

Auto-Connect via Dynamic SAML

Patrick Harding
CTO
Ping Identity



Ping Identity™

Ping Identity

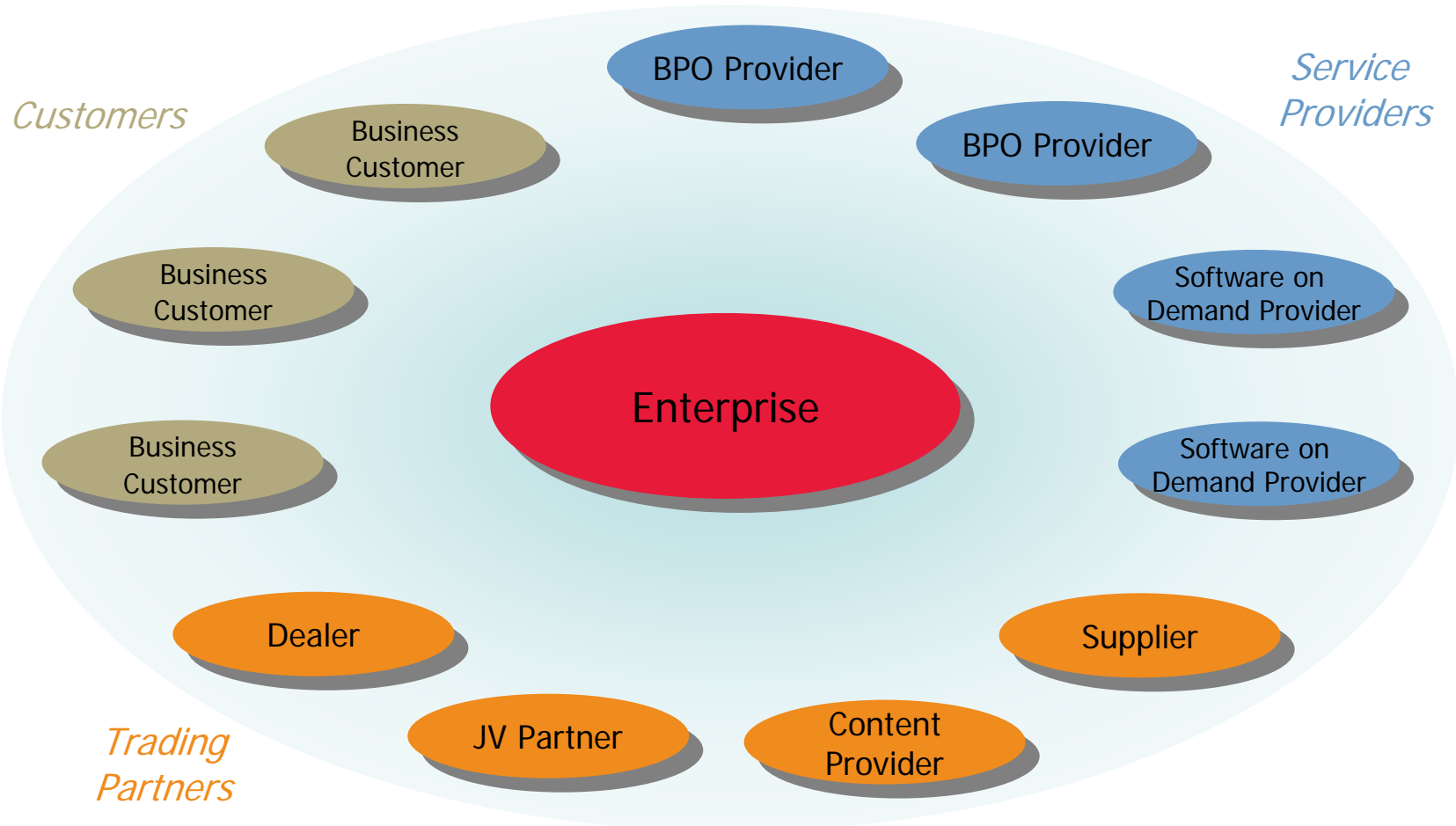


- Market Leader for **Secure Internet Single Sign-On**
- Founded in 2002
- Based in Denver, Colorado USA
- Customers Include JPMorgan, Kraft, Morgan Stanley, Comcast, Checkfree
- Investors Include Draper Fisher Jurvetson, General Catalyst, Fidelity Investments

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

$$\begin{array}{c} \text{50 partners} \end{array} \times \begin{array}{c} \text{60 days/connection} \end{array} = \begin{array}{c} \text{Over 12 years} \end{array}$$

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

Leading Food Company	7 Days
Diagnostic Imaging Benefits Management Provider	14 Days
Leading Semiconductor Manufacturer	18 Days
Consumer Products Manufacturing Conglomerate	21 Days
Major Pharmaceutical Manufacturer	27 Days
Australian Wealth Management & Financial Planning Company	28 Days

Connections Necessitate Scalability

McDonalds	18000 partner connections
3M	Too many connections to count
Caterpillar	200 dealerships

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 out source 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

The screenshot shows the PingFederate administration interface in a Mozilla Firefox browser window. The browser's address bar displays the URL: `https://saml.pingidentity.com:9999/pingfederate/app?service=direct/1/Home/Holder/portalMenu.idpWhiteList`. The page title is "PingFederate®".

The main content area is titled "Configuring My Server" and includes a navigation menu with "Main" and "IdP Whitelist" tabs. The "IdP Whitelist" tab is active, showing the "IdP Whitelist Manager" section. A green informational box states: "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."

