

## PingEnable Methodologies Overview

Born from lessons learned and practices mastered from over a 200 successful secure Internet single sign-on (SSO) deployments, PingEnable's detailed methodologies guide IT organizations and line of business owners through each step of the identity federation process. PingEnable's methodologies are available to all PingFederate customers and can be used individually or in conjunction with other PingEnable services. PingEnable methodologies include:

- Evaluation
- Quick Start Implementation
- Custom Application Interfacing
- Managing Connections Partners 2 –n

This document provides an abbreviated overview of the different PingEnable methodologies; the detailed methodologies can be downloaded at [www.pingidentity.com/products/downloads.cfm](http://www.pingidentity.com/products/downloads.cfm).

### Evaluation Methodology Synopsis

The proof of concept methodology is designed for enterprises and service provider IT organizations to execute a proof of concept, or trial, for secure Internet singles sign-on via federated identity management. The contents include a federation checklist (this list is abbreviated below for users who want a first glance) it is designed as a list of requirements to test with federated identity management vendors and is a synopsis of years of trials with hundreds of different organizations across a multitude of industries including enterprises, service provider, and government organizations and information from industry organizations such as the Liberty Alliance and OASIS. Not only can the proof of concept methodology be used to trial PingFederate, it can also be used to test other federated identity management products. Your trial should take no longer than one day to complete with the methodology.

#### **Evaluation (Abbreviated):**

1. Signing and Validation - Decide which SAML messages — assertions, responses, requests — will be digitally signed and how the messages will be verified by your federation partner.
2. Back Channel Security - Determine what type of SOAP channel authentication will be used.
3. Trusted Certificate Management - Determine whether both partners are using SSL and/or signing certificates that have been signed by a major certificate authority.
4. Deployment - Decide how identity federation fits into your existing network.

5. Server Clock Synchronization - Ensure that both the SP and IdP server clocks are synchronized.
6. User Data Stores - Identify the type of data store that contains user data when needed.
7. Web Application and Session Integration - Decide how the IdP side of PingFederate receives subject identity information to look up the session.
8. Transaction Logging - Decide whether transaction logging should be integrated with a systems management application and whether you have regulatory compliance requirements that affect your logging processes.
9. Identity Mapping - Decide whether you will use identity federation to link accounts on your respective.
10. Attribute Contract Agreement - Decide on a set of attributes that the IdP will send in an assertion.
11. Metadata Exchange - Decide whether you will use the metadata standard to exchange XML files containing configuration information.
12. Configuration Data Exchange – Decide how connected partners will exchange data.
13. Timeline – Determine project timeline.

## **Quick Start Implementation Methodology Synopsis**

The quick start implementation methodology is designed for enterprise and service provider IT and security organizations to implement Ping Identity's PingFederate. The methodology provides information about using PingFederate to deploy a secure Internet SSO via federated identity management solution based on the latest security and e-business standards. The abbreviated list below provides basics steps of what is required to implement identity federation in production.

The overall process for deploying Ping Federate in your environment can be accomplished with or without a federation partner. The steps outlined below and detailed in the methodology describe the optimal approach to deploying secure Internet SSO identity federation.

### **Quick Start (Abbreviated):**

1. Define your Network Architecture - While Ping Federate can be hosted in a number of different deployment configurations, most choose to create development, QA and Production deployment architectures.
2. Obtain your software and license key - Installation is quick and easy and extremely portable. Many choose to pilot on a development server and then promote the entire configuration to actual QA and Production platforms simply by exporting and importing the Ping Federate Configuration archive.
3. Define your Federation Role:
  - a. IdP - Define and configure your IdM source - Install and configure the appropriate Integration Adapter to extract the identity information for the federate user.
  - b. SP - Define your Target Access System(s) - Install and configure the appropriate Integration Adapter to establish a user session in the target application of access system(s).
4. Configure the IdP/SP Connection - Configure the connection definition information with cooperation from your federation partner. Determine the federation bindings, attribute contract, signing/encryption requirements, assertion consumer and transport layer.
5. Promote configurations.
6. Quality assurance test.
7. Go live.

