The Future of Federated Identity
or, Whither SAML?

Thursday, July 19, 2012 – 1 p.m. ET

Eve Maler, Principal Analyst serving security and risk professionals at Forrester Research

Tom Barton, Sr. Director for Architecture, Integration and CISO, University of Chicago

Thank you to InCommon Affiliates for helping to make IAM Online possible.
In Memoriam: R.L. “Bob” Morgan

https://spaces.internet2.edu/display/rlbob/Home
Sources & Sinks of Identity for Research & Education

• Traditional populations
  – Faculty, staff, students, affiliates, …

• Pan-organizational collaboration for research & scholarship
  – R&E data network not enough
  – SAML, shibboleth
  – InCommon Federation & peers
  – Boost campus IAM

• Blend consumer cloud services with enterprise to enhance collaboration
  – Blend mobile in too
  – Blend in groups

• Global identity services network
  – Let groups of collaborators leverage interconnected sources of identity to manage access
Our Speaker – Eve Maler

- Forrester analyst
  - Identity, security, & privacy strategy
- PayPal, Sun
- OASIS Security Services TC
  - SAML, WS-*
- One of the many experts outside of Research & Education that Bob worked with, brought his experience & vision to them, brought their work & ideas back to us
  - Eve’s here today because Bob pitched this webinar opportunity to her
Making Leaders Successful Every Day
The Future Of Federated Identity
(or, Whither SAML?)

Eve Maler, Principal Analyst

IAM Online
July 19, 2012
Sounds Awesome – Maybe Later?
Agenda

› How much has SAML achieved in the last decade?

› The problems of the extended enterprise demand more

› Are emerging solutions credible?

› What to expect in the next decade and what to do about it
Enterprise identity has grown out of directories
Today, SAML has a rich ecosystem

SAAML ASSERTIONS ARE THE “UNIVERSAL SOLVENT” OF IDENTITY DATA

Libraries and toolkits to develop SAML actors and SAML-enabled services

The Libraries and Toolkits below are used by developers to integrate applications and services into SAML federations or to build their own SAML-likes like IdPs.

<table>
<thead>
<tr>
<th>Library/Toolkit</th>
<th>Service</th>
<th>Organization</th>
<th>Location</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>PingConnect</td>
<td>PingIdentity</td>
<td><a href="https://www.pingidentity.com/our-solutions/pingconnect.dmi">https://www.pingidentity.com/our-solutions/pingconnect.dmi</a></td>
<td>On-Demand SSO for dozens of SaaS providers</td>
<td></td>
</tr>
<tr>
<td>OneLogin</td>
<td>OneLogin</td>
<td><a href="http://www.onelogin.com/">http://www.onelogin.com/</a></td>
<td>IdP for SAML- and OpenID-enabled cloud services</td>
<td></td>
</tr>
<tr>
<td>ZXIDP.org</td>
<td>ZXIDP.org</td>
<td><a href="https://zxidp.org/index-dp.html">https://zxidp.org/index-dp.html</a></td>
<td>IdP</td>
<td></td>
</tr>
<tr>
<td>PEER</td>
<td>Internet2</td>
<td><a href="https://spaces.internet2.edu/display/PEER/Home">https://spaces.internet2.edu/display/PEER/Home</a></td>
<td>Public metadata registry</td>
<td></td>
</tr>
<tr>
<td>Testshib.org</td>
<td>Testshib.org</td>
<td><a href="http://www.testshib.org/testshib-two/index.jsp">http://www.testshib.org/testshib-two/index.jsp</a></td>
<td>IdP and SP for testing</td>
<td></td>
</tr>
<tr>
<td>Federation Lab</td>
<td>Géant</td>
<td><a href="https://fed-lab.org/">https://fed-lab.org/</a></td>
<td>Test-SP, metadata registry, test tools</td>
<td></td>
</tr>
<tr>
<td>Feide OpenIdP</td>
<td>UNINETT AS</td>
<td><a href="https://openidp.feide.no/">https://openidp.feide.no/</a></td>
<td>IdP that allows any user to register, and any SP to connect</td>
<td></td>
</tr>
<tr>
<td>SAML Tracer</td>
<td>UNINETT AS</td>
<td><a href="https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/">https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/</a></td>
<td>A tool for viewing SAML messages sent through the browser during single sign-on and single logout</td>
<td></td>
</tr>
</tbody>
</table>

