The Top 5 Federated Single Sign-On Scenarios

Table of Contents

Executive Summary 1

The Solution: Standards-Based Federation 2

Service Provider Initiated SSO 3

Identity Provider Initiated SSO 3

The Top 5 Scenarios for Federated Single Sign-On 4

Scenario 1: Corporate Login to Cloud Application 5

Scenario 2: Cloud Login to Internal Application 6

Scenario 3: Corporate Login to Internal Application 7

Scenario 4: Corporate Login to Partner Application 9

Scenario 5: Identity as a Service (IdaaS) Hub 11

The EmpowerID SSO Platform 12

Broad Standards Support 12

Login Workflow 12

Cloud Metadirectory/ Extranet Directory 13

Federated Application Development Environment 13

SSO and Role-Based Security for Microsoft SharePoint 14

About The Dot Net Factory 15

Executive Summary

To increase efficiency and competitiveness, organizations are increasingly transitioning from a traditional IT model based on internally hosted and managed applications to a new model in which enterprise applications are a mix of hosted, internal, and Software as a Service (SaaS) platforms. Key goals for organizations making the transition to this computing model include increasing productivity, reducing costs, and maintaining the security of their data.

In the past, in-house teams hosted and ran an organization's critical enterprise applications. Today, these operations are being turned over to third-party providers of Cloud applications for a variety of reasons. Organizations make the switch to gain the ability to rapidly scale capacity (both up or down), to outsource the capital costs and the staff expenses associated with maintaining datacenters and providing application support, and to obtain access to best of breed applications made by possible by Cloud Computing's substantial economies of scale.

The rapid acceptance of the Cloud application model has fueled revenue growth for many organizations by simplifying the process of signing up business partners or customers to access their services and data over the web. Use of Social Media Logins for business-to-business or business-to-consumer applications has been shown to increase adoption rates by simplifying the registration and login processes. The Cloud application model offers other financial benefits that can benefit organizations, including: a reduction in costs, an improving body of standards that is facilitating both connectivity and security, rapid scalability, and a subscription billing model that allows IT to be expensed for faster cost recovery.

However, as organizations move toward using more hosted Cloud applications residing outside of the organization firewall, controlling security and IT-related costs surrounding such can become problematic. The traditional security model for internally hosted applications is fairly straightforward with all users authenticating to a single directory, such as Active Directory, and being managed by a central identity management system.

Cloud-based external applications don't have access to the company's internal directories however, and must maintain their own directories for user authentication and authorization. Given the number of Cloud and hosted applications a typical worker may be required to use, this new model can quickly lead to identity fragmentation wherein each system requires a distinct set of credentials each time the user logs in. The result is reduced productivity, compromised security and increased costs. Developing an appropriate strategy for adopting Federated Single Sign-On (SSO) is a key security challenge for organizations grappling with the new Cloud Computing model.

Top Considerations for Cloud Computing without Federated SSO:

- How to maintain and audit enterprise-wide security and enforce policies when many applications are outside the control of the IT organization
- How to consistently enforce strong authentication standards such as two-factor authentication when users are logging into Cloud applications or performing a single sign-on from Cloud to corporate applications

- How to quickly and cost effectively provision and maintain application access in Cloud hosted or SaaS applications for new users
- How to prevent exploitation and security breaches that can compromise corporate data when users have a greater number of usernames and passwords
- How to control helpdesk expenses when a greater number of usernames and passwords will dramatically increase the frequency of password reset calls
- How to monitor access to Cloud hosted applications and to ensure that access is revoked in a timely manner when a user leaves an organization

This whitepaper discusses a flexible strategy for approaching these challenges and specifically how the EmpowerID Identity and Access Management platform offers a robust and comprehensive solution for organizations seeking to fully realize the benefits of Cloud Computing.

The Solution: Standards-Based Federation

A flexible standards-based federation solution that enables users to login once and then access applications without being prompted to login again is the key to solving these critical business challenges.

Single Sign-On (SSO) is the most important of services offered by identity federation because it allows employees, customers, and partners to access multiple Cloud or internal corporate applications using a single username and password. Furthermore, federated SSO allows users who are authenticated against one directory to access additional applications and services without re-authenticating when a trust relationship has been established, removing the need for users to remember multiple usernames and passwords by enabling single sign-on between organizations.

Organizations wishing to federate with one another require mechanisms in place that allow them to trust what each other has to say about user identities. A CoT (Circle of Trust) is a federation of Identity Providers (IdP's) and Service Providers (SP's) with legal, business and operational agreements that ensure seamless, secure data transactions for their members and users. These mechanisms are defined in part by the federated identity standards adopted by each organization. Federated identity standards make it possible for organizations to interchange identity data in a way that allows them to talk intelligently with one another. An important criterion for any federation system is the ability to support all major federated identity standards in use today, including Security Assertion Markup Language (SAML), OpenID, OAuth, WS-Fed, and WS-Trust in order to enable the broadest possible set of relationships.

In any federated identity management transaction, there are always three actors involved: The subject or user, the Identity Provider (IdP), and the Service Provider (SP) or Relying Party (RP). Subjects are the users of resources about whom an identity management transaction concerns. Identity providers are those parties that authenticate users, making an assertion as to their identity. Service providers are those parties that provide services to users based (in part) on the authentication events that occur between the IdP and the user. SP's rely on the integrity of the assertion supplied to them by the IdP to properly identity the user. This separation of authentication from the applications themselves allows for greater flexibility to support users logging into applications with a single username and password as long as it is from a trusted Identity Provider.

