



myOneLogin On-Demand Identity Services for Web Applications

Enhancing your web application with federation, single sign-on and strong authentication

Contents

| | |
|--|----------|
| The Need for Identity Services | 1 |
| myOneLogin On-Demand Identity Services | 1 |
| Single Sign-On (SSO) and Becoming a Federation Consumer | 2 |
| Federation as a Service: Implementing a Federation Hub | 4 |
| myOneLogin Strong Authentication | 5 |
| Directory Integration Options | 6 |
| The myOneLogin Developer Community | 8 |
| myOneLogin Service Platform..... | 8 |

The Need for Identity Services

In today's highly networked world, web-based applications are critically important to businesses of all types. Web-based applications play vital roles in today's business: building and sustaining user communities, differentiating your company's services, and providing efficient application access for virtual employee and partner communities.

This increase in application importance and visibility puts new demands on web application developers. Once it was once enough to focus on the function and user interface of the application. Today, web developers need to be concerned with other issues as well, including:

- User authentication
- Access security
- Federation with partners for single sign-on across businesses

These identity services traditionally are managed by heavyweight solutions that reside within the enterprise. But legacy identity solutions are limited in their ability to address today's environment, where you need to integrate with partners on the fly and launch new applications as quickly as possible. And most legacy solutions require significant expertise and training on the part of the web developer.

Through the myOneLogin service, TriCipher offers essential identity services—federation, single sign-on, and strong authentication—as on-demand web services that application developers can access using basic web services calls. Using these services, developers can quickly and easily:

- Implement single sign-on across multiple applications
- Deploy standards-based federation to provide single sign-on and easier integration with partner and third-party applications
- Strengthen application access with multi-factor authentication

This paper provides a brief overview of the myOneLogin services available from TriCipher for web application developers.

myOneLogin On-Demand Identity Services

The myOneLogin On-Demand Identity Services offer simple, web-based access to advanced identity services, for rapid and low-cost integration with web-based applications.

Depending on your application needs, you can use the myOneLogin services to provide any combination of:

- Standards-based federation
- Single sign-on
- Strong authentication

These services, hosted by TriCipher within the myOneLogin service, can be integrated within applications in a matter of days, providing a rapid time-to-market. Implemented as web

services, they are platform independent. Flexible integration options give you control over where directory information and authentication takes place, and how the services are integrated within your user interface. For example:

- You can choose to have users remain entirely within your site and handle all integration through web services calls behind the scenes.
- You can take advantage of the myOneLogin user interface, but customize it with your style sheets. The user interface includes self-provisioning capabilities for users and a robust administrative interface.
- You can simply refer customers to myOneLogin without any customization or integration at all, becoming a TriCipher business partner. TriCipher will share revenues based on the number of users who subscribe to myOneLogin from your service.

For businesses and web publishers interested in the first two options, myOneLogin offers a Developer's Community, complete with sample code and a test domain. The rest of this paper describes these on-demand services and options for integration in your application.

Single Sign-On (SSO) and Becoming a Federation Consumer

If you offer many web applications on your site, you may want to give your users the option to log on only once to access their authorized applications. You can do this with myOneLogin, creating a single sign-in to your applications while retaining control over who can access which applications.

Federation extends the concept of single sign-on across different organizations, with no single source for authentication. Using federation, you can establish 'trust relationships' with partners, allowing users to authenticate only once, while maintaining control over who accesses your application(s) through your internal directories.

The Security Assertion Markup Language (SAML) is a SOAP/XML standard for implementing federation, and is gaining adoption across major web applications, including Google Apps and others. But for developers, adding SAML support to an application is a significant effort, requiring SAML expertise and toolkits. Using traditional methods to implement SAML adds cost and delay to application deployment.

Even you only need to implement single sign-on across your own applications, we recommend that you do so using SAML federation. Once a user has authenticated with myOneLogin, sign-on across the various applications will occur using SAML assertions rather than sending user names and passwords.

myOneLogin gives web application developers the ability to provide standards-based SSO across their own and partner properties using SAML federation.

