SAML/Shibboleth

Florian Mutter

21. Februar 2010

1. SAML

1.1. Einführung

Die *Security Assertion Markup Language* (im Folgenden kurz SAML benannt) ist eine XML-basierte Sprache für den Austausch von Authentifizierungs-, Autorisierungs- und Attributsinformationen über das Internet. SAML wird seit 2001 von OASIS[1] entwickelt und wurde 2002 zum ersten Mal vorgestellt. Im Jahr 2005 wurde die aktuelle Version 2.0 veröffentlicht.

SAML wurde entwickelt, um einen Standard für den Austausch von Sicherheitsinformationen über das Internet zu schaffen. Es wurde dabei darauf geachtet, dass es zwischen verschiedenen Organisationen mit unterschiedlichen Systemen eingesetzt werden kann. Die Entwickler von SAML hatten bei der Entwicklung speziell *Single Sign On* für Webanwendungen, *verteilte Transaktionen* und zwischengeschaltete *Autorisierungsdienste* als Einsatzgebiete für SAML im Kopf.

Unter Single Sign On für Webanwendungen versteht man, dass man sich für verschiedene Dienste nur einmal anmelden muss und dann alle weiteren Dienste, die auf dieselbe Infrastruktur zurückgreifen können, ohne zusätzliche Anmeldung nutzen kann.

Auch verschiedene Webdienste können auf dieselben Sicherheitsmechanismen zugreifen. Diese verteilten Transaktionen könnten zum Beispiel stattfinden, wenn eine Webanwendung die auf eBay aufbaut, die Benutzerverwaltung von eBay benutzt und nicht eine Eigene implementiert.

Autorisierungsdienste können eine Zwischenstation darstellen, an der überprüft wird, ob ein Benutzer auf eine bestimmte Resource zugreifen darf. So könnte eine Firma zum Beispiel über eine Webanwendung sicherstellen, dass nur bestimmte Mitarbeiter bei einem externen Dienstleister Bestellungen aufgeben dürfen.

Im Kontext von SAML spricht man immer von einem *Service Provider* (im Folgenden kurz mit SP benannt) und einem *Identity Provider* (im Folgenden kurz mit IdP benannt). Der SP stellt einen Dienst zur Verfügung, den ein Subjekt in Anspruch nehmen kann. Ein Subjekt kann ein Benutzer sein oder auch ein anderer Dienst, der auf den Dienst des

[1] Organization for the Advancement of Structured Information Standards

SP zurückgreift. Der IdP stellt Informationen über das Subjekt zur Verfügung, wie zum Beispiel den Benutzernamen oder die zugehörige Gruppe. Der IdP muss sich auch um die Authentifizierung des Subjekts kümmern. Dazu wird das Subjekt in der Regel vom SP an den entsprechenden IdP weitergereicht, wo es dann authentifiziert wird. Der SP wird dann vom IdP über eine *Assertion* über den Status der Authentifizierung informiert.

SAML spezifiziert im Wesentlichen vier Teile, wobei die verschiedenen Teile jeweils in anderen Teilen enthalten sind. Den Kern von SAML bilden die *Assertions*. Diese sind eingebettet in die *Protocols* und diese werden in *Bindings* übersetzt. Zusammengefasst wird das Ganze von *Profiles*.

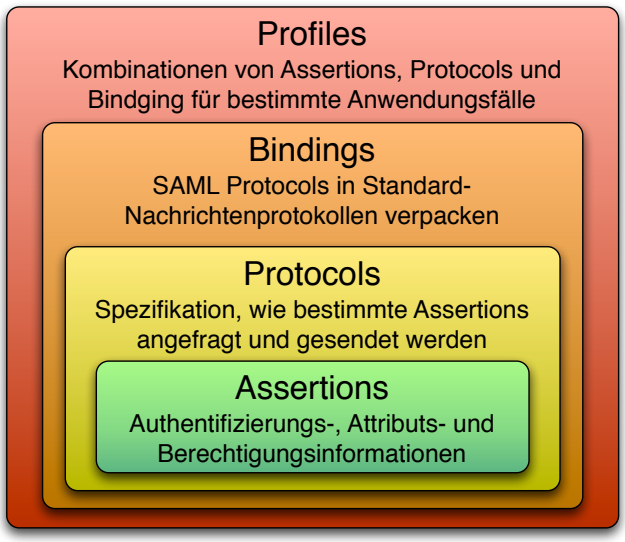

Abbildung 1: SAML Aufbau

1.2. Assertions

Assertions stellen den Kern von SAML dar. Sie enthalten die eigentlichen Informationen, die zwischen den Teilnehmern ausgetauscht werden. Es gibt im Wesentlichen drei verschiedene Arten von Assertions.