Service Provider Initiated SSO

There are two ways that single sign-on can be initiated in a SAML SSO scenario. Service provider initiated SSO is when a user attempts to access the Service Provider application and is redirected to an IdP for authentication because they do not have a current login session. After authenticating at the IdP, the user is redirected back to the Service Provider with a SAML assertion of their identity.

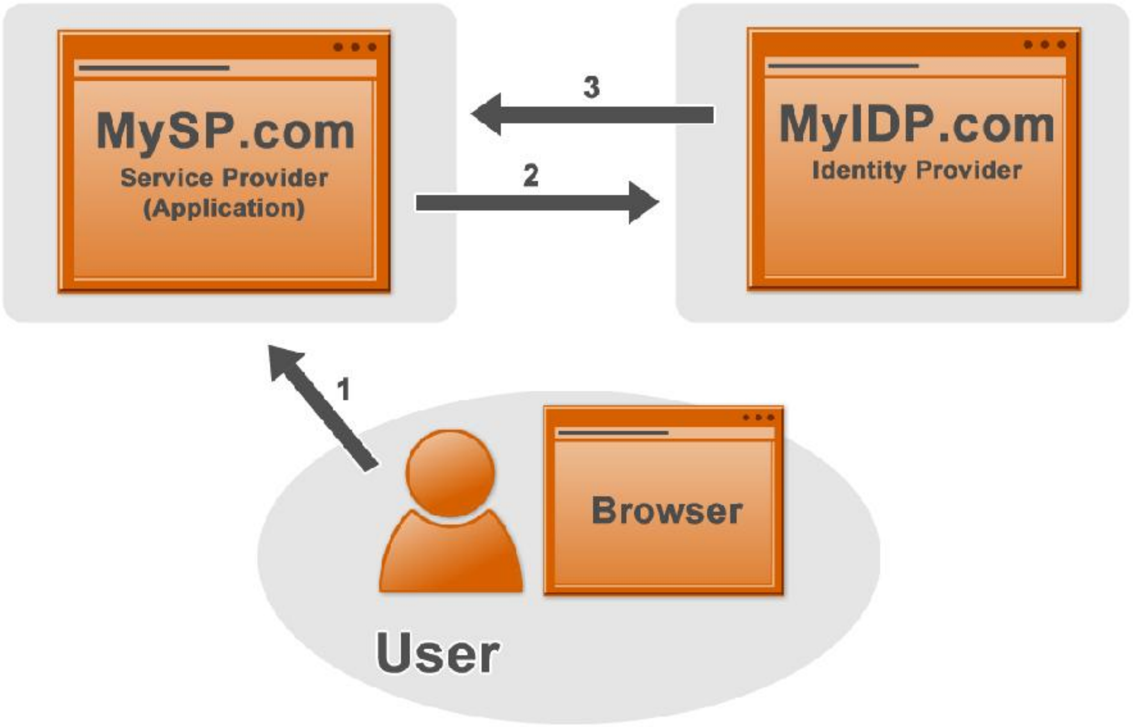

Figure 1. Service Provider-Initiated SSO

Identity Provider Initiated SSO

In Identity Provider initiated SSO, the Identity Provider is configured with specialized links for each Service Provider application. These links refer to the URL of the local Identity Provider's single sign-on service and pass parameters to the service identifying the remote Service Provider. So instead of directly visiting the Service Provider, the user goes to the Identity Provider site and clicks on one of the links to gain access to the remote Service Provider. This triggers the creation of a SAML assertion which is passed back to the user's browser and then automatically posted to the Service Provider allowing SSO access.

