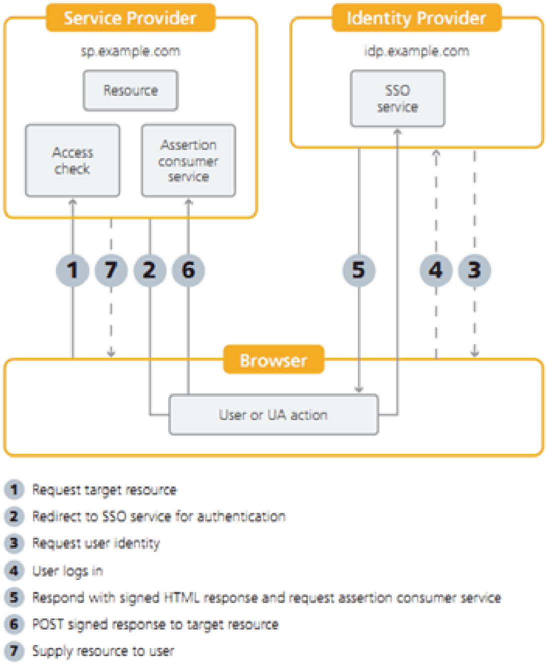
SAML Find Its Cloud Legs

Lori MacVittie, 2013-20-02

#IAM #cloud #infosec #SAML *"When I took office, only high energy physicists had ever heard of what is called the World Wide Web... Now even my cat has it's own page."* - **Bill Clinton**

Despite the slow descent into irrelevance of SOA and its core standards, several of its ancillary standards remain steadfastly alive and in some cases are growing in relevance. In particular, SAML is gaining steam thanks in large part to the explosive adoption of SaaS.


Service Provider
sp.example.com
Resource
Access check
Assertion consumer service
Identity Provider
idp.example.com
SSO service
1
7
2
6
5
4
3
Browser
User or UA action
1 Request target resource
2 Redirect to SSO service for authentication
3 Request user identity
4 User logs in
5 Respond with signed HTML response and request assertion consumer service
6 POST signed response to target resource
7 Supply resource to user

SAML (Security Assertion Markup Language), now on its second major version, was most commonly associated with efforts by the Liberty Alliance (long since defunct and absorbed into the Kantara Initiative) to federate authentication and authorization across the web. The "big deal" with SAML was that it was easily supported by the browser. Of course when it was introduced there were few services enterprises felt needed federation with corporate systems and thus despite the energy surrounding the project it was largely ineffective at producing the desired results.

Fast forward to today and the situation out there has changed. Enterprises are increasingly invested in SaaS (which is still really just a web application) and are growing more aware of the challenges associated with that investment, particularly around identity, access, and control.

Re-enter SAML. This time, with a much better chance of becoming The Standard for federating identity across cloud-deployed applications.

WHY SAML? WHY NOW?

The appeal remains, in large part, due to its focus on the browser through which most if not all enterprise resources are accessed today. Add in a healthy dose of mobile devices, roaming employees, and new off-premise enterprise services and you've got a recipe for SAML's success.

The need for organizations to get a grip on (reassert control over) access and identity management is significant. As we recently learned there are mounting concerns with respect to distributed credentials and unfettered access to corporate applications residing off-premise. SAML 2.0 offers a standards-based, increasingly supported means of accomplishing this feat of wondrous power through a combination of well-defined processes and products (er, services).

Salesforce.com: Configuring SAML Settings for Single Sign-On

> Single sign-on is a process that allows network users to access all authorized network resources without having to log in separately to each resource. Single sign-on allows you to validate usernames and passwords against your corporate user database or other client application rather than having separate user passwords managed by Salesforce.

Google: SAML Single Sign-On (SSO) Service for Google Apps

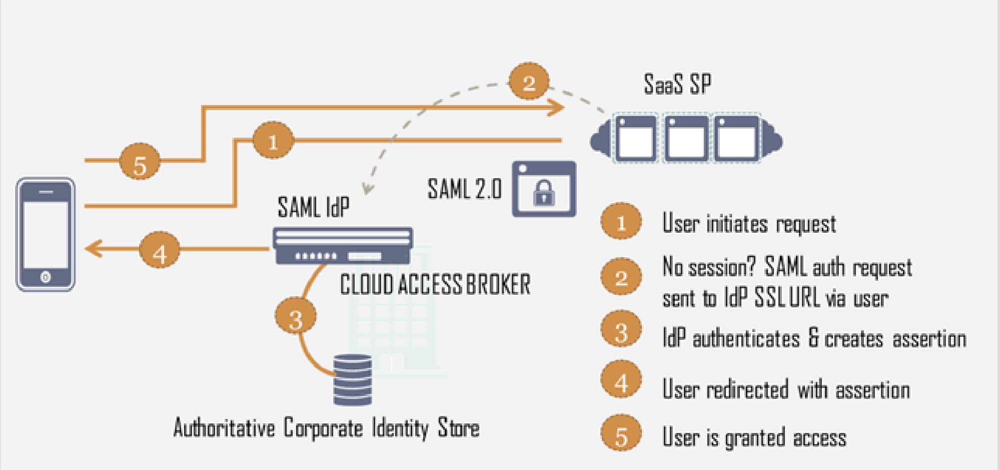
> Using the SAML model, Google acts as the **service provider** and provides services such as Gmail and Start Pages. Google partners act as **identity providers** and control usernames, passwords and other information used to identify, authenticate and authorize users for web applications that Google hosts.

The list goes on: Concur, SugarCRM, FedEx, RightScale. This is the tip of the iceberg when it comes to SAML. And it's not just vendors offering support, it's users asking for it, coding it into their applications, demanding it.

And why shouldn't they? SAML 2.0 is highly flexible in its ability to provide a standard process through which authentication and authorization to resources can be provided. It provides the process and the payload necessary to unify and federate identity across distributed applications, and it can be easily used in the browser as well as in custom applications. It's a markup language standard transported largely over HTTP.

Because it has well defined processes that describe how to federate identity using an SP (Service Provider) and an IdP (Identity Provider) organizations and vendors alike can cleanly implement support either directly or through a third-party provider like Ping Identity, One Login, or SecureAuth. SAML can support mobile devices and APIs as easily as it can traditional browser-based resources. When used by a cloud access broker acting as an access control gateway, SAML can be used to provide single-sign on for both cloud and data center hosted resources.

It's really quite a flexible little standard that seems to have finally found its sea legs - if by "sea legs" one means cloud legs.


SaaS SP
SAML 2.0
SAML IdP
CLOUD ACCESS BROKER
Authoritative Corporate Identity Store
1
2
3
4
5
1 User initiates request
2 No session? SAML auth request sent to IdP SSL URL via user
3 IdP authenticates & creates assertion
4 User redirected with assertion
5 User is granted access

How a cloud access broker uses SAML to coordinate credentials between a SaaS provider and the corporate identity store.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com