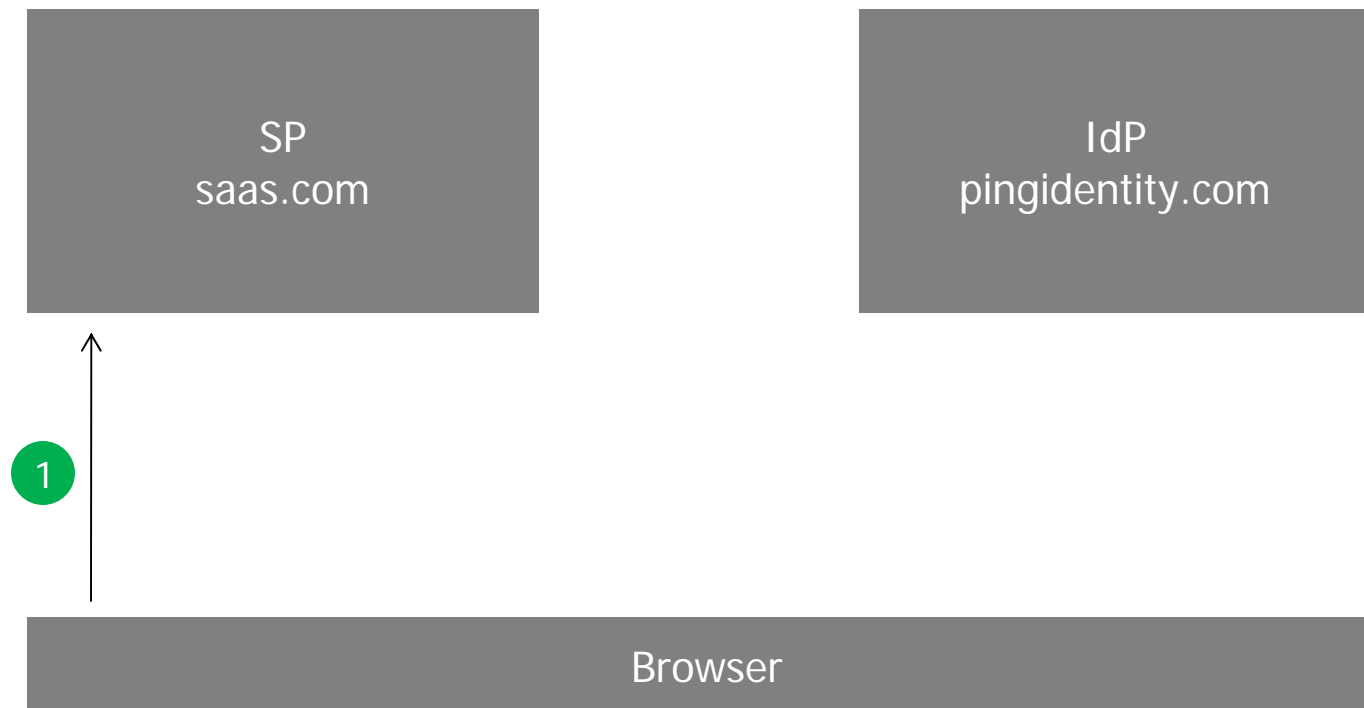
Below the informational box is a table with the following structure:

Domain Name	Action
pingidentity.com	Edit / Delete
<input type="text"/> *	<input type="button" value="Add"/>

At the bottom of the main content area, there are "Cancel" and "Save" buttons. The footer of the page contains the following information:

- Transaction Total Count: 23
- Transaction Failure Count: 0
- [License/Enforcement Status](#)
- Version 5.0.0.5-SNAPSHOT
- © 2003-2007 Ping Identity Corporation
All Rights Reserved
- PingIdentity™**