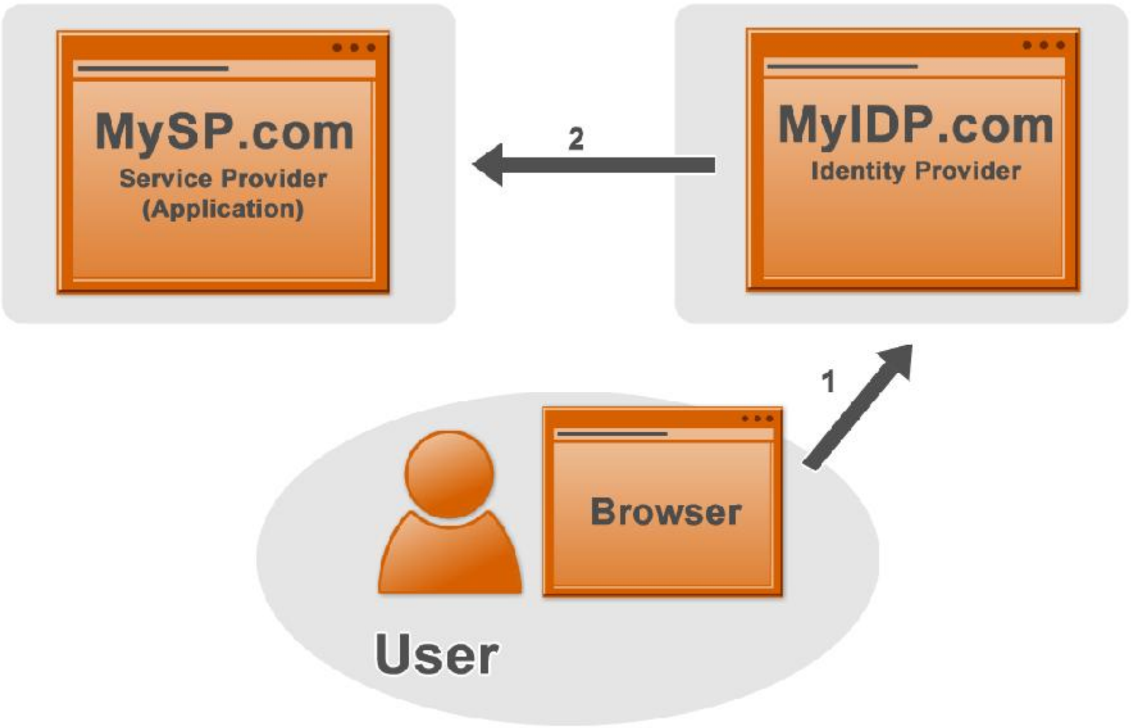

Figure 2. Identity Provider-Initiated SSO

The Top 5 Scenarios for Federated Single Sign-On

There are many scenarios for single sign-on using federation. The scenarios differ based on the location of the user account login being used for authentication, the location of the applications being accessed, and which party hosts the Federation server(s) that enable single sign-on.

In general, an organization will support multiple scenarios in order to support employee, partner, and customer access control to internal applications as well as employee access control to Cloud or partner applications. In this white paper, we discuss a successful approach to the top five most common SSO scenarios.

Scenario 1: Corporate Login to Cloud Application

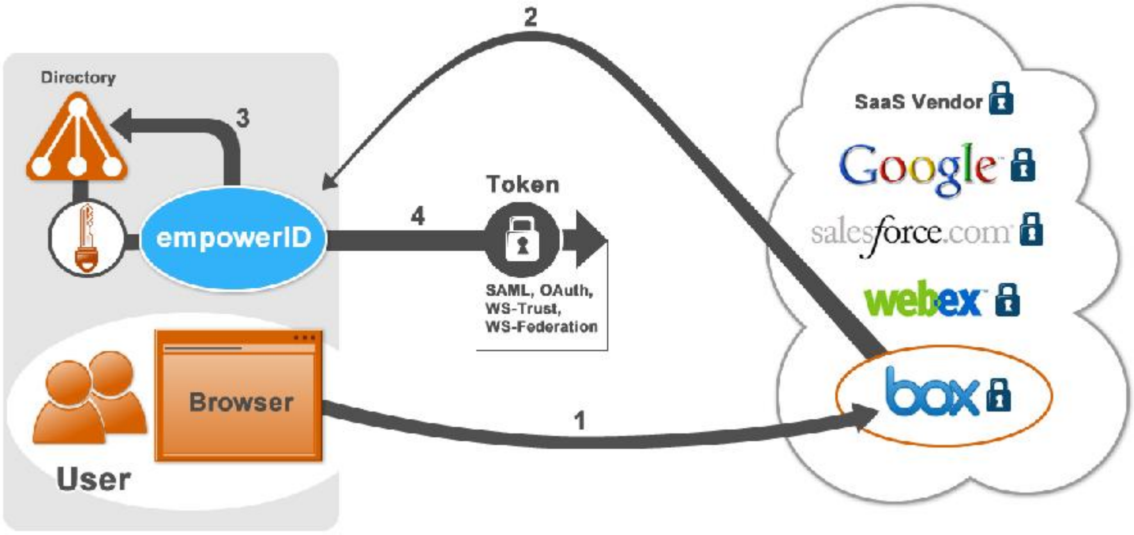

Figure 3. Corporate Login to Cloud Application

The Corporate Login to Cloud Applications single sign-on scenario is when a user logs in once using their corporate user credentials and then is able to access Cloud applications without being prompted again to authenticate. This is the most commonly supported SSO scenario in corporate IT organizations. A typical example is of a user logging in with their Active Directory credentials and then browsing to use a Cloud application like Salesforce.com without being asked to re-authenticate. In this scenario, the corporation hosts the Federation server that enables SSO with Cloud applications based on standard protocols like SAML or OAuth. Corporate Login to Cloud Application SSO has become so ubiquitous that virtually all SaaS providers support standards-based federated SSO.

Benefits of this approach:

- Users continue to use the same corporate login that they are familiar with and use for internal business applications
- No change is required to existing IT password reset procedures and tools
- Termination of access for corporate accounts results in immediate revocation of access to Cloud applications

Benefits of the EmpowerID SSO Manager module for this scenario:

- EmpowerID provides connectors and workflows to quickly and cost effectively provision application access in Cloud hosted or SaaS applications as part of the normal onboarding process
- EmpowerID maintains auditing and reporting of Cloud application login history as well as who has access to which Cloud applications
- The EmpowerID Login Workflow provides adaptive authentication security to consistently enforce strong authentication standards such as two-factor authentication and also device registration policies to control access from non-corporate devices

- EmpowerID's self-service and helpdesk password reset workflows decrease helpdesk costs to enable self-service for forgotten passwords and locked out accounts
- EmpowerID's virtual authentication directory technology supports user's logging in from multiple internal corporate directories including different directory technologies as well as multiple untrusted Active Directory domains

