Ping Identity®

White Paper

The Three Tiers of Single Sign-On (SSO)

Executive Summary

Although the term "SSO" seems self-descriptive, the technical approaches to accomplishing SSO get muddy for all but the identity security savvy IT manager. What may seem like a secure, convenient and affordable solution can impose a significant cost and risk to the enterprise, yet still have its place in the market either for the SMB or consumer businesses. This paper defines three tiers of SSO so that you can make informed decisions on which type is appropriate for your organization's identity and access management requirements.

Table of Contents

Executive Summary 1
SSO Background 3
SSO Today 3
Tier 1 SSO: Enterprises with a Cloud-1st Strategy 4
- Standards-based, Cross-domain Authentication 4
- Key Advantages 4
- Key Drawbacks 4

Tier 2 SSO: Enterprises with a Cloud-2nd Strategy 5
- Proprietary, Single Domain Authentication 5
- Key Advantages 5
- Key Drawbacks 5

Tier 3 SSO: SMBs Moving to the Cloud (outside of high-security environments) 6
- Credential Replay, Cross-Domain Authentication 6
- Key Advantages 6
- Key Drawbacks 6

Conclusion 7
Tier 1, Tier 2 and Tier 3 SSO Product Classes and Use Cases 8

SSO Background

Single Sign-On (SSO) is not a new concept in information technology. From the days of mainframes, SSO has played a key role in maintaining productivity and security INSIDE the protection of firewalls. In the 1990's many organizations moved to a combination of custom-built authentication systems, commonly known as Enterprise SSO (ESSO) and later matured into browser-based plugin or web-proxy methods known as Web Access Management (WAM). Protocols such as Kerberos also contained SSO features, however, the focus at that time was on integrating applications within the network perimeter only.

At the millennium, perspectives on SSO began to shift toward a broader adoption of cloud-based services, including Software as a Service (SaaS) and consumer-facing SSO by large-scale Internet providers, such as Facebook and Google. The reason? Enterprise users were signing into SaaS applications outside the enterprise perimeter and the domain-based SSO mechanisms were breaking.

In 2012, SSO technologies began to mature, with product options and classes to fit any size enterprise, business and consumer. This is in large part due to the SAML 2.0 protocol specification, which became an OASIS standard in March 2005. With SAML and other following open identity standards such as OpenID, OAuth, and, most recently, SCIM, a new class of SSO has emerged for the cloud generation.

SSO Today

The idea of today's SSO is simple: an end user authenticates once, gaining access to many applications. Implementation of SSO can take many forms, but the preferred architecture is for a user to authenticate to a centrally managed system, and for applications to trust that central system for identity information about the user rather than re-authenticating. But since this isn't always possible, many organizations use SSO workarounds, such as "scraping" login forms and automating authentication on behalf of a user by storing and replaying passwords. This means SaaS vendors are in a constant state of feature release rather than enjoying the long innovation cycles of the enterprise software past. The result? Customized, old-school SSO solutions are breaking.

What is passed over the Internet: Tier 1 Vs. Tier 3 SSO

Using Tier 3 SSO – Passwords are relayed

Company = acmecorp.com
Username = admin
Password = password1234

Using Tier 1 SSO – Passwords are eliminated

Token: acme.ef297c36-d88a-42f3-8651-70c5fc85c801

Tier 1 SSO: Enterprises with a Cloud-1st Strategy

Standards-based, Cross-domain Authentication

Tier 1 SSO is based on proven standards connecting a web session to the application and authenticating back to a central directory that acts as the single place to enforce policies. Tier 1 SSO does not involve exchange of passwords or duplicating of user directories – user identities are controlled by IT in a corporate directory. The very best products in this category should not require much customization at implementation, if any. Tier 1 SSO represents a "cloud applications first" stance in tackling SSO and is designed for Internet scale. Cloud-based Tier 1 SSO solutions are now coming to market providing the multi-tenancy you've come to expect in any SaaS application.

Key Advantages

1. Maximum security when moving to the Cloud
2. Highest convenience to all parties: users, IT and application providers
3. User passwords are stored once, in a location protected by the enterprise
4. Highest reliability as browser and web applications go through revisions
5. No vendor lock-in due to standards
6. Generally, the lowest Total Cost of Ownership (TCO)

Key Drawbacks

1. Must have identity expertise on-hand in some deployment scenarios
2. Requires participating parties to cooperate in implementing

The defining aspect of Tier 1 SSO is that authentication is driven by standards-based token exchange while the user directories remain in place within the centrally administered domain as opposed to synchronized externally. Use of passwords for applications are eliminated aside from the authentication process into the user directory, such as Microsoft Active Directory. All authentication information passed over the network is fully encrypted. Tier 1 SSO depends on open and proven standards, such as SAML (Security Assertion Markup Language), OpenID Connect and OAuth.

