SAML AS AN SSO STANDARD FOR CUSTOMER IDENTITY MANAGEMENT

How to Create a Frictionless, Secure Customer Identity Management Strategy
PART 1: WHAT IS SAML?
SAML in Context

Security Assertion Markup Language (SAML) is an Extensible Markup Language (XML) standard that enables secure websites and services to exchange user authentication data. SAML-based single sign-on (SSO) standards are designed to create frictionless identity verification and management processes between separate yet affiliated systems.

Dating back to 2001, SAML has evolved to support a range of identity federation and management needs. Some of today’s most popular third-party web applications such as Google Apps, Zendesk, and Salesforce use SAML to authenticate users.

The end goals? Simplify data management. Streamline user flows. Keep customers engaged with your company.

54 percent of companies have difficulty managing and integrating data from today’s many varied sources, while 50 percent are concerned about consistent data quality (Destination CRM).
Exploring Use Cases

SAML has developed a reputation as a solution for employee management for IT teams within nonprofit, government, small business, and enterprise organizations. Internally, organizations use SAML as an SSO service to manage employee, partner and contractor access to network-based applications.

But the applications of SAML extend much further.

Within the past 5-10 years, the rise of ecommerce, social networks, mobile and connected devices has created the need for businesses to develop an external identity access management (IAM) strategy to keep up with the flood of identity data being created as customers connect across channels.
How SAML Stands Out

Where SAML stands out from other authentication mechanisms is that it allows businesses to identify who users are and communicate information about them. Businesses can add structure to disparate user data to tell a rich, compelling story about each user profile.

Below is a hypothetical example for how a membership-only television site can use SAML to better understand and track their customers.

<table>
<thead>
<tr>
<th>SAML: Authorization &amp; Authentication</th>
<th>Other Authentication Standards for Enterprise SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Emily Smith</td>
<td>Name: Emily Smith</td>
</tr>
<tr>
<td>Job Title: Manager at tech company</td>
<td>Email Address: <a href="mailto:emilysmith@testemail.com">emilysmith@testemail.com</a></td>
</tr>
<tr>
<td>Gender: Female</td>
<td></td>
</tr>
<tr>
<td>Level of Membership: Platinum</td>
<td></td>
</tr>
<tr>
<td>Date Joined: 2009</td>
<td></td>
</tr>
<tr>
<td>Interest 1: Travel</td>
<td></td>
</tr>
<tr>
<td>Interest 2: Documentaries</td>
<td></td>
</tr>
<tr>
<td>Interest 3: Stand Up Comedy</td>
<td></td>
</tr>
<tr>
<td>User has permission to access features: Yes</td>
<td></td>
</tr>
</tbody>
</table>
Enterprise organizations rely on multiple service providers -- such as customer support and payment processing software -- to support core user experience goals. Companies will also often team up, through strategic partnership initiatives, to introduce new products and services to shared customer bases.

SAML creates a structured, secure, and scalable process to integrate data between these web applications and authentication processes.
Example: Video Subscription Product

Comcast XFINITY customers can stream content online. Comcast uses SAML to authenticate users, and then to provide authorization information regarding whether the user's subscription includes access to Discovery's online video content.
PART 2: THE TECHNOLOGY
How SAML Works

Think of SAML as a “handshake with an upgrade.” SAML uses something called an assertion document -- an XML file that connects pieces of information -- between a service provider and an identity provider. In contrast, other standards provide identity management using only strings of text, which allow for only a very basic handshake.

SAML’s assertion document is more elaborate and more structured than other standards, making it an ideal identity management solution for enterprise organizations. SAML (1) identifies the user and (2) communicates predefined characteristics about that user. OAuth, in contrast, communicates only an access token, or alpha-numeric string, which can be used to obtain information about the user, but does not provide that information directly.