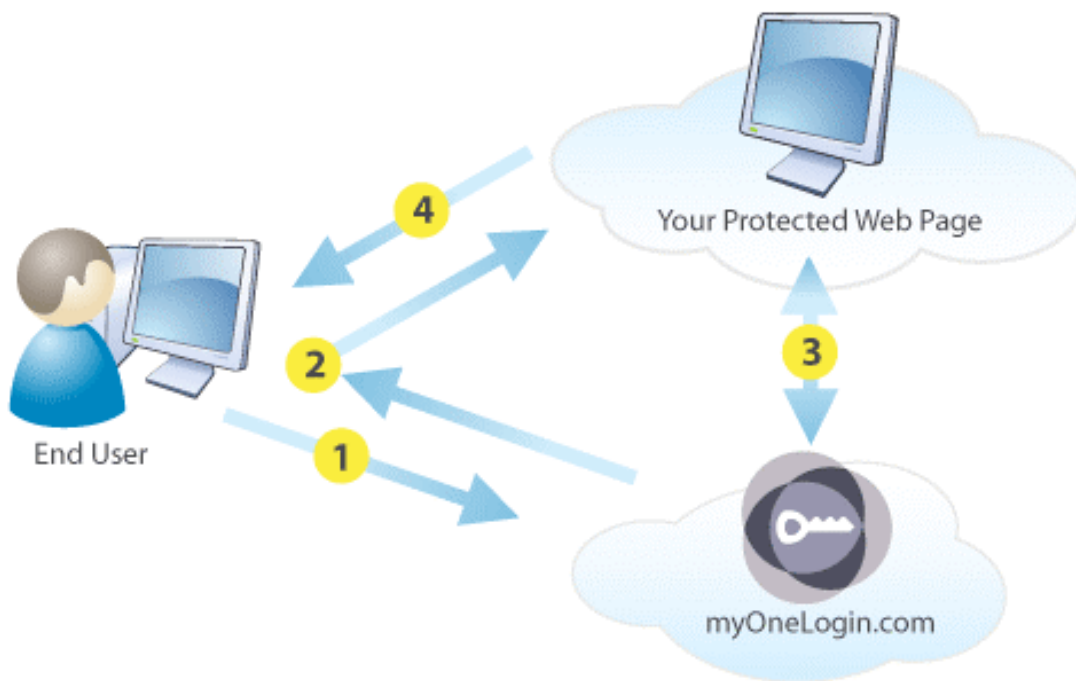
- If your application already supports federation standards (SAML, WS-Federation or ADFS), myOneLogin will support it; you can use myOneLogin to establish SSO across multiple applications.

- If your application does not yet support federation, you can implement it quickly and easily using the myOneLogin Federation Consumer service.

The myOneLogin Federation Consumer Service supports a rapid deployment of SAML using basic web services calls. If your application receives a SAML assertion (from myOneLogin or another application), you can send a standard web services query to the myOneLogin service, which will either confirm or deny the identity.

Using the consumer service gives you a simple, platform-independent way to implement federation in your application, without major application rewrites.

The following diagram depicts one of the options for implementing federation services within your application. In this example, the myOneLogin service manages the user credentials. Other directory configuration options are described in a following section.



1. The user accesses a myOneLogin page requesting your protected web page. (This access may be a redirect from your application, or a customized link you provide that looks and feels like your login page.)
2. The myOneLogin service generates a SAML assertion and redirects the user's browser to your protected web page, along with the assertion.
3. Your web page receives the SAML assertion and initiates a web services call to the myOneLogin consumer service to validate it.
4. If validation is successful, the session can proceed.

In looking at this simple use case, remember that you have many options for integrating myOneLogin to provide federation and SSO in your application environment.

- *Directory options:* The myOneLogin service can maintain the user directory. In this case, user authentication occurs entirely within myOneLogin, whether or not you are using strong authentication as described in the next section. Or you can have myOneLogin validate the second factor and pass the request for directory validation to your internal directories. See the section *Directory Integration Options* for more details.
- *User Interface:* You can make use of the myOneLogin user interface for user setup and login, customized with your own style sheets to match the look and feel of your application. Or you can make calls to the myOneLogin service from within your existing user interface.