Auto-Connect Example

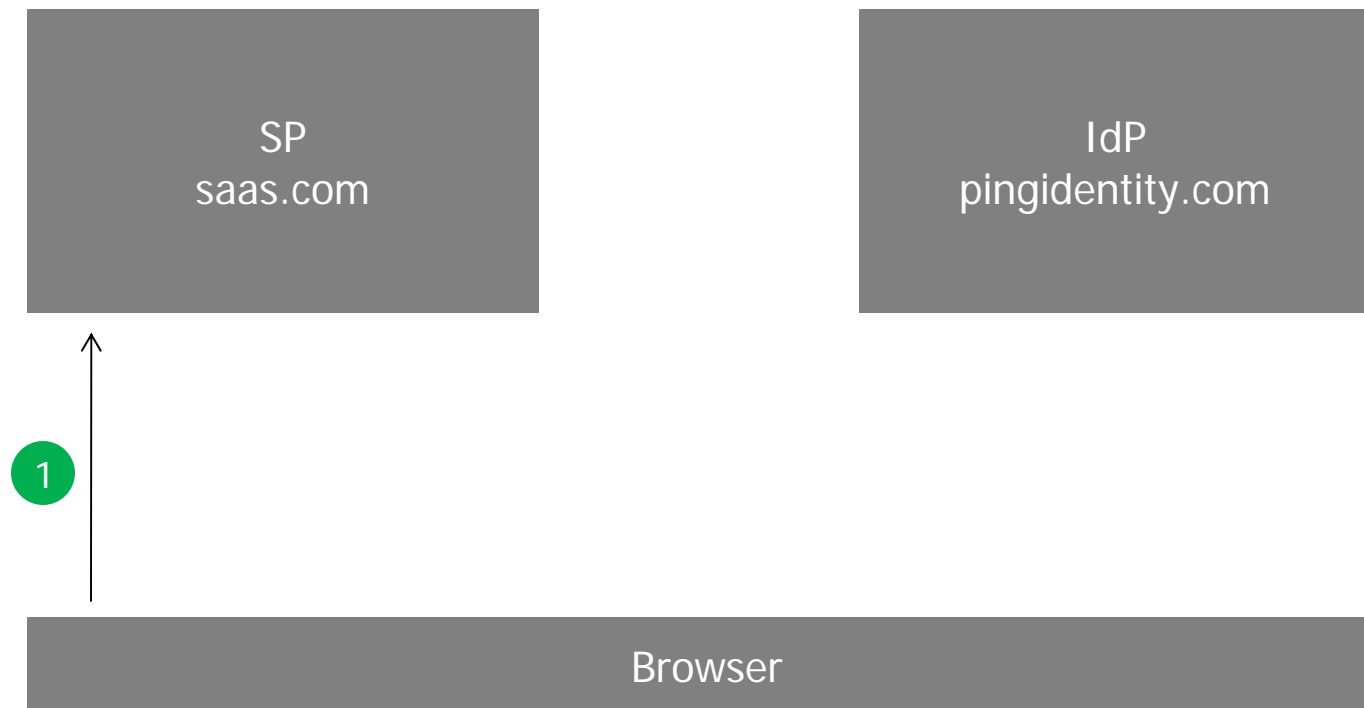


(1) The user attempts to access a resource at the SP

Service Provider Prompts User for Email Address

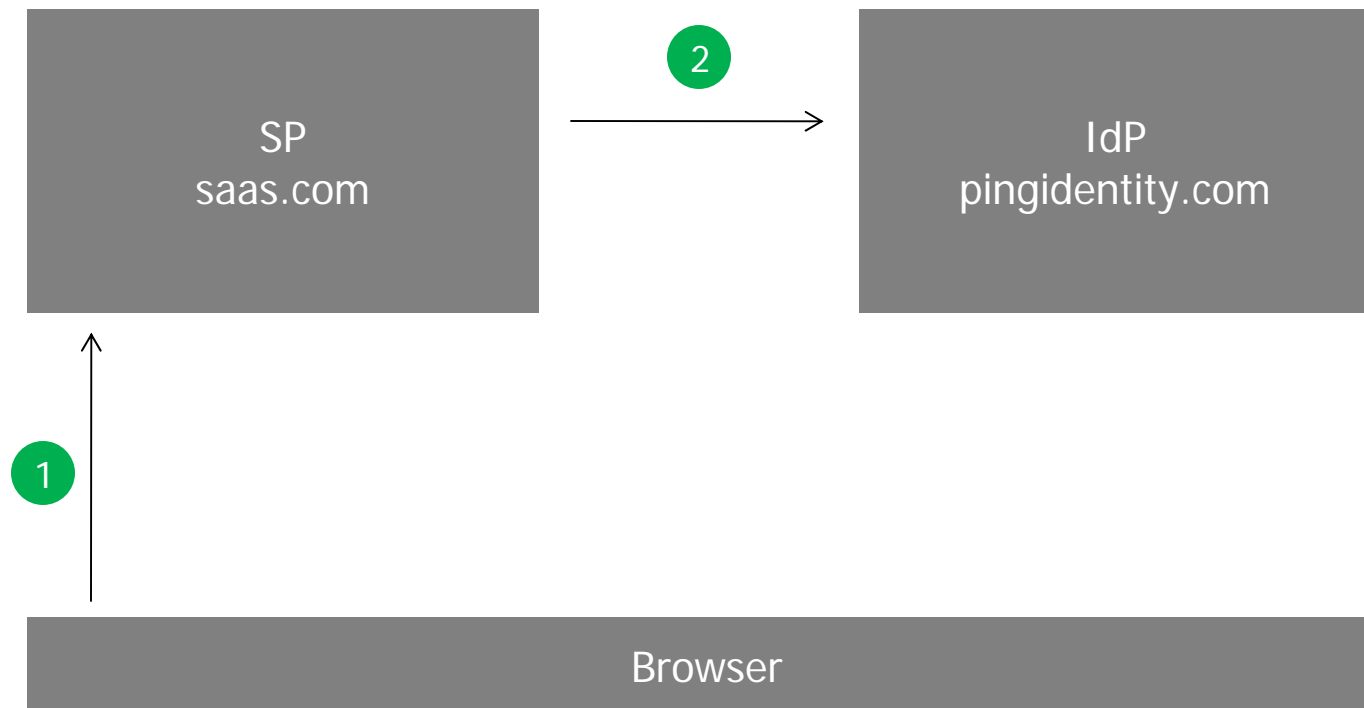
The screenshot shows a Mozilla Firefox browser window with the title "Welcome to the SP Sample Application - Mozilla Firefox". The address bar contains the URL "https://saml.pingidentity.com:9031/quickstart-app-sp/go?action=dynafedform". The main content area features a white box with the heading "My Service Provider Sample Application". Below this heading is a link labeled "Back to the Welcome page". The next section is titled "Auto-Connect" and contains the text: "This SP will discover the IdP that corresponds to your email address dynamically. You will be redirected to the IdP for authentication." Below this text is a text input field with the value "jdoe@pingidentity.com" and a button labeled "Single Sign-On". At the bottom right of the page, the PingIdentity logo is displayed along with the copyright notice "© 2007, Ping Identity Corporation All Rights Reserved".