In a Tier 1 SSO solution, when the connection to an application is made, the SSO service is removed from the flow of traffic after the session is established vs. remaining in the middle as a constant proxy through which all traffic must travel. This assists in maximizing throughput, reducing latency, eliminating a single point of failure and potential privacy violations. There are legitimate cases where a proxy may be necessary, especially in certain industries— for instance, packet inspection for governance functions–but these are adjunct services rather than the core of SSO.

Tier 2 SSO: Enterprises with a Cloud-2nd Strategy

Proprietary, Single Domain Authentication

Tier 2 SSO may be necessary in organizations with many legacy applications that cannot be integrated into more modern user directories, such as Microsoft Active Directory. Tier 2 SSO product suites have been modified in recent years to accommodate cloud applications on the margin using **Web Access Management** methods. In Tier 2, SSO to SaaS applications is sub-optimized to prolong the life of older applications that can't make the switch from older authentication and authorization methods.

Key Advantages

1. Provides password relief in older, legacy enterprise environments for applications, which can't use modern user directory technologies
2. Provides a single centralized domain-centric session to apply policy
3. Tier 2 environments may already exist and provide sufficient SSO functionality for internal needs

Key Drawbacks

1. Often highly customized and proprietary
2. Very high Total Cost of Ownership (TCO)
3. Need control of both browser and application versions or will break
4. Not well-suited for integration of cloud-based applications
5. Opportunity for security compromises at several points

Tier 2 SSO is mature and has traction, but often uses proprietary technology to track user sessions and interface with remote applications. In the case of WAM, an encrypted session cookie is used to maintain state – a mechanism that cannot work in the Cloud due to Same Origin web policy for cookies. Token-based Tier 2 protocols, like Kerberos, are also unable to cross multiple domains. Some Tier 2 products are bridging these gaps by bolting on Tier 1 functionality, such as SAML modules; other Tier 2 products have chosen to bolt on Tier 3 functionality, such as **screen scraping** and password duplication.

Because Tier 2 infrastructure is often embedded into monolithic application stacks, it can be easier to create hybrid architectures where Tier 1 solutions layer on top of Tier 2 solutions, using Tier 2's heavily domain-centric integrations to enable a standards-based jump to the Cloud.

Tier 3 SSO: SMBs Moving to the Cloud (outside of high-security environments)

Credential Replay, Cross-Domain Authentication

Tier 3 SSO stores usernames and passwords outside of IT control and replays the usernames and passwords to the applications over the Internet. This approach is a quick fix, relieving user password burden and IT password resets, but at the cost of optimizing security practices. Depending on the industry vertical of the organization, Tier 3 SSO may not meet compliance or regulatory requirements.

Key Advantages

1. Relatively low up-front cost in some cases (solutions can be free)
2. Small business users can store their personal information in the repository, which can be seen as a company benefit

Key Drawbacks

1. Security risk – in most solutions, users are in control of password strength; on non-SSL sites, credential text is freely passed across the Internet
2. Requires constant maintenance as password relay "breaks" when login pages are changed by vendors
3. Mixing personal and corporate data in a system controlled by an employer is a legal liability

Tier 3 SSO may include many different architectural deployment models where a database is deployed in a cloud service, private cloud, local server or even at the employee PC level. The attributes surrounding Tier 3 SSO include the following:

1. There is at least partial reliance on unique username and password storage for each accessed application vs. the passing of a secure token.
2. The employee is tasked with entering credentials into the database. Some Tier 3 SSO solutions may both auto-strengthen the password and mask it from the user.
3. The solution may still rely on a central corporate directory, but that is primarily used to get into the database.
4. Tier 3 SSO solutions may rely, in some part, on consumer services acting as an identity provider. For example, "Facebook Connect" or "MSN Live".

Tier 3 SSO can actually provide both user convenience and reduced IT administration costs (fewer password resets) for a small business. However, Tier 3 SSO makes it very difficult to enforce a central identity policy. Most solutions in this class allow employees to simply store a self-generated username and password. This is a **well-documented quandary** in enterprise IT as many usernames and passwords are statistically guessable.