Scenario 2: Cloud Login to Internal Application

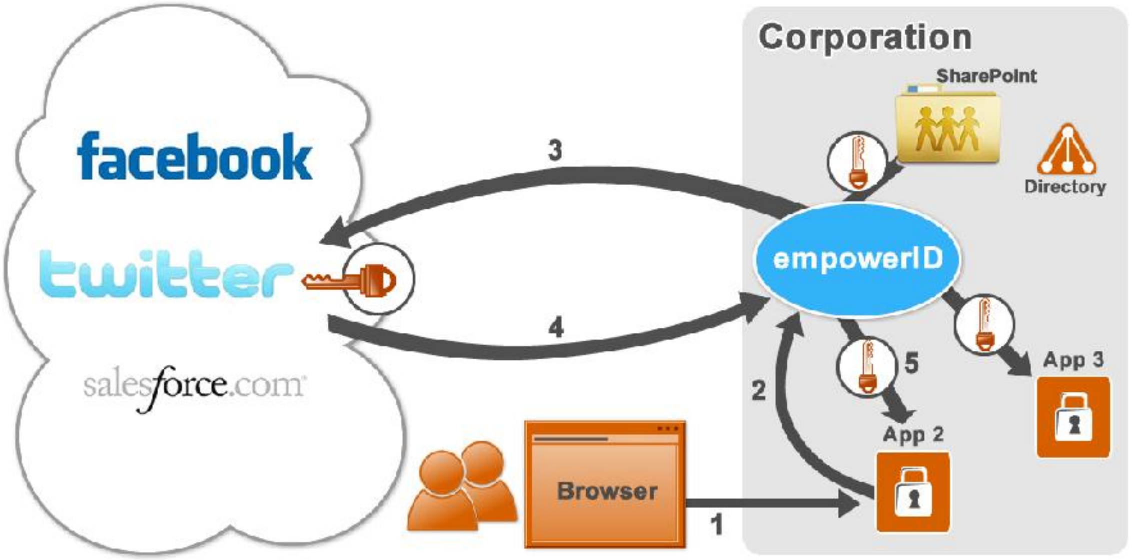

Figure 4. Cloud Login to Internal Application (SP Initiated)

The Cloud Login to Internal Application single sign-on scenario, also known as Social Media Login, is when an organization allows users to login to corporate application using their Cloud user credentials. Examples of commonly used Cloud Logins would be Facebook, Google, Windows Live, Yahoo, or Twitter. A typical scenario of this is a consumer logging into a corporate SharePoint web site with their Facebook account.

Cloud Login to Internal Application SSO is commonly supported when an organization wants to extend access for internal applications to consumers who are already accustomed to using their Cloud Logins to access sites on the Internet. A familiar, consumer-friendly model like this is easy to use and decreases support costs associated with a large consumer population.

Benefits of this approach:

- Increases revenues by decreasing the friction of the customer registration process
- Eliminates costs associated with forgotten passwords as users do not need to know another username and password

Benefits of EmpowerID for this scenario:

- EmpowerID Login workflow can perform just in time provisioning to internal directories as part of the login or registration process when required by internal applications being exposed to consumers
- The EmpowerID metadirectory can be used as a directory to store an internal version of a consumer account for use by internal applications that require an account for security
- EmpowerID is a Claims Provider for Microsoft SharePoint allowing EmpowerID metadirectory users and roles to be assigned permissions directly within the native SharePoint user interfaces.
- EmpowerID acts as a hub to maintain all single sign-on connections in one place for applications and identities, whether maintained internally, at partners, or in the Cloud
- EmpowerID supports all of the widely used standards for Cloud Identity Providers including OpenID and OAuth
- EmpowerID maintains auditing and reporting of Cloud Login history, recording who logged in and to which corporate applications they were granted access
- The EmpowerID Login Workflow provides adaptive authentication security to consistently enforce strong authentication standards such as two-factor authentication and it also provides device registration policies to control access from non-corporate devices

Scenario 3: Corporate Login to Internal Application

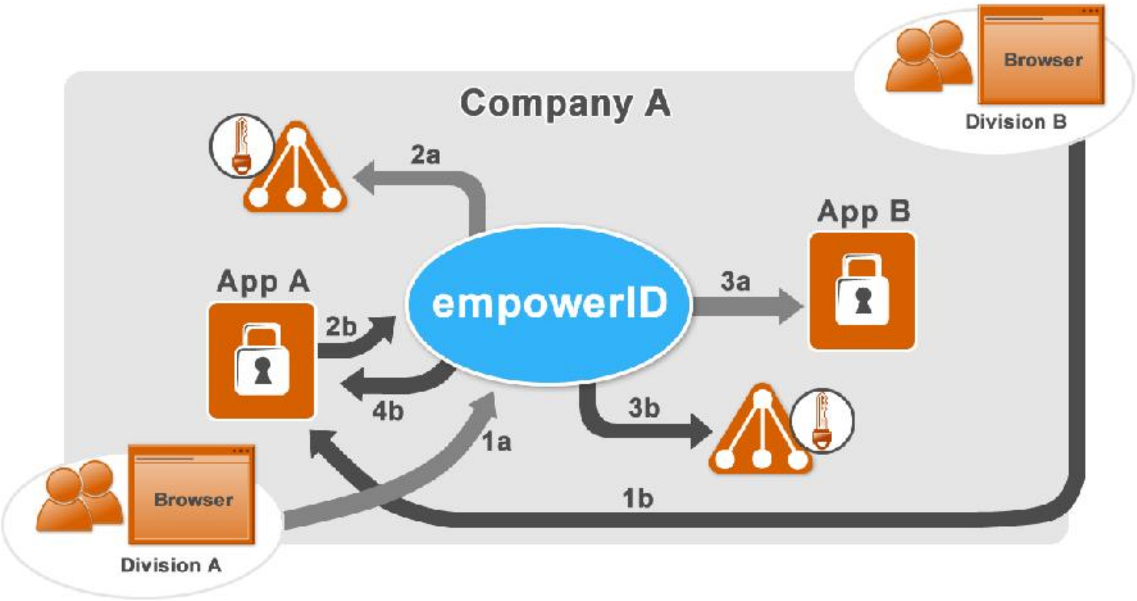

Figure 5. Corporate Login to Internal Application (a = SP Initiated, b = IdP Initiated)

The Corporate Login to Internal Corporate Application single sign-on scenario occurs when a user logs in once using their corporate user credentials and is then able to access any internal corporate applications without being prompted to re-authenticate.