Auto-Connect Example



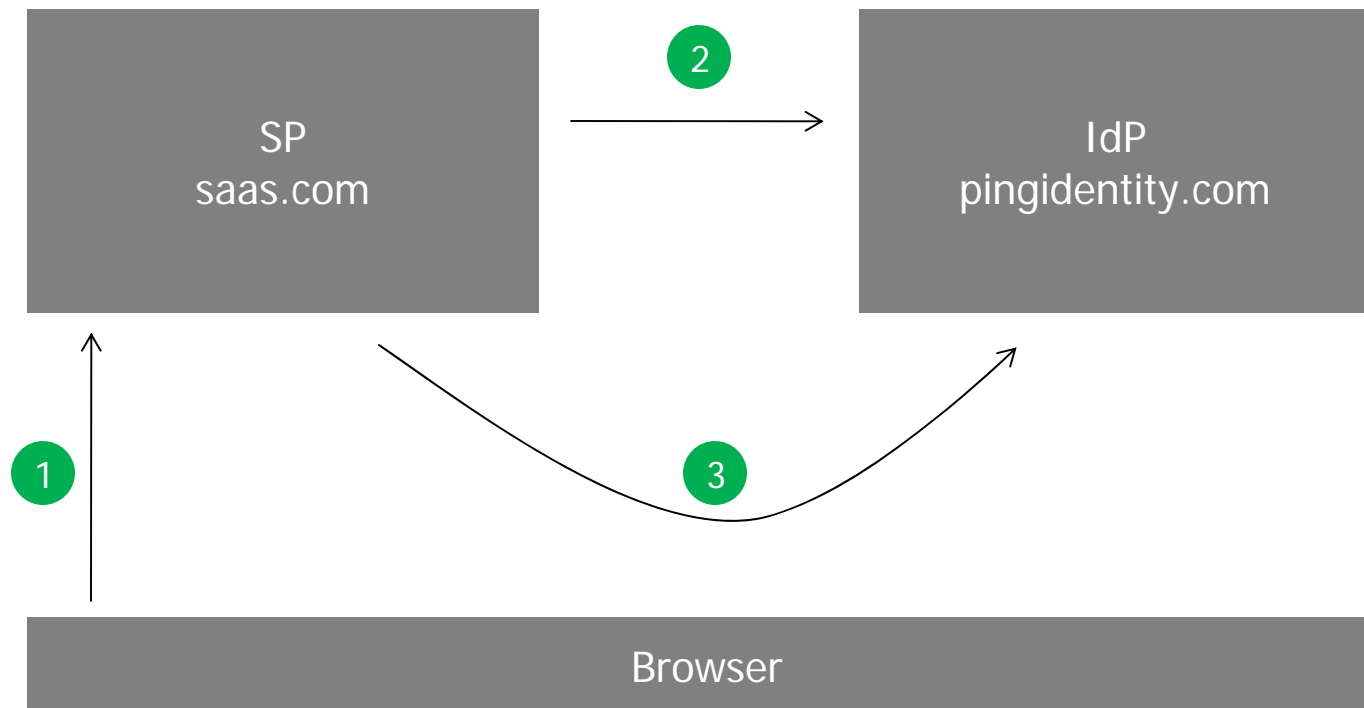
(1) The user attempts to access a resource at the SP

Auto-Connect Example



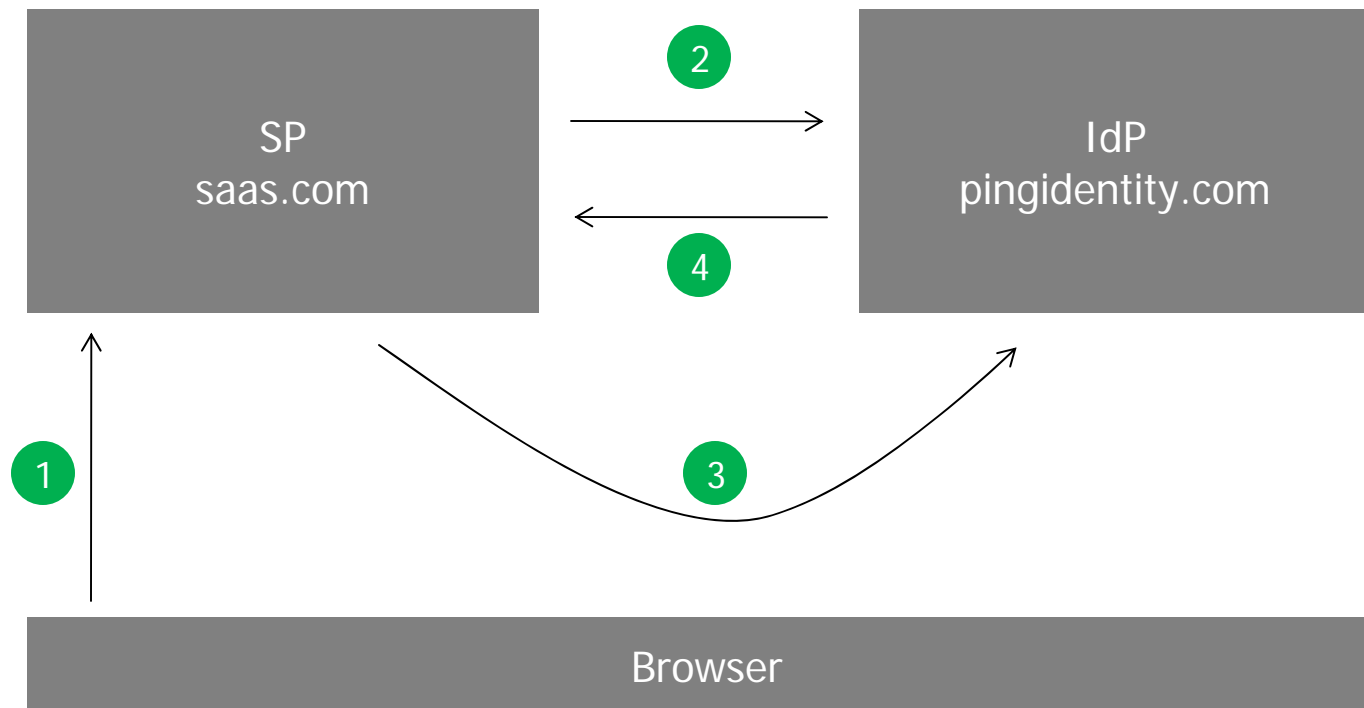
(2) SP retrieves and validates a signed metadata file from the IdP