Long-term cost and reliability should be considered very carefully, even for small businesses with password-reset pain. Tier 3 SSO solutions tend to rely on a process known as "screen scraping" where the product relays credentials in its database to an input screen on an application. Changes on a SaaS application log-on screen can happen quarterly in many cases, and this will break the relay of the credentials to the application, which breaks the SSO process. In addition, if there is no Secure-Socket Layer (SSL) service in place between the Tier 3 SSO application and the service provider, plain credential text will be passed across the Internet, which is a security liability.

Finally, businesses should consider that with Tier 3 SSO solutions, employees can store private SSO information, such as banking or frequent flyer log-in credentials. When an employee leaves the organization, they may be locked out of private data, making the corporation liable and responsible for resolution. As with data storage and corporate equipment, mixing corporate and personal use of a corporate-supplied Tier 3 SSO must be first carefully vetted with corporate policy. Often the best option is to direct employees to a Tier 3 consumer SSO solution, which they control post-employment.

Conclusion

As enterprises move critical corporate assets out of their data centers, Tier 1 SSO solutions become an important requirement. Every time a password is duplicated, attack vectors multiply and corporate risk increases, making Tier 3 SSO solutions dangerous. Tier 2 SSO solutions remain a useful internal strategy for managing applications, but cannot natively support the cross-domain communication requirements of the Cloud. Only through the use of standards-based Tier 1 SSO do enterprises gain the full advantage of SSO convenience without compromising security and control. It is advised to first understand your organization's particular use cases, compliance and regulatory requirements before jumping into the world of SSO for a better computing future.

Tier 1, Tier 2 and Tier 3 SSO Product Classes and Use Cases

SSO Class	Optimized Use Case	Defining Characteristics		Key Disadvantage	Reliability & Security	Representative Vendors
Tier 1	**Cloud-1st IT Strategy** Medium to large enterprises & governments with more than 75% of applications in a private or public cloud. Security, scale and "set and forget" is paramount.	**Standards-based, cross-domain authentication**	100% standard protocols; Passwords are eliminated. Applications do not store passwords. User directory information remains safely in place.	Requires participation and coordination between connecting parties.	Very high[1] Generally considered a "set and forget" approach.	Ping Identity Oracle (Federation) IBM Microsoft
Tier 2	**Cloud-2nd IT Strategy** Medium to large enterprises and governments with more than 75% of applications on legacy internal systems and on the domain.	**Proprietary, single domain authentication**	A domain-centric architecture. Depends, in great part, on proprietary protocols and cookies, translated by proprietary agents. Suitable for organizations who only need SSO within the domain. Highly customized ESSO and WAM products. High dependency on browser and web service-specific plugins and proxies.	Stability comes from strict browser and application version control in addition to all parts of the system. Generally highly customized and expensive. Domain specific use. Does not extend well in the cloud model.	Moderate[2] Higher touch over time than standards-based SSO. Customization requires customized support.	CA SiteMinder Imprivata Oracle (Passlogix) IBM NetIQ
Tier 3	**SMBs moving to the Cloud** Small and medium business looking to quickly take password reset burdens off of IT and employees. Self-help and cost are primary concerns. Security is a tertiary concern.	**Credential replay, cross-domain authentication**	Depends, at least in part, on replay of login forms AKA "screen scraping" versus protocols. Requires user listing passwords in a database; passwords are relayed to a login page.	Highly fragile. Security risk. The burden of password generation and updates are outside of IT control. Subject to breaking when browsers and applications are refreshed.	Low[3] Requires ongoing maintenance by employees, IT and vendors as app providers modify log in pages. "Screen scraping" is fragile.	SplashData 1 Password LastPass Okta Symplified OneLogin VMWare

1 Does not rely on customization. "Set and forget."
2 High degree of customization, often-proprietary techniques, resulting in high long-term maintenance due to the number of integrated pieces.
3 Relies in great part on "screen scraping" and relaying of credentials. Webpage changes frequently break flow.

About Ping Identity

Ping Identity provides cloud identity security solutions to the world's foremost companies, government organizations and cloud businesses. For more information, dial U.S. toll-free 877.898.2905 or +1.303.468.2882, email sales@pingidentity.com or visit pingidentity.com.

3/12.5