

Enabling Freedom of Choice for SaaS Single Sign-on

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Ping Identity

October 2009



IT MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS AND CONSULTING

Table of Contents

Executive Summary	1
Introduction: Securing the SaaS Opportunity	1
Understanding Today's Options for SaaS Single Sign-on.....	2
When Maintaining Enterprise Control is a Priority.....	2
When Convenience is Key	3
Which Approach is Best?.....	3
EMA Perspective: Ping Identity	4

Executive Summary

Software-as-a-Service (SaaS) and related concepts such as Cloud Computing are top-of-mind in the enterprise today, but there are factors organizations must weigh when considering a SaaS alternative. User access credentials such as usernames and passwords can pose significant risks if not controlled. Single sign-on (SSO) for SaaS offers a way for enterprises to not only gain control over user credentials, but to make the SaaS experience more seamless for users, allowing them to access SaaS resources more transparently.

Enterprises must, however, weigh how they employ SSO for SaaS. Today, a number of alternatives exist, allowing organizations to choose the best fit for balancing business priorities with risk control. Some will look to a SaaS provider to manage user identities directly, as part of the larger value of the SaaS offering. Increasingly, leading SaaS providers enable their customers to leverage their user accounts in SSO with other SaaS vendors. Outsourcing identity management has value for the business, and a provider that may be able to deliver a higher or more consistent level of control may have appeal to risk managers, if they understand the implications of this alternative.

For the enterprise that prefers to leverage its own identity and access management resources, established approaches such as identity federation have been joined in the market more recently by SSO as a service for SaaS. SSO as a service enables organizations to integrate with one resource that can enable SSO with many SaaS providers. This approach can be balanced with “first mile” integration with readily deployed techniques inside the enterprise such as identity federation, which even more strongly protects usernames and passwords from external exposure.

In this paper, Enterprise Management Associates (EMA) examines these alternatives and the factors organizations will want to consider when weighing their SSO for SaaS options. The values Ping Identity brings to this market are considered, as an example of a vendor who has long focused on enterprise SSO as its primary interest.

Introduction: Securing the SaaS Opportunity

The concept of IT offered as a service has become one of the hottest topics in the industry. From existing Software-as-a-Service (SaaS) offerings, to what the future of Cloud Computing may hold, IT delivered as a service offers high promise for reducing IT costs and administrative overhead. SaaS offerings in particular enable large enterprises and small businesses alike to gain access to valuable functionality without requiring a substantial up-front investment in an equivalent buildout, shifting IT costs from the capex to the opex side of the budget. Just as importantly, SaaS eliminates the long-term burdens of maintenance, technology turnover and talent retention required to keep on-premises resources running.

In order to capitalize on the SaaS opportunity, however, enterprises must become fully aware of the risks. For example, a SaaS offering often creates its own set of access credentials for individual users. This adds to the number of individual accounts users must manage. When this involves functionality sensitive to the enterprise, it complicates the management of access to important resources and can amplify risk exposure.

From existing Software-as-a-Service (SaaS) offerings, to what the future of Cloud Computing may hold, IT delivered as a service offers high promise for reducing IT costs and administrative overhead.

Today, a number of approaches to solving this problem are emerging, giving flexibility to enterprises of all sizes. In order to make the best choice for an individual business, however, enterprises should consider the right fit for the need.

When weighing how best to gain control over identity and access management for SaaS, organizations must consider factors of security and compliance, as well as convenience and ease of administration and use.

Understanding Today's Options for SaaS Single Sign-on

When weighing how best to gain control over identity and access management for SaaS, organizations must consider factors of security and compliance, as well as convenience and ease of administration and use. Some businesses will prefer to outsource identity and access management to a service provider, who may offer a level of control not otherwise available to a small or highly resource-constrained business. Others will want to retain more direct management over access control to assure a higher level of security and (where relevant) regulatory compliance.

When Maintaining Enterprise Control is a Priority

Enterprises that wish to retain more direct control may want to consider extending existing in-house identity and access management capabilities to their SaaS resources. This approach effectively creates Single Sign-on (SSO) for SaaS using existing enterprise user accounts, enabling an individual to use their enterprise login to access SaaS providers as well as on-premises resources.