An example of this is when a user logs in with their Active Directory account and then browses to an internally-hosted SharePoint site that is in a different, untrusted Active Directory Forest managed by a different division. This scenario is often required by organizations as they acquire other companies but cannot create trusts between their Active Directory domains due to legal limitations imposed by differing localities, time constraints or other internal policies.

Another example of this scenario is organizations that are developing new applications internally. Best practice security architecture is to decouple authentication/ authorization from within each application and to leverage centralized services for these functions. In this case, internal applications would be developed as "relying parties" that trust an internal corporate identity management system for authentication / authorization decisions.

Benefits of this approach:

- Users continue to use the same corporate login that they are familiar with and use for internal business applications
- No change is required to existing IT password reset procedures and tools
- Termination of access for corporate accounts results in immediate revocation of access to applications
- Internal application development can be standardized on a centrally maintained authentication and authorization system decreasing the cost of developing and managing security in multiple applications

Benefits of EmpowerID for this scenario:

- EmpowerID is a development platform supporting all major federated identity standards in use today including Security Assertion Markup Language (SAML), OpenID, OAuth, WS-Fed, and WS-Trust.
- EmpowerID is a full-feature identity management platform with over 375 workflows to manage provisioning and control of corporate identities and application access
- The EmpowerID Login Workflow provides adaptive authentication security to consistently enforce strong authentication standards such as two-factor authentication and also device registration policies to control access from non-corporate devices
- EmpowerID's federation is fully programmable in C# in Workflow Studio and offers access to all connected sources of information to use when making authorization decisions and generating claims for use by trusting systems.
- EmpowerID's self-service and helpdesk password reset workflows decrease helpdesk costs to enable self-service for forgotten passwords and locked out accounts

- EmpowerID's virtual authentication directory technology supports user's logging in from multiple internal corporate directories including different directory technologies as well as multiple untrusted Active Directory domains
- EmpowerID acts as a hub to maintain all single sign-on connections in one place for applications and identities maintained internally, at partners, and in the Cloud
- EmpowerID supports all of the widely used standards for Cloud Identity Providers including OpenID and OAuth
- EmpowerID maintains auditing and reporting of Cloud Login history – who has been logging in and which corporate applications were accessed
- The EmpowerID Login Workflow provides adaptive authentication security to consistently enforce strong authentication standards such as two-factor authentication and device registration policies to control access from non-corporate devices (an increasingly common scenario that organizations are under pressure to accommodate in order to expand access and usage – in fact, ubiquitous access is becoming a fundamental hallmark of the Cloud Computing paradigm shift)

Scenario 4: Corporate Login to Partner Application

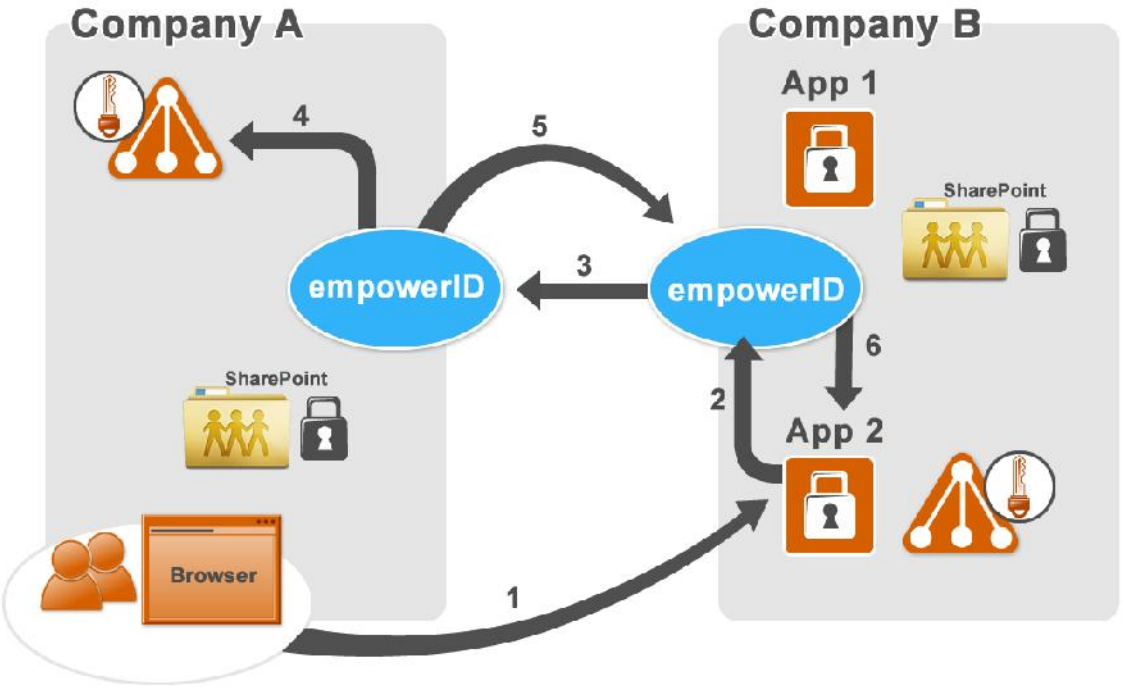

Figure 6. Corporate Login to Partner Application

The Corporate Login to Partner Application single sign-on scenario occurs when a user logs in once using their corporate user credentials and then is able to access any external corporate applications made available by an organization's business partners without being prompted again to authenticate. A typical example of this would be a user logging in with their Active Directory user account and then browsing to a partner organization's SharePoint site that is hosted and managed at the partner organization and linked into their corporate directory.