Sample SAML Assertion for Sites

The following shows the portal_id, organization_id, and siteurl attributes in a SAML assertion statement:

```xml
<saml:AttributeStatement>
  <saml:AttributeValue xml:ns xsi="http://www.w3.org/2001/XMLSchema"
    xsi:ns="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xs:anyType">060900000004cDk</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="organization_id">
  <saml:AttributeValue xml:ns xsi="http://www.w3.org/2001/XMLSchema"
    xsi:ns="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xs:anyType">00D900000003bX0</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="siteurl">
  <saml:AttributeValue xml:ns xsi="http://www.w3.org/2001/XMLSchema"
    xsi:ns="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xs:anyType">https://salesforce.com/mySuffling</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```
The three SAML components include assertions, protocol, and binding.

An assertion is a package of information related to user identity and security. There are three types of SAML assertions: authentication, attribute, and authorization. Authentication assertion is used to validate user identity, attribute assertion contains information about the user, and authorization assertion identifies what the user can do.

SAML protocol refers to how data gets transmitted from the sender to receiver. Sample binding determines how SAML requests map to standard messaging and communications protocols.

SAML works with multiple protocols including Hypertext Transfer Protocol (HTTP) Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP). SAML also supports SOAP, BizTalk, and Electronic Business XML (ebXML).

### Assertion Examples from Membership Video Site:

<table>
<thead>
<tr>
<th>Type of Assertion</th>
<th>Question Asked</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Who is the user?</td>
<td>The user is a valid user.</td>
</tr>
<tr>
<td>Attribute</td>
<td>What do we know about this particular user?</td>
<td>The user is male, 34 years old, lives in Nebraska and subscribes to premium channels such as HBO.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Is the user authorized to access this particular membership area or website feature?</td>
<td>Comcast subscriber who pays for Discovery Channel access can watch Discovery Channel TV shows on XFINITY</td>
</tr>
</tbody>
</table>
## SAML Cheat Sheet

SAML has a lot of moving parts -- it’s a complex topic that is challenging to grasp. We put together the following ‘cheat sheet’ for you to quickly and consistently reference as needed.

<table>
<thead>
<tr>
<th><strong>Federation</strong></th>
<th>In IT, federation describes the process of connecting a person’s electronic identity and attributes, which are typically stored across more than one identity management system. Federation is a means of connecting data, whereas SSO refers to seamless access, with no need for re-authentication.</th>
</tr>
</thead>
</table>
| **Single Sign on (SSO)** | SSO is universal login across multiple applications. When a user logs into one system, she is automatically authenticated across additional sites or touchpoints as she visits them.  
To improve company security and employee convenience, many businesses leverage SSO to allow employees to seamlessly access internal and external applications that are part of an SSO group with a single point of entry and no need for re-authentication. As web-based services and applications multiply, SSO is gaining momentum across consumer-facing properties as well. |
| **Social Login** | Social login is a form of SSO that uses existing login information from social networking services like Twitter or Facebook. Social Login reduces the barriers to register and login to your site, allowing users to authenticate using a preferred pre-existing identity. The Gigya service can be used as an external authentication system, allowing users to login/register to your site using an increasing number of platforms, such as Facebook, Twitter, Google+, Yahoo, LinkedIn and more. Social login is proven to increase registration rates by as much as 90% and provides permission-based access to rich, first-party user data so you can create a completely personalized user experience. |
| **Identity Provider (IdP)** | IdPs are systems that create, maintain, and manage identity information for users, services, and systems. IdPs provide principal authentication to other service providers (known as applications). The social networks mentioned in the above social login example function as IdPs. |
| **Service Provider** | Service providers include software and applications that are requesting identity verification. Service providers use IdP credential services to authenticate users. |
| **Relying Party** | ‘Relying party’ is another term for service provider. |
SAML Visualized: How It All Fits Together

This diagram explains how an example service provider would verify users with an identity provider.

- User attempts to reach a hosted service or application.

- The service or application generates a SAML request, which is encoded and embedded into the URL for the partner’s SSO service. A parameter, set up as an identifier, is passed back without any modification or inspection.

*Image Source: Google*
SAML Visualized: How It All Fits Together (cont’d)

- The application sends a redirect to the user’s browser, which includes the encoded SAML authentication request that should be submitted to the partner’s SSO service.

- The partner decodes the SAML request and authenticates the user.

- The partner generates a SAML response that contains the authenticated user’s username. In accordance with the SAML 2.0 specification, this response is digitally signed with the partner's public and private DSA/RSA keys.

*Image Source: Google*
PART 3:
THE BIG PICTURE -- IS SAML RIGHT FOR YOU?
Companies are collecting volumes of first-party data for product, marketing, business development, and support initiatives. To be action-oriented in creating a high-impact user experience and making a monetization plan, this data needs to be organized into a framework that supports scalable processes -- to break down identity silos and create a consolidated customer profile.

SAML can help bind social and other unstructured profile data with internal profile data attributes via a trusted connection. This structured approach to organizing, analyzing, and using data provides the input to build predictive analytic capabilities, web personalization models, and marketing automation systems.

Over 2.5 exabytes of data are created every single day *(HBR)*.

More than 90% of social media data is unstructured *(Business Insider)*.

90% of all the data in the world has been created in the last two years *(IBM)*.
Addressing Security Risks

Enterprise organizations are targets for security breaches that could put them and their consumers at risk. Your identity management strategy needs to create an extremely secure environment for your businesses and your customers.

SAML requires both the IdP and relying party to register with one another. The two sides exchange encryption keys and the SAML request-response sequence can be signed and validated. This is the most secure verification process available, as the two systems (1) know about each other and are (2) talking to each other directly.

A solution like OpenID, for example, allows a relying party to request authentication from an IdP without prior registration and is used for public authentication. It’s less secure than SAML.

For this reason, SAML is the ideal option for consumer-facing enterprise organizations and companies -- like banks, for instance -- that are looking to engage in secure transactions.
The Balancing Act of Planning

SAML’s strongest benefit is also its biggest challenge.

SAML is much more elaborate than other solutions like OpenID and requires careful pre-planning -- it is much more time consuming to implement than other solutions. You have to configure the sender and the recipient and determine the data structure for your assertion document upfront.

The challenge with SAML is that, in order to make your system work, you have to configure your endpoint configuration as well as the configuration of the sender and receiver. Your system needs to be compatible with the SSO standard, and you’ll need an interface that accommodates your end users.
Where Gigya Fits In

Gigya's Customer Identity Management Platform allows companies to collect, consolidate, and manage first party customer data in the cloud, developing an end-to-end customer identity data management strategy built for today's variety of channels, devices and data.

With the ability to serve as a SAML service provider or identity provider, as well as function as the service provider for social login and any OpenID identity provider, Gigya can help your business choose and implement an SSO standard that meets your business goals.
To learn how Gigya can help provide you with the tools and technology needed to develop a successful SAML strategy, visit gigya.com, or call us at 888.660.1469.

ABOUT GIGYA

Gigya's Customer Identity Management Platform helps companies build better customer relationships by turning unknown visitors into known, loyal and engaged customers. With Gigya’s technology, businesses increase registrations and identify customers across devices, consolidate data into rich customer profiles, and provide better service, products and experiences by integrating data into marketing and service applications.

Gigya’s platform was designed from the ground up for social identities, mobile devices, consumer privacy and modern marketing. Gigya provides developers with the APIs they need to easily build and maintain secure and scalable registration, authentication, profile management, data analytics and third-party integrations.

More than 700 of the world’s leading businesses such as Fox, Forbes, and Verizon rely on Gigya to build identity-driven relationships and to provide scalable, secure Customer Identity Management.

For more details about Gigya, visit www.gigya.com.