You can combine the federation and single sign-on capabilities with strong authentication for those applications that require it.

Federation as a Service: Implementing a Federation Hub

myOneLogin Federate lets you create an easy-to-use, fully functional federation hub that:

- Produces federation assertions for connecting users to web-based applications
- Consumes assertions (validating identities) from enterprise portals or partners
- Manages trust relationships and applies them automatically
- Transforms federation assertions between versions and standards

The myOneLogin service acts as a federation ‘hub’ for your business, connecting you seamlessly with applications and partners. For example, your application can generate SAML 1.1 assertions, yet work with a partner’s application that uses WS-Federation.

Contact myOneLogin if you are interested in evaluating this service.

You can use myOneLogin Federate to connect users from your enterprise portal to web-based applications, enabling single sign-on across web-based as well as internal applications. In this case, the myOneLogin service is completely transparent to the user.

Or, you can use this service to enable or participate in sites aggregating applications from multiple partners. You can automatically give trusted partners the ability to authenticate and connect users to your applications, and use myOneLogin Federation Services to connect your users to partner applications.

myOneLogin Federate offers a web-based interface for managing the trust relationships between federation providers and partners.

| | demo.myonelogin.com | beaportal2 | orgidpprod |
|--------------------------|---------------------|------------|------------|
| green_xentra_net_2008082 | ✓ | ✓ | ✓ |
| JuniperRP | ✓ | ✓ | ✓ |
| JuniperSSLVPN | ✓ | ✓ | ✓ |
| SalesForce | ✓ | ✓ | ✓ |
| SalesForceNativeSAML | ✓ | ✓ | ✓ |
| SalesForceQA | ✓ | ✓ | ✓ |
| SalesForceTest | ✓ | ✗ | ✓ |
| WebEx | ✓ | ✓ | ✓ |
| WebExRP | ✓ | ✓ | ✓ |

[Submit](#)

[Manage Federation](#)
[Back to myOneLogin Portal](#)

Using this interface, you can map applications to federation providers. For example, users connecting from your enterprise portal should be able to get federated single sign-on to all of your applications, while those requests coming from a distributor partner should only be able to access the applications you make available to partners. You can create these highly granular trust relationships using a simple web-based interface.

myOneLogin Strong Authentication

Passwords alone are insufficient protection for many applications that contain sensitive data. Passwords can be compromised by phishing attacks or discovered by keystroke loggers. Man-in-the-middle attacks may intercept passwords and hijack accounts. And a surprisingly high number of users simply tell their passwords when asked, or use the same simple password across insecure accounts and those hosting valuable information. Whenever one of your users experiences a password breach, it reflects badly on your application, regardless of the cause.

With myOneLogin Identity Services, you can add strong authentication to your application with minimal effort and expense, and without the difficulties of distributing and managing token devices to your users.

myOneLogin uses TriCipher's unified authentication technology, which offers patented multi-factor authentication using a variety of methods. myOneLogin Strong Authentication currently supports the following authentication methods:


- Encrypted browser cookies
- Browser certificates (X.509 digital certificate)

One part of the credential resides on the user's computer, the other part securely in the myOneLogin service. Both parts are necessary for authentication. However, the secondary

factor verification is completely transparent to the user. From the user's perspective, the experience of authenticating is as simple as providing a user ID and password.

developer **myOneLogin**
Armored by TriCipher

Enter Password



Welcome, Anne

Your confidence image and welcome message, which you created when you first signed up, should be displayed above. If the image and message are correct, please enter your password to sign in. **Remember, never type your password if the image and message are not correct.**

Password:

[Submit](#) [Sign In Again](#)

COPYRIGHT © 2008 TRICIPHER. ALL RIGHTS RESERVED. [Get Support](#) [Privacy Policy](#)

The password page can include a personalized confidence image and message

A user connecting from another device without the secondary factor (something other than their usual desktop or notebook) can gain a one-time authorization by answering personalized security questions selected during the self-provisioning process, and having a security key sent to a phone number registered for that account.