In this scenario, single sign-on is achieved by the creation of a federation trust between the federation servers at the user's organization and those at the partner organization. When the user attempts to access the partner's exposed application (e.g. SharePoint), the partner application redirects the user to the federation login screen on the partner organization federation server. The user would be presented with an option or tile to login with their corporate credentials, which when clicked would redirect them back to their corporate federation server for authentication. Upon authentication, the user's federation server would redirect them back to the partner federation server which then sends them into the application.

Benefits of this approach:

- Users continue to use the same corporate login that they are familiar with and use for internal business applications to access partner applications
- Terminations and access revocation is more accurate and timely as terminations are managed at the organization in which the user is employed
- Termination of access for corporate accounts results in immediate revocation of access to applications
- No change is required to existing IT password reset procedures and tools
- Internal application development can be standardized on a centrally maintained authentication and authorization system decreasing the cost to develop and manage security in multiple applications

Benefits of EmpowerID for this scenario:

- EmpowerID supports all of the widely used standards for Identity Federation, including the most common ones: SAML, WS-Trust, and WS-Federation
- The EmpowerID Login Workflow provides adaptive authentication security to consistently enforce strong authentication standards such as two-factor authentication and also device registration policies to control access from non-corporate devices
- EmpowerID's federation is fully programmable in C# in Workflow Studio and offers access to all connected sources of information to use when making authorization decisions and generating claims for use by trusting systems
- In addition to handling SSO for internal applications, EmpowerID can automate the granting and revoking of application access as well as auditing and attestation of access grants
- EmpowerID acts as a hub to maintain all single sign-on connections in one place for applications and identities maintained internally, at partners, and in the Cloud
- EmpowerID maintains auditing and reporting of Partner Login history, recording who has logged in and to which corporate applications access was granted

Scenario 5: Identity as a Service (IdaaS) Hub

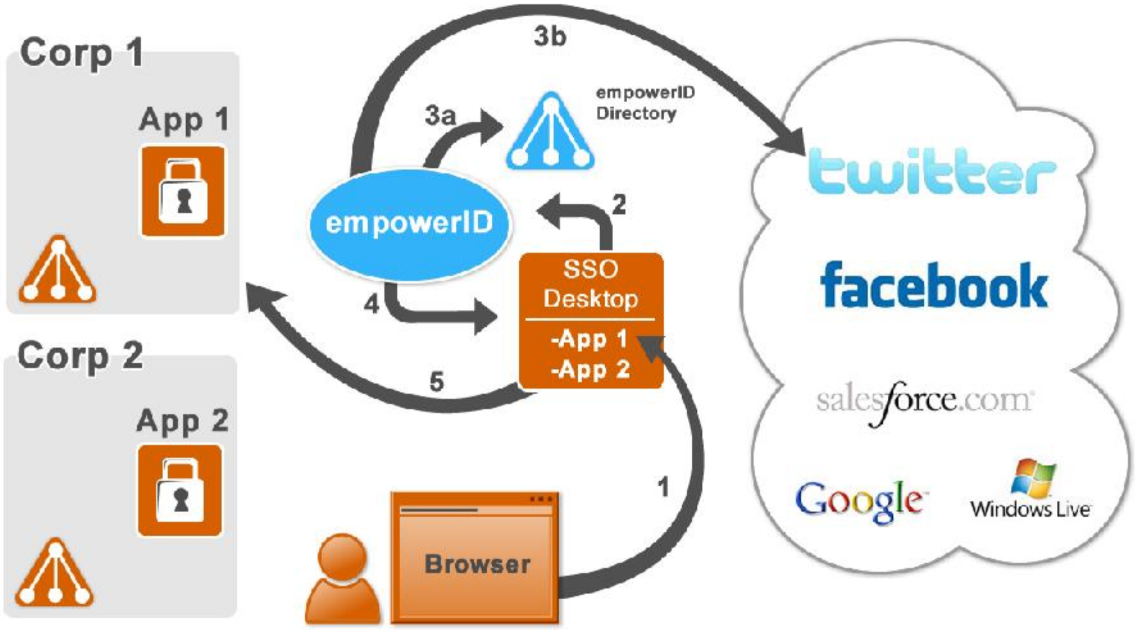

Figure 7. Identity as a Service (IdaaS) Hub

In this scenario, users log in with an identity maintained by a Cloud Identity as a Service (IdaaS) Provider and can then access multiple Cloud hosted SaaS applications or corporate hosted partner applications without being prompted to re-authenticate. Typically, the IdaaS provider will maintain processes to support registration, delegated administration, and a user interface for end users to see links they may click on to login via IdP initiated SSO to access partner or affiliate Service Provider applications.