Auto-Connect Example



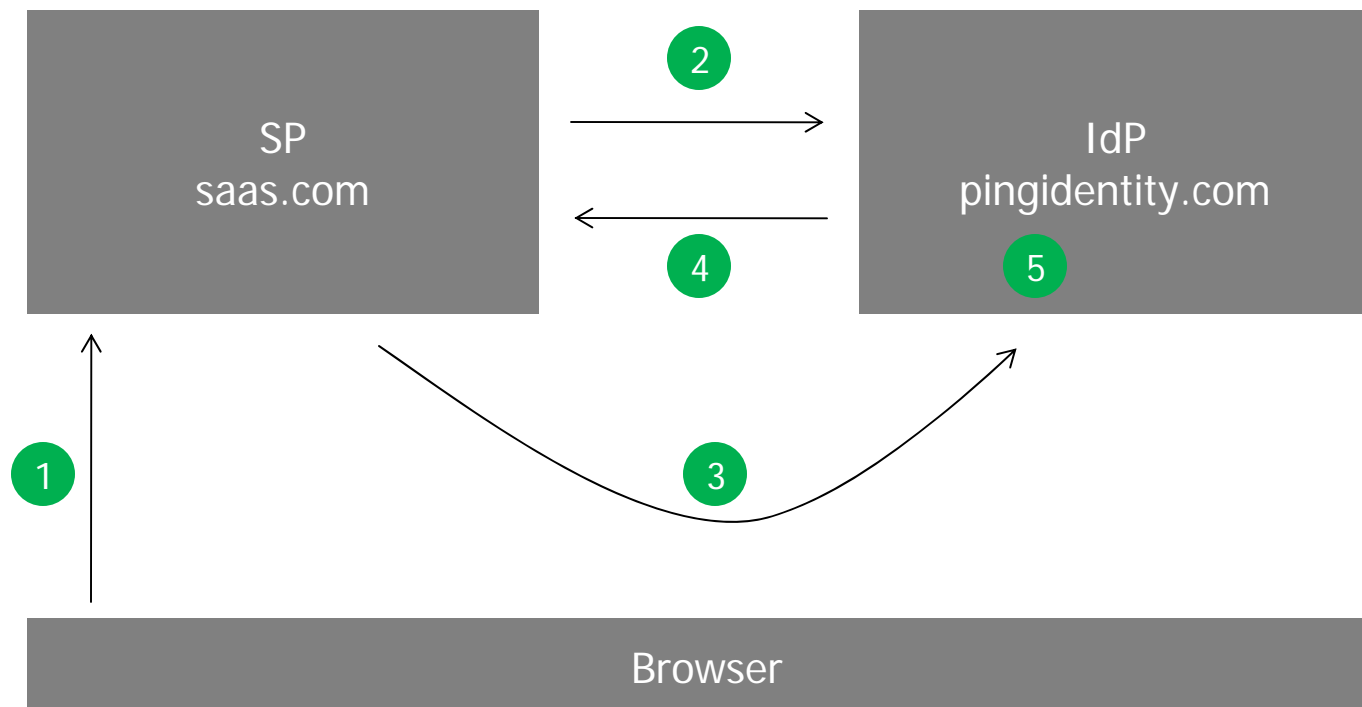
(3) The service provider redirects the user to the identity provider's single sign-on URL with a SAML AuthNRequest