SAAML-related Services

<table>
<thead>
<tr>
<th>Library/Toolkit</th>
<th>Service</th>
<th>Organization</th>
<th>Location</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shibboleth</td>
<td>Internet2</td>
<td>OSS</td>
<td>IdP, SP, Discovery</td>
<td></td>
</tr>
<tr>
<td>SimpleSAMLphp</td>
<td>UNINETT AS</td>
<td>OSS</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>Synthlab</td>
<td>commercial</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>IBM</td>
<td>commercial</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>NTI Software</td>
<td>commercial</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>ZUR</td>
<td>zuri.org</td>
<td>OSS</td>
<td>X</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>ZUR</td>
<td>zuri.org</td>
<td>OSS</td>
<td>X</td>
</tr>
</tbody>
</table>

Source: KantaraInitiative.org
But identity federation has mostly reached enterprises with deep pockets

THINK OF IT AS “RICH” VERSUS “REACH”

“What are your firm’s plans to adopt federation technologies?”

<table>
<thead>
<tr>
<th>Category</th>
<th>Interested but no plans</th>
<th>Not interested</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB (20-999 employees)</td>
<td>21%</td>
<td>50%</td>
</tr>
<tr>
<td>Enterprise (1,000 or more employees)</td>
<td>24%</td>
<td>23%</td>
</tr>
</tbody>
</table>

Base: 1,071 North American and European security decision-makers

Source: Forrsights Security Survey, Q2 2011

Source: October 26, 2011, Forrester report “OpenID Connect Heralds The ‘Identity Singularity”

© 2012 Forrester Research, Inc. Reproduction Prohibited
In fact, SOA-style distributed computing in general is far from ubiquitous.

<table>
<thead>
<tr>
<th></th>
<th>Use now</th>
<th>Will use</th>
<th>Investigating</th>
<th>Don’t know</th>
<th>Will not use</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-Security</td>
<td>30%</td>
<td>16%</td>
<td>11%</td>
<td>40%</td>
<td></td>
</tr>
<tr>
<td>WS-Security — username token</td>
<td>18%</td>
<td>11%</td>
<td>15%</td>
<td>52%</td>
<td></td>
</tr>
<tr>
<td>WS-Security — SAML token</td>
<td>13%</td>
<td>15%</td>
<td>16%</td>
<td>52%</td>
<td></td>
</tr>
<tr>
<td>WS-Security — Kerberos token</td>
<td>14%</td>
<td>12%</td>
<td>13%</td>
<td>53%</td>
<td></td>
</tr>
<tr>
<td>WS-Security — X509 token</td>
<td>11%</td>
<td>12%</td>
<td>14%</td>
<td>58%</td>
<td></td>
</tr>
<tr>
<td>Direct use of XML Signature and/or XML Encryption*</td>
<td>13%</td>
<td>8%</td>
<td>16%</td>
<td>58%</td>
<td>5%</td>
</tr>
</tbody>
</table>

**Highest commitment**

Source: November 2008 Global Software Strategies Online Survey

*As opposed to using them through WS-Security

Agenda

- How much has SAML achieved in the last decade?
- The problems of the extended enterprise demand more
- Are emerging solutions credible?
- What to expect in the next decade and what to do about it
Old access management solutions don’t “work less well”; they don’t work at all.
The world of the extended enterprise requires you to think outside the box.