In the IdaaS Hub scenario, a group of organizations agree to leverage a shared Identity Provider service in order to facilitate application sharing between them. A central shared Identity Provider functions as a hub of authentication, allowing federation trusts to be established with all major Identity Providers using industry-standard protocols like SAML, WS-Federation, WS-Trust, OpenID, and OAuth. This trust relationship simplifies the creation and maintenance of federation trusts by allowing an organization to only configure their applications to trust one Identity Provider. Smaller member organizations can configure their Service Provider applications to directly trust the IdaaS system, while larger organizations with an in-house federation system can configure it to broker the trust with the IdaaS federation services. Federation connections only need to be made once between partner systems and the central Identity as a Service (IdaaS) federation provider, with new services becoming immediately available to all subscribers of the service.

This is a much more cost effective solution when there are a large number of organizations that require federation and that utilize a common set of applications, preventing the exponential increase in costs as the number of federation partnerships increases. These cost savings create strong incentives for organizations to provide these shared Identity Service partnerships. This scenario is more common in specific industries such as healthcare where hospitals and doctor's practices partner with insurance companies and health care plans.

Benefits of this approach:

- Dramatically decreases costs as organizations only trust the hub and are not required to maintain connections on a point to point basis
- Lower legal costs for authorizing federation trusts due to only requiring a trust relationship with one organization
- Easier for end users because one interface displays all of their available applications

Benefits of EmpowerID for this scenario:

- The EmpowerID metadirectory can be used as a Cloud Directory avoiding the cost of creating an extranet directory or the security risk of adding users to an internal directory
- EmpowerID acts as a hub to maintain all single sign-on connections in one place for applications and identities maintained internally, at partners, and in the Cloud
- EmpowerID supports the widest variety of protocols to support connecting with Cloud and corporate systems including SAML, WS-Trust, WS-Federation, OAuth, and OpenID
- EmpowerID provides a rich development environment supporting the creation of custom system connectors for inventory and SSO
- EmpowerID maintains auditing and reporting of Cloud login history including who has been logging in and to which corporate applications access was granted
- The EmpowerID Login Workflow provides adaptive authentication security to consistently enforce strong authentication standards such as two-factor authentication and it also provides device registration policies to control access from non-corporate devices

The EmpowerID SSO Platform

EmpowerID is an Identity Management and Cloud security platform that provides a unique and powerful solution for the top 5 scenarios for Federated Single Sign-On.

Key Features of the EmpowerID Federated SSO Platform:

Broad Standards Support

The EmpowerID Federation platform that supports all of the standard single sign-on protocols including SAML, OpenID, WS-Trust, WS-Federation, and OAuth. In addition to protocol support, EmpowerID provides out of the box integration with a large number of Internet and Corporate Identity Providers including Active Directory, LDAP, Facebook, OpenID, Twitter, SalesForce.com, Google, and Yahoo among others.

Login Workflow

EmpowerID is an identity management and provisioning platform in addition to providing federated SSO. The EmpowerID login workflow supports the automatic provisioning of user accounts in Active Directory, LDAP, database, or any system at the Service Provider during the user's first SSO login. The Login workflow is infinitely configurable and can be visually designed to accommodate any onboarding or registration scenario.

Adaptive authentication policies in the login workflow can demand stronger "step up" authentication based on what credentials and Service Provider application to which a user is attempting to Single-Sign On. For example, an employee using AD credentials to SSO into Google apps might only need their password and username to gain access but the same employee may browse to SSO into Salesforce.com and require a second factor authentication to sensitive customer information. With adaptive authentication, the user's AD credentials would be "stepped up" to conform to the authorization policy for the resource being accessed.

Also as part of the adaptive authentication model, EmpowerID can enforce policies based on IP address or the device being used for access. Device registration allows an enterprise to force users attempting to login from an unrecognized device (iPad, Laptop, Smartphone, etc.) to prove and verify the device type.

EmpowerID typically handles this with a one-time password sent via email that allows the user to prove ownership and control of the device.

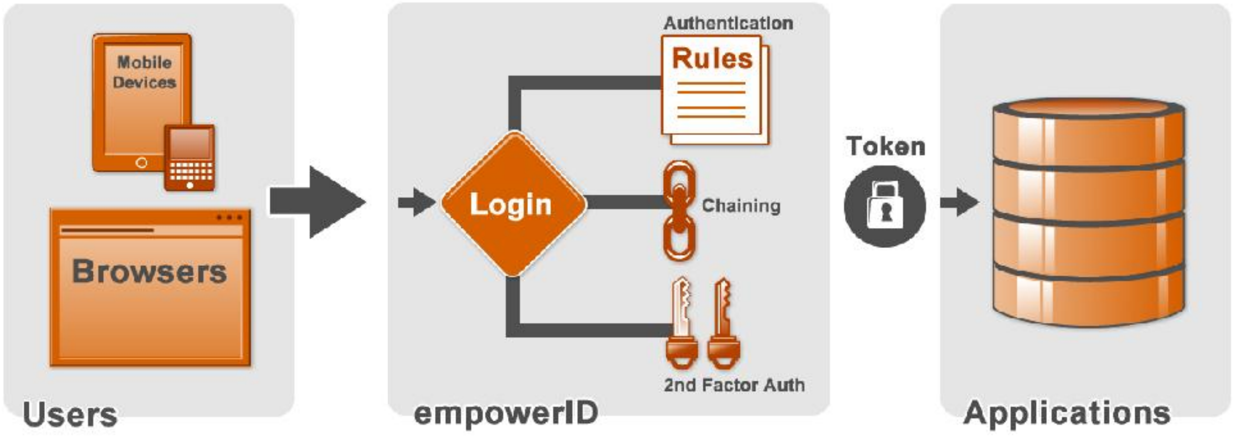

Figure 8. EmpowerID Login Workflow

Cloud Metadirectory/ Extranet Directory

EmpowerID also provides its own "Cloud Metadirectory" or extranet directory for Service Providers to use for authentication so that another directory is not required. The EmpowerID metadirectory provides built in support via workflows for delegated administration, self-provisioning, password management, information self-service, access requests, and more.