Auto-Connect Example



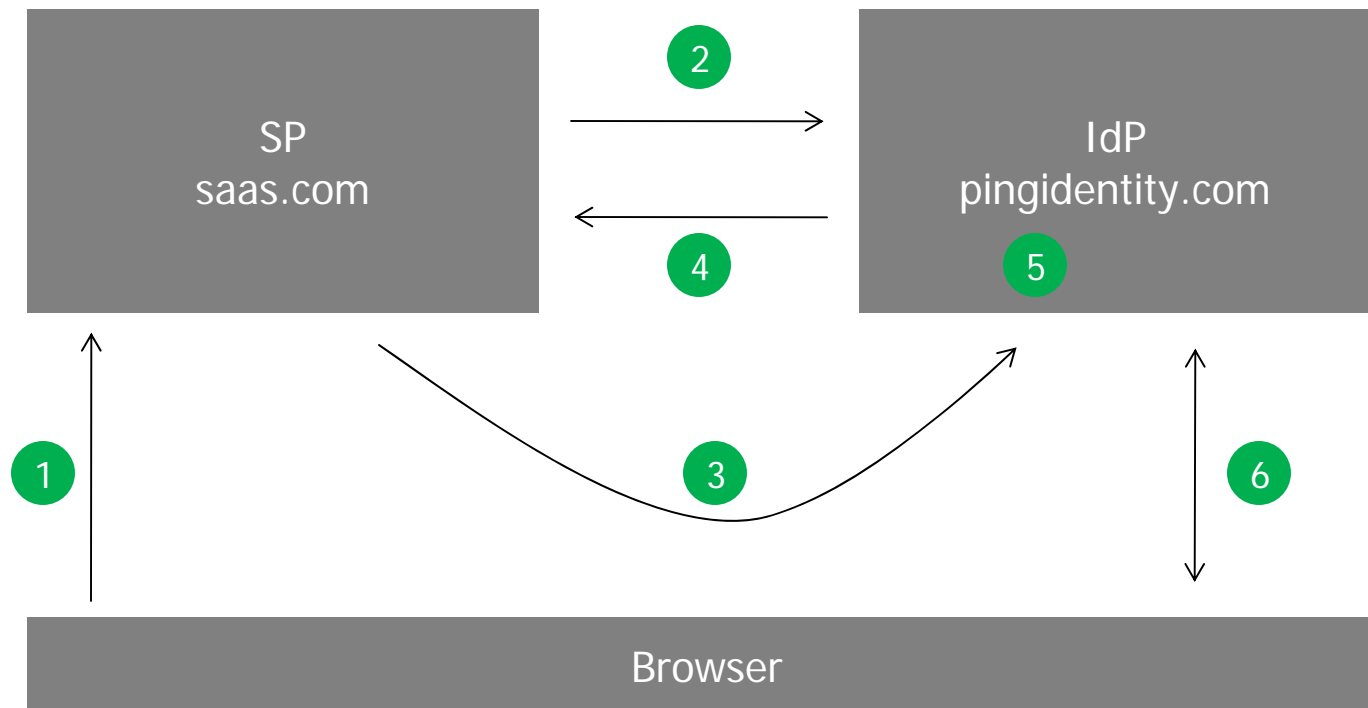
(4) The IdP retrieves and validates the signed metadata file from the SP