Die *Authentication Assertions* werden vom IdP an den SP ausgestellt um ein Subjekt zu authentifizieren. So kann in unserem Beispiel aus der Einführung, eBay eine Authentication Assertion an unsere Webanwendung ausstellen, damit diese sicher sein kann, dass der Benutzer sich korrekt bei eBay angemeldet hat. In den Authentication Assertions sind auch Informationen enthalten, wie lange ein Benutzer angemeldet ist. Es werden Zeiten angegeben, zwischen denen die Assertion gültig ist. Ist dieser Zeitraum abgelaufen, muss eine neue Assertion angefordert und ausgestellt werden.

Die *Attribute Assertions* enthalten verschiedene Informationen zu einem Subjekt. Sie werden benutzt um Informationen über das Subjekt, die der IdP bereitstellt, zum SP

zu übermitteln. Die Kontrolle über die Daten, die herausgegeben werden liegt also beim IdP. So kann der Benutzer zum Beispiel aufgefordert werden, zu bestätigen, welche Daten übermittelt werden. So kann die Privatsphäre des Benutzers geschützt werden.

Die *Authorization Decision Assertions* werden benutzt um Berechtigungsinformationen auszutauschen. Über diese Assertions kann festgelegt werden, ob ein Benutzer auf eine bestimmte Resource zugreifen darf. Diese Entscheidung kann zum Beispiel von einer dritten Instanz neben dem SP und IdP getroffen werden.

1.3. Protocols

Die SAML-Protokolle geben an, wie eine Assertion verpackt sein muss, wenn sie einen bestimmten Zweck erfüllen soll. Es gibt in SAML sechs verschiedene Protokolle. Tabelle 1 enthält eine kurze Beschreibung für alle Protokolle.

Assertion Query and Request Protocol	Über diese Protokoll werden Anfragen zu bestehenden oder neuen Assertions gestellt. Es wird eine Assertion ID benutzt.
Authentication Request Protocol	Es werden Anfragen zur Authentisierung von Subjekten gestellt.
Artifact Protocol	Bietet die Möglichkeit Anfragen zu Assertions über Referenzen aus anderen SAML Nachrichten zu stellen.
Name Identifier Management Protocol	Es können Änderungen des Name Identifier (z.B. Benutzername) ausgetauscht werden.
Single Logout Protocol	Mit diesem Protokoll kann man eine Simultane Abmeldung von mehreren Diensten realisieren.
Name Identifier Mapping Protocol	Dieses Protokoll dient dazu, verschiedene Name Identifier zuzuordnen. SP und IdP müssen nicht den selben Benutzernamen verwenden.

Tabelle 1: SAML Protokolle

1.4. Bindings

SAML Bindings dienen dazu, Assertions in bestehende Standard-Protokolle einzubinden. Es werden verschiedene Protokolle unterstützt, wie zum Beispiel SOAP oder HTTP.

1.4.1. SAML SOAP

SOAP[2] ist ein standardisiertes Protokoll zur Übertragung von XML-basierten Nachrichten. Es bildet daher eine weitere Abstraktionsschicht und kann selbst wieder zum Beispiel über HTTP transportiert werden.

1.4.2. Reverse SOAP (PAOS)

Hier werden die SAML Assertions als SOAP direkt über HTTP verschickt. Die Assertions werden also direkt als HTTP Request vom SP oder IdP verschickt.

1.4.3. HTTP Redirect

SAML Assertions werden über HTTP Redirect transportiert. Der Benutzer wird zum Beispiel automatisch von der Seite des IdP zur Seite des SP weitergeleitet und dabei wird die SAML Assertion direkt in die URL eingebettet.

1.4.4. HTTP POST

SAML Assertions werden über den Browser des Benutzers transportiert in dem ein Formular erzeugt wird, das dann sofort an den Empfänger der Nachricht geschickt wird.

1.4.5. HTTP Artifact

Es wird nur die Referenz auf SAML Assertions übertragen. Diese wird eingesetzt, falls ein Teilnehmer keine vollständige SAML-Nachrichten transportieren kann. Die SAML-Nachricht kann dann zum Beispiel mit SAML SOAP abgeholt werden.