App sourcing and hosting
- SaaS apps
- Apps in public clouds
- Partner apps
- Apps in private clouds
- On-premises enterprise apps

Enterprise computers
- Enterprise-issued devices
- Public computers
- Personal devices

Employee access channels

User populations
- Employees
- Contractors
- Partners
- Members
- Customers

Portable consumer identities have arrived

ON THE WEB, YOU’RE A FREE AGENT

Source: ladygaga.com, sears.com
Web APIs have become business-enabling tools, particularly for mobile

<table>
<thead>
<tr>
<th>Sector</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>Sears, Best Buy, wine.com</td>
</tr>
<tr>
<td>Content</td>
<td>Springer, Netflix, USA Today</td>
</tr>
<tr>
<td>Geolocation</td>
<td>white pages, WeatherBug</td>
</tr>
<tr>
<td>Financial services</td>
<td>TransUnion, Intuit</td>
</tr>
</tbody>
</table>
In the API economy, security pros’ control diminishes with distance

THE WEBDEVIFICATION OF IT
Our security worlds are colliding

UNIFY YOUR STANCE AND PREPARE FOR ANYTHING

B2C

B2E + B2B

SaaS

the

identity

singularity
To unify, apply the Zero Trust model: assume all systems are equally far apart.
Go from IDaaS to “IAM as an API”

The business app’s own API determines access control granularity.

Robustly protect all interfaces, regardless of their sourcing model.

API façade pattern

Back-end apps, web apps, mobile apps . . .

API client

Web service and app APIs

Scale-out infrastructure

API client

Business apps

Internet

IAM API client

IAM API client

Internet

APIs for authentication, authorization, provisioning . . .

IAM infrastructure

Applying the pattern to IAM functions

Source: March 22, 2012 “Navigate The Future of IAM” Forrester report
Agenda

» How much has SAML achieved in the last decade?

» The problems of the extended enterprise demand more

» Are emerging solutions credible?

» What to expect in the next decade and what to do about it
New identity solutions disrupt...but attract.

Or, The good thing about reinventing the wheel is that you can get a round one.*

*Douglas Crockford, inventor of JavaScript Object Notation (JSON)
Emerging IAM standards have an edge over traditional ones for Zero Trust

IAM functionality
- Provisioning, proofing, self service
- Authentication, session management, SSO, federation
- Authorization, consent, access control

Established SOA-friendly standards
- SPML
- SAML
- WS-Security

Emerging web-friendly standards
- SCIM
- OpenID Connect
- UMA
The new Venn of access control

- OpenID Connect
- OAuth 2.0
- UMA
- UMA
Web 2.0 players invented OAuth just to solve the “password anti-pattern”
What it really does is let a person delegate constrained access to an app.
OAuth can help manage risk, cost, and complexity

FOR INTERNET-SCALE ZERO TRUST, YOU NEED IT ALL

Gets client apps out of the business of storing passwords
Friendly to a variety of user authentication methods and user devices, including smartphones and tablets
Allows app access to be tracked and revoked on a per-client basis
Allows for least-privilege access to API features
Can capture explicit user authorization for access
Lowers the cost of secure app development

Bonus: provides plumbing for a much larger class of needs around security, identity, access, and privacy
OAuth vendor solutions are popping up all over the place
OpenID Connect turns SSO into a standard OAuth-protected identity API

<table>
<thead>
<tr>
<th>SAML 2.0, OpenID 2.0</th>
<th>OAuth 2.0</th>
<th>OpenID Connect</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Initiating user’s login session</td>
<td>✗ Not responsible for session initiation</td>
<td>✓ Initiating user’s login session</td>
</tr>
<tr>
<td>✗ Not responsible for collecting user consent</td>
<td>✓ Collecting user’s consent to share attributes</td>
<td>✓ Collecting user’s consent to share attributes</td>
</tr>
<tr>
<td>✓ High-security identity tokens (<em>SAML only</em>)</td>
<td>✗ No identity tokens per se</td>
<td>✓ High-security identity tokens (<em>using JSON Web Tokens</em>)</td>
</tr>
<tr>
<td>✗ Distributed and aggregated claims</td>
<td>✗ No claims per se; protects arbitrary APIs</td>
<td>✓ Distributed and aggregated claims</td>
</tr>
<tr>
<td>✓ Dynamic introduction (<em>OpenID only</em>)</td>
<td>✗ Client onboarding is static</td>
<td>✓ Dynamic introduction</td>
</tr>
<tr>
<td>✗ Session timeout</td>
<td>✗ No sessions per se</td>
<td>✓ Session timeout (<em>on the docket</em>)</td>
</tr>
</tbody>
</table>