Federated Application Development Environment

A unique feature of the EmpowerID Federation platform is its extensive programmability. EmpowerID Workflow Studio provides wizards and code editors for easily creating complex SAML and WS-Federation claims extensions that can be used by applications for authorization. As an example, EmpowerID claims extensions allow information from any enterprise system to be used for assigning role-based permissions with Microsoft SharePoint 2010.

EmpowerID is fully programmable allowing custom Federation Extensions to be created in the Workflow Studio C# development environment. EmpowerID also supports application developers that wish to externalize application security into a central system utilizing flexible Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) authorization. EmpowerID enables developers to maintain application security outside of their application, minimizing security risks and the need to write application security code into each new application.

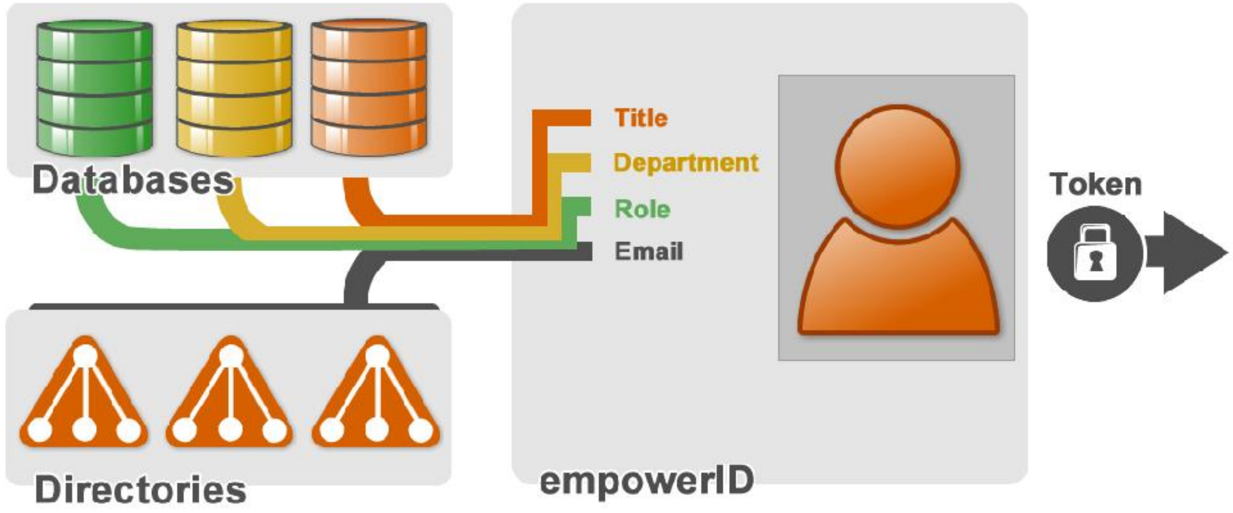

Figure 9. Attribute aggregation for Claims from multiple authoritative stores

SSO and Role-Based Security for Microsoft SharePoint

EmpowerID acts as a SharePoint Claims Provider (IdP) and Claims Augmentation Provider to enabled Role-Based and Attribute-Based Access Control (RBAC and ABAC). As a SharePoint Claims Provider, users are redirected to the EmpowerID federated log-in page when logging into SharePoint. EmpowerID acts as an authentication hub allowing federation trusts to be established between EmpowerID and other major Identity Providers using industry-standard protocols like SAML, WS-Federation, OpenID, and OAuth. Organizations can allow users to login to SharePoint using their username and password from any trusted system such as Active Directory, Google, Facebook, Windows Live, among others while adding on more stringent security controls such as enforcing device registration and second-factor authentication.

EmpowerID's powerful hybrid RBAC and ABAC model can be used directly inside SharePoint's People Picker user interface to grant access to sites, lists, documents, etc. The People Picker allows end-users to search and select any EmpowerID security object such as People, Groups, Roles and dynamic collections just as they would normally search for users or groups. The dynamic nature of these roles can dramatically reduce the administrative burden of manually setting security assignments and automates access granting and revocation based on changes in user's job status, function or location.

Key Benefits of Federated SSO with EmpowerID:

- Reduces the cost of password management – users are required to only remember one set of credentials
- Strengthens security and reduces the risk of a breach by providing a single centralized authentication point for applying stronger policies
- Creates new revenue opportunities allowing partners and customers to securely sign-up and access corporate resources
- Frees constrained technical resources from unneeded direct participation in granting access by securely delegating to users and privileged staff rights based on their roles or directly assigned privileges
- Speeds deployment by shipping with over 25 ready-to-use workflows for SSO

EmpowerID provides the most flexible and secure solution to reducing the costs of password management by enabling secure Federated SSO between organizations and the Cloud.

About The Dot Net Factory

The Dot Net Factory creates EmpowerID, the only Identity Management and Cloud Security product built entirely on a Business Process Automation platform. Empower ID ships with 375+ ready-to-use workflows that can be customized, extended, or used as templates to create new processes. EmpowerID minimizes risk, cuts costs, and reduces downtime by securing enterprise systems, streamlining access control and identity management processes.

Readers interested in learning more: please visit The Dot Net Factory "Learning Library" for a range of information about Federation Services, SAML, other standards and more at www.TheDotNetFactory.com