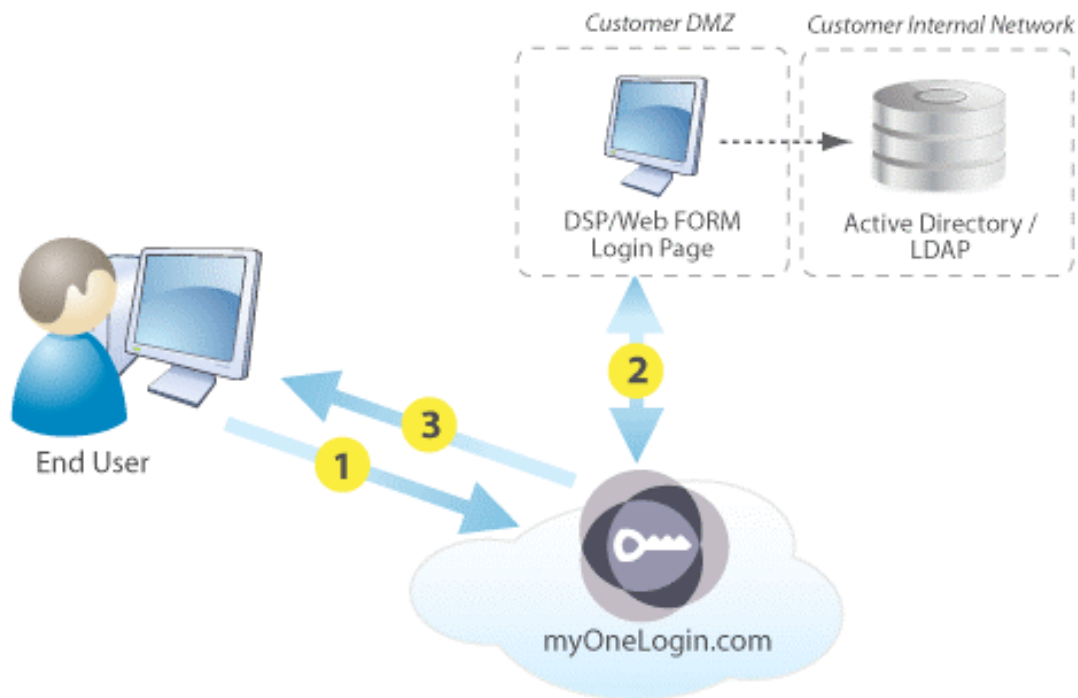
Again, as you implement strong authentication you can choose how to integrate your directory information. myOneLogin can access your Active Directory or LDAP directory to authenticate the user's password, while validating the secondary authentication factor on the myOneLogin service. Or, the myOneLogin service can maintain the user directory information and validate both factors. The options are described in more detail in the next section.

Directory Integration Options

For some applications, you may want myOneLogin to maintain the directory of users. If, for example, you are publishing a web application for a large number of customers and do not have an existing directory of users you need to validate, it may be simplest to let the myOneLogin service maintain the user directory as users self-enroll. You can send a batch file to speed the process of provisioning existing users.

If you want to maintain the user directory internally, there are several ways to build the integration between the myOneLogin service and your LDAP, Active Directory or database.

All use the same overall flow. The second factor is always validated within the myOneLogin service, while the password can be validated against an internal directory or database.



1. The user connects to myOneLogin with a username and password. If the user does not yet have a second factor, they are prompted to enter a password. If the user is already registered with myOneLogin, myOneLogin validates the second factor before prompting the user for a password.
2. myOneLogin performs a back channel validation of the username and password against the internal directory or database using one of the methods described below.
3. myOneLogin authenticates the user. If the user is registering for the first time, they receive a second factor at this point.