1.4.6. SAML URI

Es wird über eine URI auf eine SAML Assertion zugegriffen, dabei ist die Antwort bereits die SAML Assertion. Dieses Protokoll ist nicht geeignet für die gesamte Kommunikation, sondern wird nur benutzt um einzelne Assertions noch einmal abzufragen.

1.5. Profiles

Es gibt zwei verschiedene Arten von Profilen in SAML. Einmal wurden SAML-Profile definiert um den Einsatzbereich von SAML einzuschränken. Dies erhöht die Kompatibilität zwischen verschiedenen Anwendungen, die auf SAML aufbauen. Des Weiteren sind Abbildungen von anderen Systemen in SAML definiert, zum Beispiel, wie Informationen aus einem LDAP Verzeichnis in SAML abgebildet werden.

Einige Profile können in Kategorien unter den Begriffen „SSO Profiles“ und „SAML Attribute Profiles“ zusammengefasst werden. SSO steht für Single Sign On und fasst alle Profile zusammen, die für Single Sign On-Lösungen benötigt und verwendet werden

[2] vor Version 1.2: Simple Object Access Protocol

können. Die SAML Attribute Profiles sind alle Profile, die Abbildungen von anderen Systemen in SAML darstellen. Über diese Profile werden Attribute zu Subjekten abgefragt. In Abbildung 2 sind alle SAML Profile und die Kategorien aufgeführt.

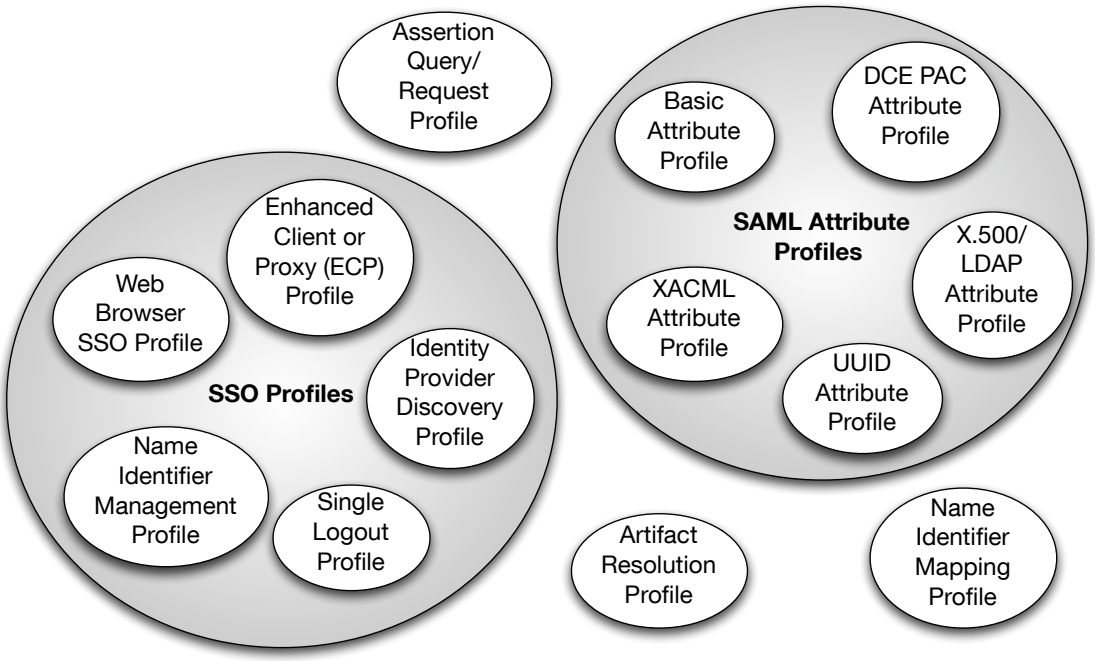

Abbildung 2: SAML Profiles

2. Shibboleth

2.1. Einführung

Shibboleth ist ein Open Source-Softwarepaket zur verteilten Authentifizierung und Autorisierung von Web-Anwendungen. Shibboleth basiert auf SAML und wird hauptsächlich im Bereich Wissenschaft und Lehre eingesetzt. Shibboleth wir von der Internet2 Arbeitsgemeinschaft entwickelt, die 2003 die Version 1.0 veröffentlichte. Die aktuelle Version 2.0 wurde 2008 fertiggestellt. Das Ziel von Shibboleth ist, dass sich jeder Benutzer nur noch einmal bei seiner Heimatorganisation authentifizieren muss und dann auf Dienste zugreifen kann, die andere Organisationen bereitstellen.