When today's emerging approaches to SSO for SaaS leverage the well-established technology of identity federation, they may differ significantly from traditional federation techniques. In a traditional approach to federation, an enterprise may have been required to establish federation relationships with *each* external resource in a "one-to-many" scenario. Instead, today's SSO for SaaS offerings enable the enterprise to establish a "one-to-one" relationship with a *single* resource which, in turn, facilitates SSO with a number of SaaS providers. This one-to-one relationship reduces complexity and improves the manageability of SSO for SaaS, which in turn helps to reduce risk. It parallels the benefits of SaaS by reducing the amount of buildout and maintenance the enterprise must undertake in order to extend SSO to multiple SaaS offerings. For the SaaS provider, centralized SSO as a service enables it to extend more manageable SSO capabilities to a much larger number of enterprises.

One of the advantages of identity federation is that it protects users and enterprises by abstracting authentication information, protecting usernames and passwords as well as primary identity stores from direct exposure to exploit. When federation is offered as a service, however, this may require direct interaction between enterprise identity stores and the federation service outside the enterprise boundary. Organizations concerned about exposing these interactions beyond the enterprise may therefore consider a hybrid approach, in which a resource such as a federation server is placed inside the enterprise to protect these "first mile" exchanges. It is then the federation server that interacts with the service, insulating enterprise identity resources from direct external contact. This approach keeps direct interaction with enterprise identity management systems entirely within the boundaries of the enterprise, further reducing risk. When an on-premises federation server performs this function, it also enables the enterprise to leverage well-established identity federation standards such as SAML (the Security Assertions Markup Language) to extend SSO more broadly to other business partners as needed.

When SSO deployments leverage existing identity federation standards and specifications such as SAML or WS-Federation, they employ techniques that have been in enterprise operations for years, and may have been developed in part through community involvement. These approaches often offer a strong set of security capabilities that can be leveraged to strengthen the confidence in single sign-on beyond the enterprise, with substantial flexibility in defining an appropriate level of control.

When Convenience is Key

Other organizations may choose to outsource identity and access management itself to a SaaS provider. This serves the business that, for example, elects to utilize SaaS for a wide range of functionality such as office productivity and enterprise applications. In these cases, the enterprise sees user identity and access management as part of the larger value of the SaaS offering. It is also an option for the business that turns to SaaS as an alternative to maintaining its own IT investment, often the case for resource-constrained businesses or organizations that would otherwise find it difficult to assure an adequate level of control over identity and access management on their own.

In this approach, the SaaS provider manages user accounts directly. Increasingly, it may also be able to extend its user accounts to SSO for other SaaS offerings. A noteworthy example is Google Apps Premium, which leverages user accounts to extend SSO with other SaaS offerings through established identity federation techniques such as SAML, as well as through more recent approaches such as OpenID. OpenID is one of a group of emerging approaches to so-called “user-centric” identity, which allow individuals to use a single identity with multiple resources. Many already have an OpenID and may not know it, if they have an account with Gmail, Yahoo!, AOL, LiveJournal, or other OpenID-aware services.

This breadth of OpenID-capable services reflects an OpenID design philosophy that some have expressed as “trust and accept all comers.” Businesses, however, need constraints. In Google’s case, it has added security measures to its implementation of OpenID that enhance the validation of identity providers (those who supply identity credentials in an OpenID exchange), as well as validation of the exchanges themselves. When using Google Apps identities in SAML-based SSO with other service providers, Google leverages Ping Identity’s PingConnect, which provides the proven enterprise-class capabilities of SAML as a service. Thus, by choosing Google Apps, the enterprise is using an already existing and centrally maintained resource as the identity authority for multi-service SaaS SSO, rather than building another copy of identity information in an authentication store.

Which Approach is Best?

Which approach to SSO for multiple SaaS providers is right for a given organization? That depends on the risk profile and preferences of the enterprise, as well as its business requirements and constraints.

Outsourcing the direct management of user accounts to a SaaS provider that enables SSO with other SaaS resources offers the advantage of “offloading” user account and access management, and its related costs and other burdens such as ongoing maintenance. It may also reduce the complexity of management for the

Which approach to SSO for multiple SaaS providers is right for a given organization? That depends on the risk profile and preferences of the enterprise, as well as its business requirements and constraints.

customer, which may help to reduce risk. Above all, it is convenient. It leverages existing accounts already managed by a service such as Google Apps, and adds to them the ability to use existing identity credentials with a number of other SaaS offerings.