Both of the following approaches enforce secure communications between myOneLogin and the internal directories. User passwords are not stored in myOneLogin, but are simply validated against the internal user store. A password change to Active Directory or LDAP is automatically enforced when myOneLogin checks the directory. And if you remove users from internal directories, user access to myOneLogin is automatically removed.

FORM login

The simplest approach to integrating with an internal directory or database is to use a Web FORM login page, hosted on a web server in the DMZ.

myOneLogin communicates with the FORM page using SSL (HTTPS). If you are using strong authentication, myOneLogin validates the second authentication factor (browser cookie or certificate) before passing the user credential to the FORM page.

You write the FORM page; TriCipher can provide sample code. The FORM page validates the credentials passed from myOneLogin against the internal directory or database.

You can add checks to the FORM page to verify that the caller's IP address is that of the myOneLogin service. This will prevent users from circumventing second-factor authentication if you require it. The FORM page can also return user attributes that myOneLogin can pass to other relying applications (such as SAML federation attributes).

Directory Services Proxy

TriCipher can provide you with the TriCipher Directory Services Proxy (DSP), a lightweight Java application that runs in your DMZ and communicates with the myOneLogin service to verify passwords against your LDAP or AD directory. The DSP requires a web application server like Tomcat.

All communication between the DSP and myOneLogin uses SSL (HTTPS). The DSP communicates with Active Directory using LDAP over SSL, so the user information is never exposed on the network. The DSP verifies the myOneLogin IP address before communicating with the myOneLogin servers.

The myOneLogin Developer Community

If you are interested in using the myOneLogin identity services within your application, you should register for the myOneLogin Developer Community. (Visit www.myonelogin.com/developers and select the Sign Up option.)

The Developer Community is itself hosted within a myOneLogin domain, so as you enroll you can see the various processes used to implement federation and strong authentication. There is no cost to register.

From the community, you can access

- Online documentation
- Source code samples
- Forums and blogs
- Test environment for SAML validation

myOneLogin Service Platform

The myOneLogin service uses the TriCipher Armored Credential System (TACS), a unified authentication infrastructure that uses patented multi-part credentials while maintaining the familiar experience of entering a user name and password.

The myOneLogin service uses the TriCipher ID Vault appliance, a FIPS 140-2 Level 2 rated appliance that securely manages user information and authenticates users as part of the TACS. An Authentication Gateway acts as the services layer.

myOneLogin provides end-to-end security from the user's browser all the way to the back-end data encrypted and stored in myOneLogin. The service is hosted in a third-party SAS 70 Type II-certified data center that employs advanced security and protection technologies and meets high industry standards, including:

- SAS 70 Type II compliance
- HIPAA and PCI DSS compliance
- Physical and network security measures
- Full redundancy

All data is encrypted in transit and in storage

The service uses a secure, multi-tenant architecture in which you will have your own, dedicated domain with complete data isolation. Role-based access control gives you granular control over administrative access to the system.

Summary

Using myOneLogin Identity Services, you get the advantages of strong, flexible multi-factor authentication and SAML-based federation, without having to develop that expertise in-house or delay the time-to-market for your application. You can integrate the service within your application, so the look and feel remains consistent for the user. And you can deploy the solution almost instantly, for a rapid time-to-market.

About myOneLogin and TriCipher

MyOneLogin is a service provided by TriCipher, the experts in strong authentication technologies. myOneLogin uses the TriCipher Armored Credential System, a flexible, scalable authentication infrastructure proven in demanding financial services environments.

For more information, contact sales@myonelogin.com.

TriCipher Headquarters:

750 University Avenue, Suite 260
Los Gatos, CA 95032
Phone: +1.650.372.1300
Fax: +1.650.376.8301

TriCipher Worldwide Sales:

Email: sales@tricipher.com
Phone: +1.650.376.8326
Fax: +1.650.376.8301

Copyright © 2008 TriCipher, Inc. The information in this document is subject to change without notice. TriCipher and myOneLogin are either registered trademarks or trademarks of TriCipher, Inc. All other business and product names mentioned are the property of their respective owners.