© 2012 Forrester Research, Inc. Reproduction Prohibited
An OpenID Connect killer app: “Street Identity”

Service provider needs trusted data
Attribute provider has it
Identity provider can broker your permission to provide it
AP can demand a fee from SP for it
Lather, rinse, and repeat for all valuable user data
Where SAML is “rich,” OpenID Connect holds promise for “reach”

- Already exposing customer identities using a draft OpenID Connect-style API
- Working to expose workforce identities through OpenID Connect

LOB apps and smaller partners can get into the federation game more easily; complex SAML solutions will see price pressure over time
UMA turns online sharing with *anyone* into a “privacy by design” solution

Alice-to-Alice, Alice-to-Bob, Alice-to-org...and org-to-org

Claims-based and policy-based authorization

User can impose terms on requesters

Centralizable authorization function

Brokered protection outsourcing
Some real-life UMA use cases

- Patient-centric healthcare data sharing
- Citizen-centric secure government services
- Personal data lockers and personal clouds
- Student-centric trusted education data sharing
- Direct business control over employee SaaS access
References normatively as an option
(sharing some features as a result)

OpenID Connect

- You achieve federated single sign-on and login-time attribute exchange
- You control access to claims about you

Claims can come from distributed sources
Apps get access using bearer-style tokens
You delegate scope-constrained access to other apps
Calling app is recognized based on authenticated identity
Apps can get access after you go offline

OAuth 2.0

- You control access to web APIs
- Apps can use a variety of access token types

UMA

- You can grant access to apps operated by anyone
- You control access to a variety of protected resources
- You can grant access by setting policies and terms ahead of time
- The authorization function is standard and centralizable
- Requesting party is authorized based on claims

© 2012 Forrester Research, Inc. Reproduction Prohibited
Agenda

- How much has SAML achieved in the last decade?
- The problems of the extended enterprise demand more
- Are emerging solutions credible?
- What to expect in the next decade and what to do about it
Get ready: OAuth and friends are spreading fast because Zero Trust is pulling them along.
What will happen to today’s SAML products and deployments?

**IT’S LIKE BUYING THE WHITE ALBUM ALL OVER AGAIN**

- **By 2012**
  
  Major cloud IdPs and enterprises will expose managed identities with OpenID Connect.
  
  Existing SAML-to-OAuth bridge solutions will grow to encompass OpenID Connect subtleties.

- **By 2016**
  
  STSes will support JSON Web Tokens (JWTs) natively while still offering legacy SAML support.
  
  Strategic JWT use will spread to on-premises SOA infrastructure.

- **By 2021**
  
  IT organizations will move away from SAML use for cost savings.
  
  Proprietary token formats will always remain; the SAML token format will fade away.
You have opportunities to be a Zero Trust Identity hero

- Exposing SAML IdP already? Consider an OpenID Connect interface
- Working with SaaS providers? Encourage federated access into those services on a standardized basis
- Rolling out mobile apps? Explore OAuth patterns that offer added security
- Love SAML with all your heart? Get on a speaking basis with OAuth, OpenID Connect, and JWT
Thank you

Eve Maler
+1 617.613.8820
emailer@forrester.com
@xmlgrrl

www.forrester.com
Evaluation
Please complete the evaluation of today’s IAM Online:

IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline

Next IAM Online – August 8, 2012 (3 pm EDT)
“Demystifying Privilege and Access Management – Strategies for local, federated and cloud environments”
www.incommon.org/iamonline
Thank you to InCommon Affiliates for helping to make IAM Online possible.

Brought to you by InCommon, in cooperation with Internet2 and the EDUCAUSE Identity and Access Management Working Group