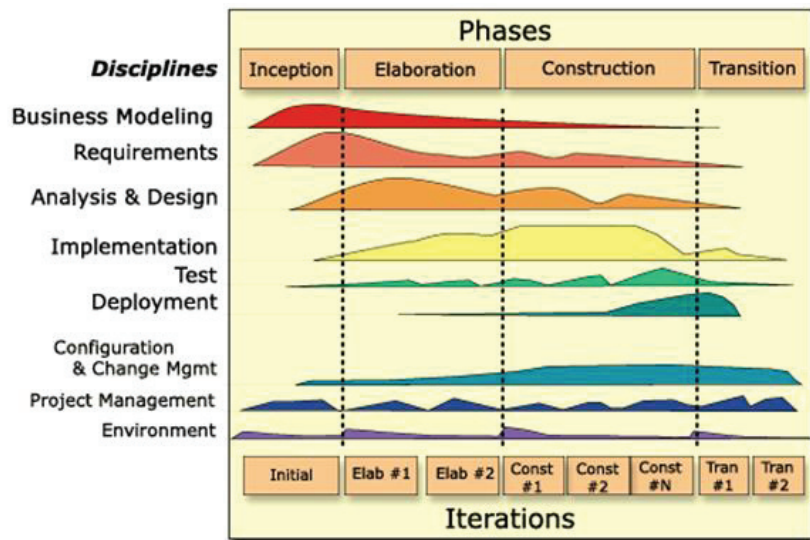
## Custom Application Interfacing Methodology Synopsis

To get started, download the SharePoint software solution at [www.pingidentity.com/products/downloads.cfm](http://www.pingidentity.com/products/downloads.cfm). You can easily have SSO to and from SharePoint in hours.

The custom application interfacing methodology is designed for enterprise and service provider IT, security and engineering organizations to integrate a custom application, or in-house developed system, with Ping Identity's PingFederate. The methodology provides information about integrating different applications designed in Java, .NET and PHP with PingFederate to deploy a secure Internet SSO via federated identity management. This methodology is derived from a Rational Unified Process. It includes four phases: inception phase, elaboration phase, construction phase and transition phase.

The abbreviated list below provides a brief overview of the four basic phases and what can be expected to develop a custom integration with PingFederate.

### Custom Application Interfacing (Abbreviated):



## Managing Connections Partners 2 - n Methodology Synopsis

The managing connections partners 2 thru n methodology is designed for enterprise and service provider IT, security and engineering organizations develop a handbook for turning up partner connections with PingFederate. Economies of scale are achieved in identity federation when the time to turn-up new connections is decreased. By completing the partners 2 thru n methodology, you will build a handbook that will provide specific step-by-step instructions for your partners in order to decrease the time and effort to provide secure Internet SSO. The methodology provides a process for engaging and educating customers and includes onsite and offsite phases.

The abbreviated list below provides a brief overview of the basic phases and what can be expected to connect with your partners.

### Managing Connections Partners 2 - n (Abbreviated):

1. Onsite meeting with connecting partner to gain understanding of connection requirements
2. Deployment architecture planning
3. Interoperability policy
4. Certificate management policy
5. Authentication management policy
6. Attribute management policy

7. Session policy
8. Logging policy
9. Risk and liability management policy
10. Error and event management policy

### **About PingFederate**

It is easy to see why identity federation projects can take six months or longer with hundreds of possible ways to implement SSO that works over the Internet. That is why Ping Identity developed PingEnable, customizable service and support designed to meet the specific needs of our customers' identity management environments. PingEnable's expert methodologies, training, support and services are available for each step of the identity federation process from learning, evaluation, and implementation, to deployment of the 100th connection. Customers who take advantage of PingEnable successfully deploy secure Internet single sign-on in 30 days or less. Learn more at <http://www.pingidentity.com/support-services>.

### **About Ping Identity Corporation**

Ping Identity's dedication to delivering secure Internet single sign-on software and services for over 200 customers worldwide has earned us recognition as the market leader in federated identity management. PingFederate®, the world's first rapidly deployable identity federation software, provides an organization's users safe access to Internet applications without the need to re-login. Through standards-based identity federation, PingFederate reduces repeated user provisioning and time-consuming proprietary SSO implementations. Over a dozen PingFederate integration kits easily enable first-mile integration, leveraging existing identity management infrastructure, and last-mile integration, providing scalable target application connections. PingFederate provides an additional module for Web Services. Download a free trial at <http://www.pingidentity.com>. For more information, dial toll-free 877.898.2905 or + 1 303.468.2882, or email [sales@pingidentity.com](mailto:sales@pingidentity.com).

© 2008 Ping Identity Corporation. All rights reserved. Ping Identity, PingFederate, and the Ping Identity logo are trademarks or registered trademarks of Ping Identity Corporation. All other trademarks or registered trademarks are the properties of their respective owners.