Shibboleth bietet eine Single Sign On-Lösung auf Basis von SAML. Die Benutzerverwaltung wird durch Shibboleth erleichtert, da nur eine zentrale Benutzerverwaltung pro Organisation nötig ist. Es müssen keine Benutzer von anderen Organisationen verwaltet werden. Auch der Datenschutz wird berücksichtigt, da zwischen zwei Organisationen nur die Informationen über Benutzer ausgetauscht werden, die von der entsprechenden Anwendung benötigt werden. In der Regel bekommt der Benutzer die zu übertragenden

Daten noch zu sehen und kann den Vorgang abbrechen, wenn er möchte. Shibboleth legt auch die Art der Authentifizierung von Benutzern nicht fest. Shibboleth kann so einfach in eine bestehende Infrastruktur eingebunden werden.

2.2. Föderationen

Um dies zu ermöglichen setzt Shibboleth auf sogenannte Föderationen. Eine Föderation ist ein Zusammenschluss von Organisationen, zum Beispiel Universitäten. Jede Organisation in einer Föderation vertraut den anderen Organisationen, dass diese für eine sichere Benutzerverwaltung sorgen. So kann dann zum Beispiel Universität A den Studenten von Universität B Zugriff auf Lehrinhalt gestatten und muss sich nicht um die Anmeldung oder Verwaltung der Studenten kümmern.

Über Föderationen wird auch technische Unterstützung für Mitglieder der Föderation bereitgestellt und es werden gemeinsame Richtlinien festgelegt, die für einen reibungslosen Betrieb nötig sind.

Es gibt in vielen Ländern Föderationen von Universitäten, so zum Bespiel in Deutschland die DFN-AAI[3] oder InCommon in den USA.

2.3. Aufbau

Wie in SAML zum Teil vorgesehen, setzt sich Shibboleth aus drei Komponenten zusammen. Der *Service Provider*, der *Identity Provider* und dem *Identity Provider Discovery* Dienst. Der SP stellt Resourcen für autorisierte Benutzer zur Verfügung und leitet nicht authentifizierte Benutzer zu ihrer Heimatorganisation weiter, damit diese sich dort authentisieren können. Der SP gibt dann die Resource frei, falls der Benutzer auch autorisiert dazu ist.

Der IdP überprüft die Identität eines Benutzers über *LoginHandler*. Diese können einen Benutzer über verschiedene Methoden authentifizieren, zum Beispiel über Benutzername und Kennwort oder über X.509 Zertifikate. Der IdP verwaltet auch einen Timeout, wie lange der Benutzer angemeldet bleibt, nach dem er sich authentisiert hat. Über eine *User Session* verwaltet der IdP Informationen über angemeldete Benutzer, wie zum Beispiel an welchen Diensten der Benutzer angemeldet ist und oder von welchen er abgemeldet werden muss.

Der IdP Discovery Dienst wählt zu jedem Benutzer, der auf eine Ressource zugreifen möchte und noch nicht authentifiziert ist den passenden SP aus und leitet den Benutzer dorthin weiter. Dazu gibt es mehrere Möglichkeiten. Es kann einmal über ein *Protocol Handler* ein passender IdP gefunden werden, dazu muss der IdP der Benutzers aber bekannt sein. Bei einem *Discovery Handler* muss der IdP des Benutzers nicht bekannt sein, sondern wird dann ermittlet. Die verschiedenen Methoden können auch aneinander angehängt werden, so dass alle durchlaufen werden, bis ein passender IdP gefunden wird. Die Tabelle 2 enthält die Handler und die verschiedenen Methoden der Handler.

[3] Deutsches Forschungsnetz - Authentifizierungs- und Autorisierungs-Infrastruktur

Protocol Handler	SAML2 SessionInitiator
	SHIB1 SessionInitiator
	ADFS SessionInitiator
Discovery Handler	SAMLDS SessionInitiator
	WAYF SessionInitiator
	Cookie SessionInitiator
	Form SessionInitiator

Tabelle 2: SAML Protokolle

A. Weitere Informationen

- OASIS Security Services (SAML) TC
  http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
- SAML XML.org
  http://saml.xml.org/
- Wikipedia: SAML
  http://de.wikipedia.org/wiki/Security_Assertion_Markup_Language
- Shibboleth
  http://shibboleth.internet2.edu/
- DFN-AAI
  https://www.aai.dfn.de/
- Wikipedia: Shibboleth
  http://de.wikipedia.org/wiki/Shibboleth_(Internet)