Auto-Connect via Dynamic SAML

Patrick Harding
CTO
Ping Identity
Ping Identity

- Market Leader for Secure Internet Single Sign-On
- Founded in 2002
- Based in Denver, Colorado USA
- Customers Include JPMorgan, Kraft, Morgan Stanley, Comcast, Checkfree
- Investors Include Draper Fisher Jurvetson, General Catalyst, Fidelity Investments
B2B Federation Today

• Protocol Debates are Over

• Organizations Have Enabled 5 – 10 Federation Connections
  ▸ The Value of Federation Has Been Justified

• Common Business Scenarios Have Become Apparent
Today Federation is Enterprise-Centric

"High Leverage" Partner Drives Federation
Common Use Cases

• **Outbound SSO**
  - for users to access software-as-a-service (SaaS) applications, business process outsourcing (BPO) services, and trading partners

• **Inbound SSO**
  - for relationships such as BPOs and managed services where external users access the enterprise’s resources over the Internet

• **Internal SSO**
  - for the enterprise and its acquisitions, affiliates, subsidiaries and joint ventures

• **SSO to third-party hosted industry hubs**
  - for information sharing by users and application access among industry organizations
The Federation Challenge

- Federation Takes 6 – 9 Months to Implement
  - Each Connection Is Customized
  - Every Connection Is Tested
  - Perception That Contracts Are Meticulous
  - Connections are implemented serially

\[
\begin{align*}
50 \text{ partners} & \times 60 \text{ days/connection} = \text{Over 12 years}
\end{align*}
\]

Does not scale!
Yesterday

• The Register – “OASIS Ratifies SAML” - 11/2002

“SAML is an XML-based framework for web services, that allows the exchange of authentication and authorization information among business partners. It enables web-based security interoperability functions, such as single sign-on, across sites hosted by multiple companies”

“PKI has been dogged by issues of complexity, integration difficulties and user apathy”

http://www.theregister.co.uk/2002/11/07/oasis_ratifies_saml/
PingFederate Users Can Federate in 30 Days or Less

<table>
<thead>
<tr>
<th>Company</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leading Food Company</td>
<td>7 Days</td>
</tr>
<tr>
<td>Diagnostic Imaging Benefits Management Provider</td>
<td>14 Days</td>
</tr>
<tr>
<td>Leading Semiconductor Manufacturer</td>
<td>18 Days</td>
</tr>
<tr>
<td>Consumer Products Manufacturing Conglomerate</td>
<td>21 Days</td>
</tr>
<tr>
<td>Major Pharmaceutical Manufacturer</td>
<td>27 Days</td>
</tr>
<tr>
<td>Australian Wealth Management &amp; Financial Planning Company</td>
<td>28 Days</td>
</tr>
</tbody>
</table>
## Connections Necessitate Scalability

<table>
<thead>
<tr>
<th>Company</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>McDonalds</td>
<td>18000 partner connections</td>
</tr>
<tr>
<td>3M</td>
<td>Too many connections to count</td>
</tr>
<tr>
<td>Caterpillar</td>
<td>200 dealerships</td>
</tr>
</tbody>
</table>
Speed to Connect is Crucial

- Simplify Federation Connectivity
- Rapid Connection Configuration
- Minimize Testing and Ongoing Maintenance
- Publish Conventions and Best Practices
- Automate meta-data exchange
Focus on B2B Use Cases

• Business to Business
  ‣ Enterprise Employees Accessing Outsourced or Partner Applications

• Companies rely on existing business contracts to address:
  ‣ Operational service level agreement disputes
  ‣ Liability associated with protecting sensitive information

• Most Service Providers are actually happy to outsource authentication to their customers and partners
Technical Friction

- Partners must negotiate which of many SAML options to use
  - Multiple protocols, profiles, bindings

- Service Providers NOT leveraging SP-Initiated SSO
  - IdP Selection/Discovery is poorly defined

- Products require manual configuration of partner information

- Certificate Management is problematic
  - Trust established through manual exchange of certificates
Auto-Connect Paradigm

- When a mail server is set-up it can immediately receive or send mail to any other mail server on the Internet
  - White lists and Black lists suffice to constrain mail flow between parties

- Federating with business partners must become this simple if it is to scale effectively

- All without making any changes to the SAML 2 core specification
Auto-Connect Basics

• Control Federation Connections with White Lists

• Leverage Conventions & Best Practices

• Automated SAML meta-data exchange
  ‣ via Standardized EntityID URL Derived from Domain Name
  ‣ abc.com → http://saml.abc.com

• Optionally use Email Address to Bootstrap IdP Discovery

• Eliminate Manual Key/Certificate Management
  ‣ Cryptographic keys derived from meta-data
  ‣ Leverage Root CA’s as Trust Anchors

• Limit options for SSO & SLO
  ‣ POST and Redirect Only
Service Provider Admin Adds Domain to White List

- Configuring My Server
  - Main
  - IdP Whitelist Manager
- Manage partners allowed to authenticate users for Auto-Connect™ requests. Users requesting access to a protected resource will be denied if their domain does not appear in this table.
- Domain Name | Action
  - pingidentity.com | Edit / Delete
  - [ ] | Add
Auto-Connect Example

1. The user attempts to access a resource at the SP

SP
saas.com

IdP
pingidentity.com

Browser
Service Provider Prompts
User for Email Address
Auto-Connect Example

(1) The user attempts to access a resource at the SP
Auto-Connect Example

1. Browser

2. SP retrieves and validates a signed metadata file from the IdP

(2) SP retrieves and validates a signed metadata file from the IdP
Auto-Connect Example

(3) The service provider redirects the user to the identity provider's single sign-on URL with a SAML AuthNRequest
(4) The IdP retrieves and validates the signed metadata file from the SP
Auto-Connect Example

(5) IdP validates the SAML AuthNRequest
Auto-Connect Example

1. SP saas.com
2. IdP pingidentity.com
3. Browser
4. IdP authenticates the user
5. Browser

(6) IdP authenticates the user
User Authenticates At Their Identity Provider
Auto-Connect Example

(6) IdP authenticates the user
Auto-Connect Example

(7) IdP creates the SAML Assertion and redirects the user back to the SP
Auto-Connect Example

(8) SP validates the SAML Assertion and generates a local security context for the user
Secure Internet SSO in 5 Seconds!

My Service Provider
Sample Application

User Attributes From the IdP

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserId</td>
<td>John</td>
</tr>
<tr>
<td>authnInst</td>
<td>2007-11-29 18:11:08-0700</td>
</tr>
</tbody>
</table>

Welcome.

You have successfully signed on to this Service Provider (SP) site using SSO — your identity has been verified by the Identity Provider (IdP) who maintains your login credentials.

The IdP has also sent along some information about you ("User Attributes" at left), which a real partner SP would use to enhance and streamline your experience at its site.

You can now either log out of this SP session locally (using the link in the navigation bar above) or log out globally (using the Single Logout links below, which exercise different SAML bindings). If you log out locally, you will not have to sign on at the IdP site again to reach this domain via SSO, since your IdP session is still active. Single logout ends both your IdP and SP sessions, and you will be asked to log on again at the IdP.

PingIdentity™
© 2007, Ping Identity Corporation
All Rights Reserved
Whats Next

• Solicit and incorporate use case feedback
  ‣ Shibboleth, Concordia, DI DW, Vendors

• Develop Dynamic SAML profile in SSTC
  ‣ Drives to interoperable products

• Leverage Liberty SAML 2.0 Interoperability service
  ‣ Forces interoperable products

• Standard Attribute Schemas for B2B
Questions