Customers should be aware, however, that they are giving up a measure of control to the SaaS provider in order to reap the benefits of outsourced management, and will therefore want to work with the SaaS provider to assure that the provider protects the customer's interests to the extent possible. It also means that authentication takes place "outside the firewall." Usernames and passwords are exchanged directly with a service beyond the enterprise, as opposed to techniques such as identity federation that originates from inside the enterprise, such as the hybrid approach described earlier. Accepting the service provider's approach may also limit flexibility for adding capabilities such as strong authentication when warranted.

When the enterprise has confidence in its capability to assure sufficient risk control in its own management of user identity and resource access, or priorities such as direct control or flexibility in strengthening authentication are primary concerns, businesses may prefer to extend the enterprise identity management investment through enterprise-class federation, or through the increasingly visible option of integrating with SSO services for SaaS. Both offer the option of keeping usernames and passwords inside the enterprise, abstracting authentication through techniques such as identity federation. They can leverage existing enterprise identity resources such as LDAP or Microsoft Active Directory for SSO beyond the firewall. When leveraging standards such as SAML, they take advantage of years of testing and evaluation in deployment.

EMA Perspective: Ping Identity

When it comes to thought leadership in single sign-on, few have dedicated themselves to the challenge as much as Ping Identity. For many years, Ping has focused primarily on identity federation, resulting in one of the largest installed bases of federation customers in the industry, with more than 370 at present, including 42 of the Fortune 100. As IT delivered as a service comes increasingly into its own,

Ping may find itself in an enviable position of having focused on a primary technology for cross-domain identity enablement.

When it comes to thought leadership in single sign-on, few have dedicated themselves to the challenge as much as Ping Identity.

Today, Ping's offerings make the most of this expertise. The company's PingFederate product enables a more straightforward deployment of identity federation, in days rather than months in some cases, mitigating one of the most significant concerns of an identity management deployment. Its more recent PingFederate Express offering enables service providers to quickly establish SAML connections with PingFederate identity providers, providing a more convenient approach to SSO integration leveraging SAML

techniques. With the establishment of PingConnect, Ping offers enterprise SSO for multiple SaaS providers as a service, enabling businesses to connect with a single service provider for SaaS authentication. Customers can either connect directly with PingConnect or integrate an on-premises federation server such as PingFederate for more secure cross-domain SSO.

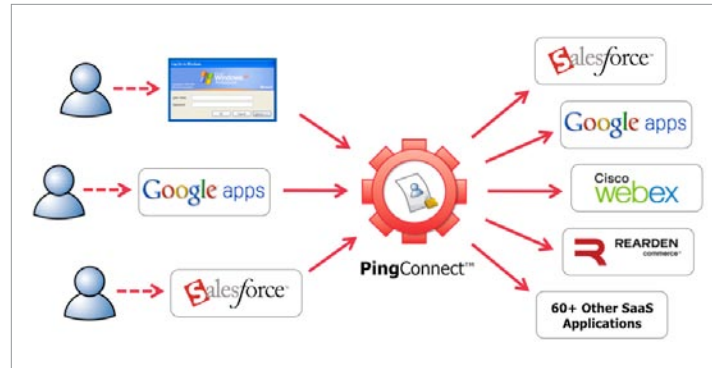


Figure 1: PingConnect is Ping Identity's on-demand SaaS Single Sign-on and user account management service, offering easily configured SSO for SaaS that interfaces with Microsoft Active Directory, Google Apps, and a number of popular SaaS offerings.

When considering the emerging range of options for SaaS single sign-on, enterprises will want to consider how Ping Identity's offerings capitalize on the proven capability of federation techniques such as SAML, which have become widely adopted among global enterprises. Ping's approach reflects years of dedication to optimizing one identity per user for multiple business requirements. The fact that Ping's capabilities have been embraced by thought leaders such as Google speak to its distinctive leadership opportunity in SSO for SaaS, giving the potential customer of IT delivered as a service a new range of options and freedom of choice in finding the single sign-on solution that fits best.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow [EMA on Twitter](#).

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2009 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com



1962.093009