Auto-Connect Example



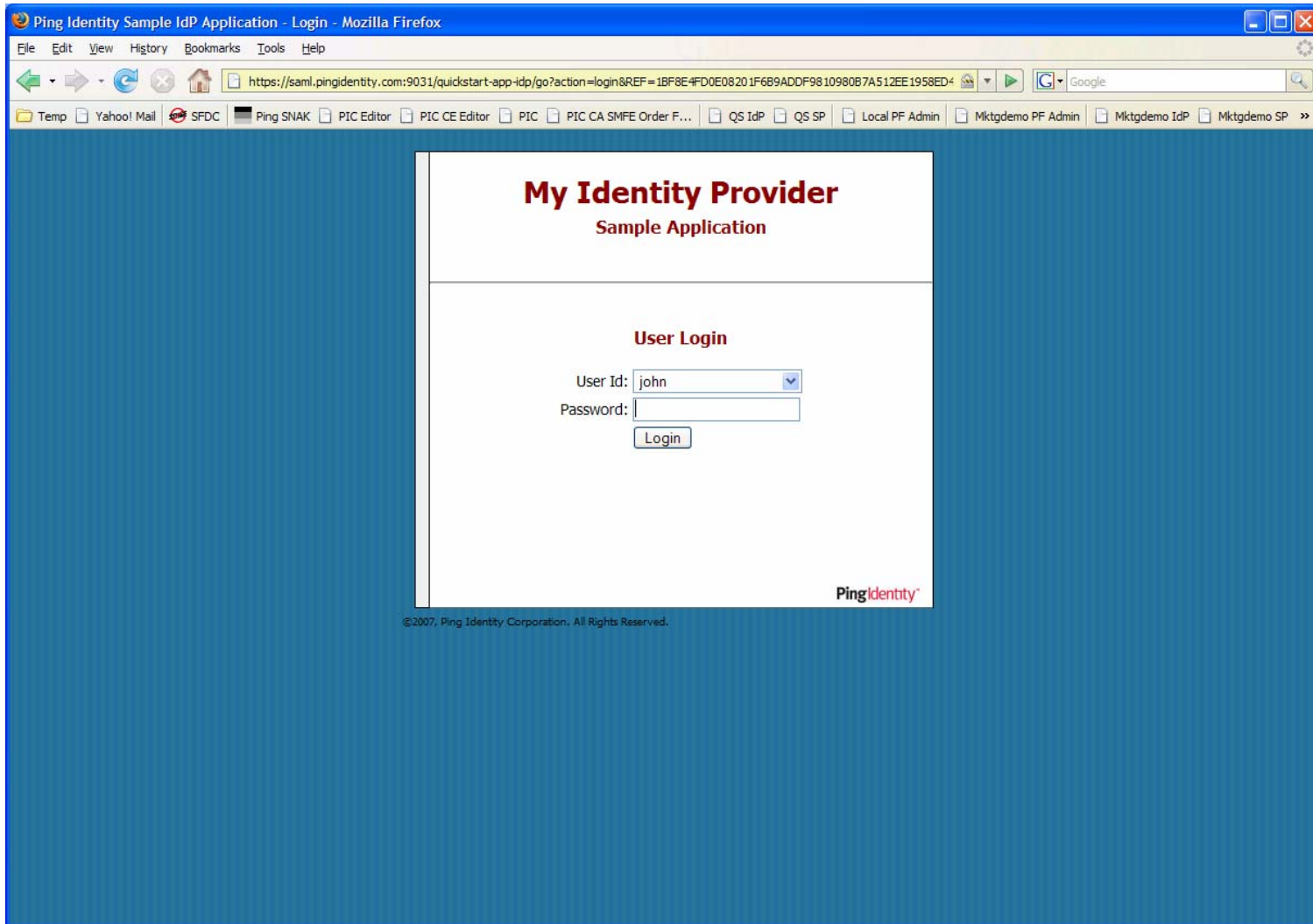
(5) IdP validates the SAML AuthNRequest

Auto-Connect Example

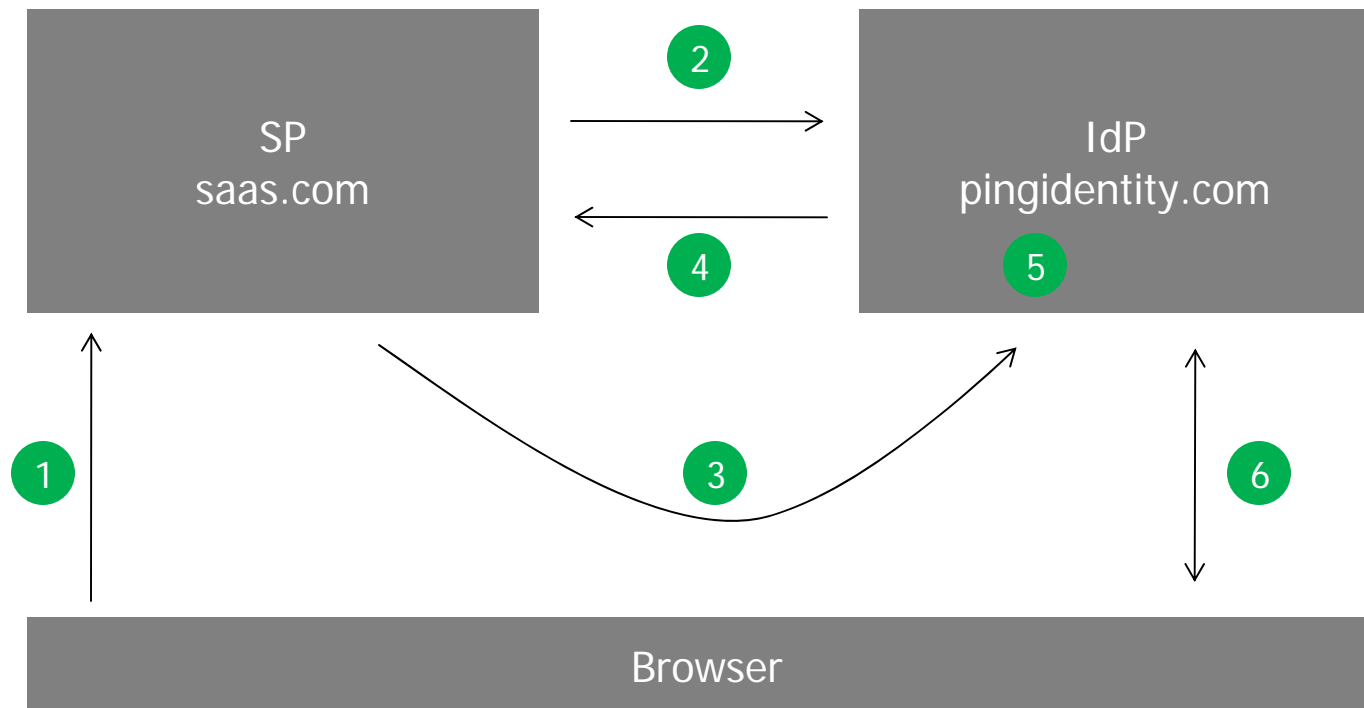


(6) IdP authenticates the user

User Authenticates At Their Identity Provider

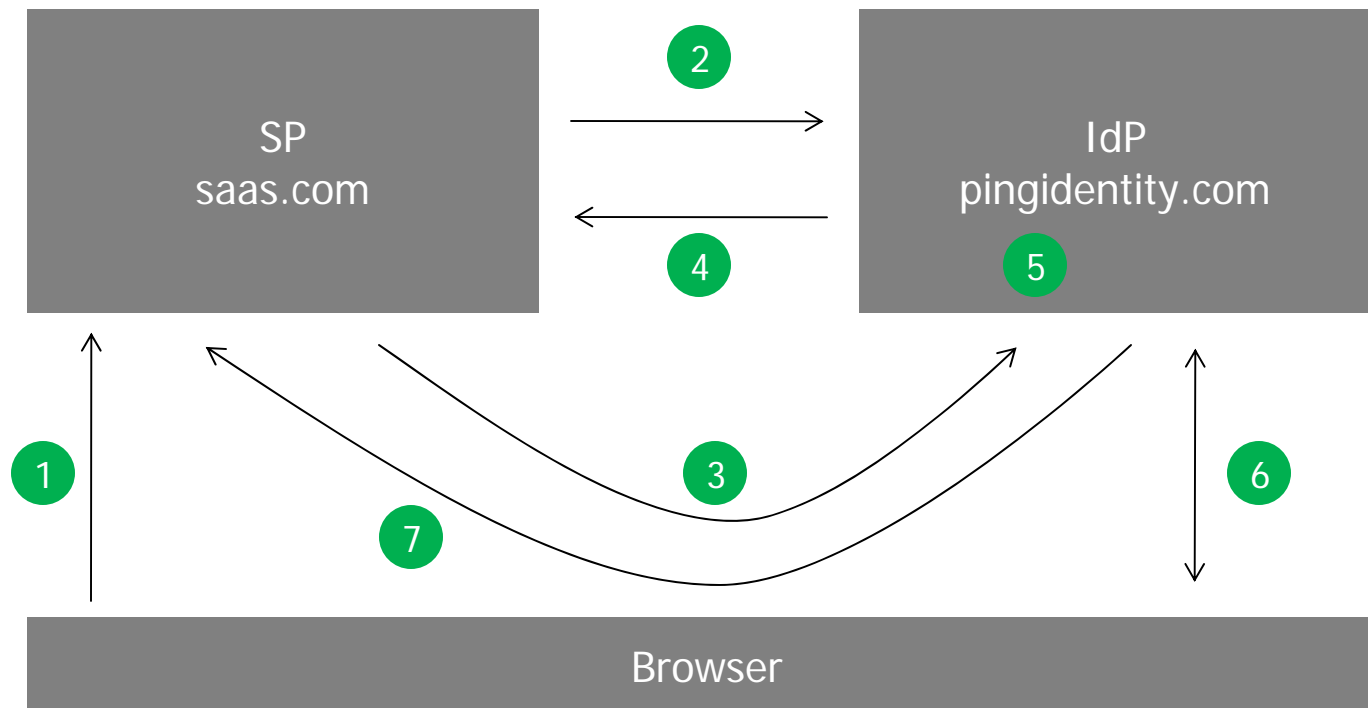


Auto-Connect Example



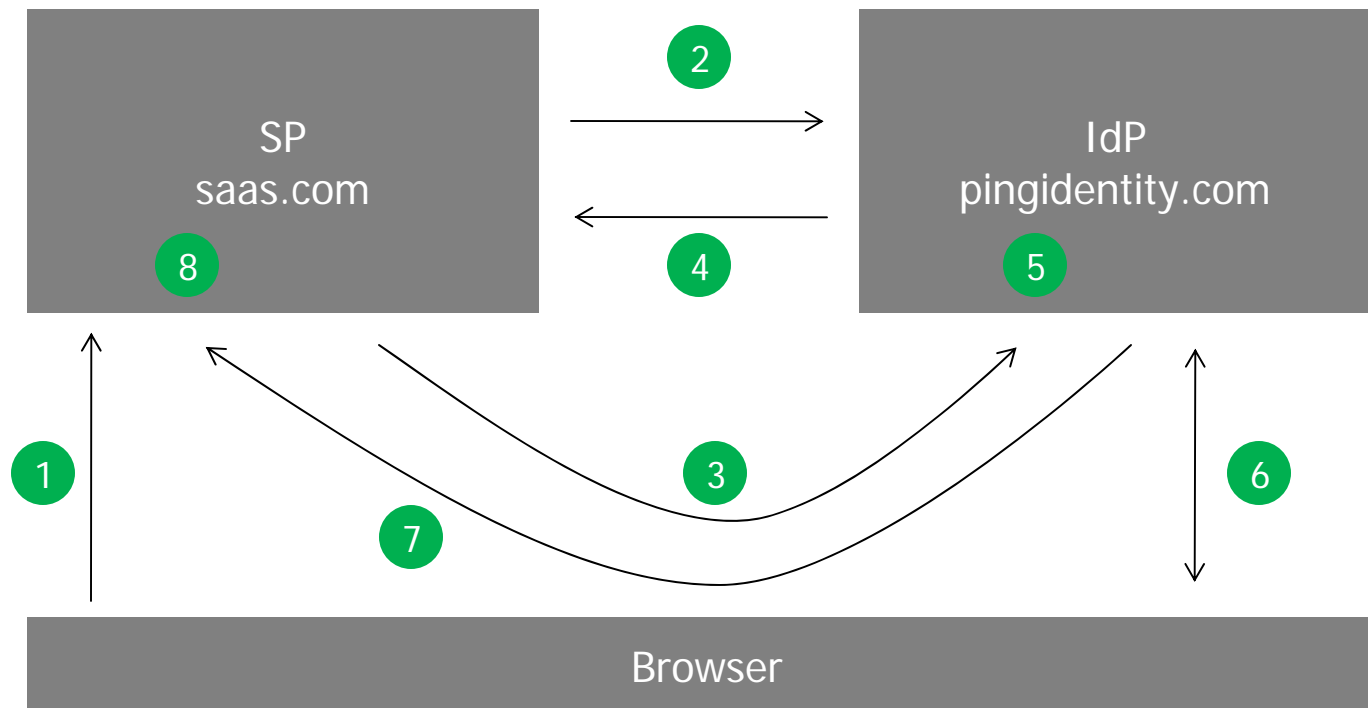
(6) IdP authenticates the user

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!

Sample SP Application - Target Resource - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://saml.pingidentity.com:9031/quickstart-app-sp/go?REF=938E72E797F0B0DC11681C5E43A5978B8AFA26F8B0AA69FB9A7F2C33: Google

Temp Yahoo! Mail SFDC Ping SNAK PIC Editor PIC CE Editor PIC PIC CA SMFE Order F... QS IdP QS SP Local PF Admin Mktgdemo PF Admin Mktgdemo IdP Mktgdemo SP >>

My Service Provider Sample Application

Local Logout

User Attributes From the IdP

Attribute	Value
UserId	john
authnInst	2007-11-29 18:11:08-0700

Terminate Account Link

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.

Single Logout | via: Redirect | POST | Artifact | SOAP

PingIdentity™
© 2007, Ping Identity Corporation
All Rights Reserved

Whats Next

- Solicit and incorporate use case feedback
 - ▶ Shibboleth, Concordia, DIDW, 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