganze Assertions mithilfe von XML Encryption zu verschlüsseln. Damit kann die End-zu-End Sicherheit gewährleistet werden.
- Mit den neuen *ECP-Profilen* (Enhanced Client and Proxy) erlaubt SAML auch SSO für Mobile Endgeräte hinter WAP Gateways.

2.2 Liberty Alliance

Die Liberty Alliance ist eine Wirtschaftsinitiative bestehend aus 150 Unternehmen, Non-Profit Organisationen und Regierungsorganisationen mit dem Ziel, Richtlinien, offene Standards und Best Practices für Federated Identity Management zu erarbeiten. Das Projekt wurde 2001 von Sun Microsystems als Reaktion auf Microsofts Passport Service ins Leben gerufen.

Die Liberty Alliance hat ihr Identity Federation Framework (ID-FF) auf der Basis von SAML 1.X

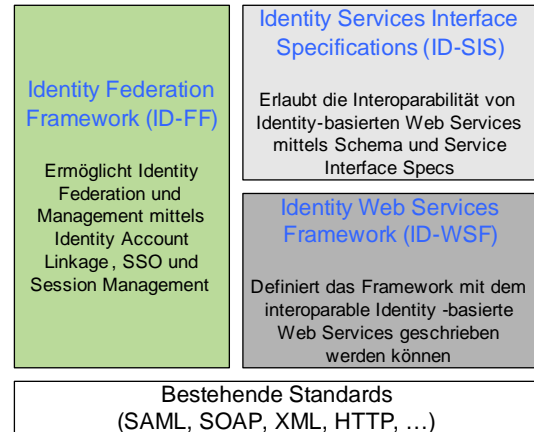


Abbildung 4: Architektur des Liberty Alliance Projekts

definiert und den Funktionsumfang erheblich ausgebaut. Im Juli 2002 wurde Version 1.0 vom ID-FF veröffentlicht, gefolgt von 1.1 im Dezember 2002. Das nächste Release, ID-FF 1.2, wurde schliesslich als Input zu SAML 2.0 an OASIS übergeben. SAML 2.0 hat sehr vieles aus ID-FF übernommen, einige Punkte wurden allgemeiner gelöst, andere einfach anders. Stellenweise ist der Wortlaut in den Standards sogar identisch, trotzdem sind SAML 2.0 und ID-FF 1.2 nicht kompatibel zueinander [4]. Die Unterschiede von ID-FF 1.2 zu SAML 2.0 sind allerdings zu gering, um sie hier genauer zu erörtern.

Das Projekt Liberty Alliance befasst sich über den von SAML abgedeckten Bereich hinaus mit Identity Federations. Dazu wurden bisher drei verschiedene Spezifikationen erarbeitet, welche sich zu der in Abbildung 4 dargestellten Architektur zusammenfügen. Neben ID-FF für WebSSO sind vor allem Identity-basierte Web Services ein wichtiger Teil der Arbeit der Liberty Alliance. Die folgenden beiden Spezifikationen dazu gibt es:

ID-WSF Das Identity Web Services Framework definiert ein gelayertes, SOAP-basiertes Framework zur Implementation und Verwendung von Identity Services. Identity Services sind Webdienste, die Zugriff zu einem bestimmten Aspekt einer Identität gewähren, beispielsweise dem persönlichen Kalender oder derzeitigen Standort eines Principals. In der neus-

Horw, 11. Juni 2008
LITERATUR

ten Version 2.0 setzt das ID-WSF Framework auf SAML 2.0 Assertions zur Kommunikation von Authentisierungs- und Autorisierungsinformationen zwischen den Webservice Aktoren.

ID-SIS Diese Identity Services Interface Specifications definieren eine Reihe von Anwendungen, die auf dem ID-WSF aufbauen. Diese Dienste sind beispielsweise der "Personal Profile Service" oder der "Geolocation Service". Durch die Basis des ID-WSF wird erreicht, dass verschiedene Service Provider diese Dienste nutzen können, ohne dass die Sicherheit oder die Privacy kompromittiert werden.

Literatur

- [1] Digital ID World. Inside American Express's Federated Identity Strategy, Jan/Feb 2004.
- [2] John Hughes and Eve Maler. Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1, May 2004. [sstc-saml-tech-overview-1.1-cd](#).
- [3] Ping Identity. Federated Identity Primer, September 2006.
- [4] Internet2. Differences Between SAML V2.0 and Liberty ID-FF 1.2, Feb 2007. <https://spaces.internet2.edu/display/SHIB/SAMLLibertyDiffs>.
- [5] Bert Latamore. Boeing Pioneers Federated Identity Management with Partners, May 2006. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000324&source=NLT_NTS&nid=107.
- [6] Neil Macehiter. The Identity Web Services Framework (ID-WSF), October 2006. <http://www.it-analysis.com/enterprise/content.php?cid=8872>.
- [7] Paul Madsen and Eve Maler. SAML V2.0 Executive Overview, April 2005. [sstc-saml-exec-overview-2.0-cd-01](#).
- [8] Rick Ragouzis, John Hughes, Rob Philpott, and Eve Maler. Security Assertion Markup Language (SAML) V2.0 Technical Overview, October 2006. [sstc-saml-tech-overview-2.0-draft-10](#).
- [9] Wikipedia. Federated Identity, 2007. http://en.wikipedia.org/w/index.php?title=Federated_identity&oldid=171828368.