

White Paper
Intel Information Technology
Computer Manufacturing
Security

Improving Security and Productivity through Federation and Single Sign-on

Intel IT has developed a strategy and process for providing seamless user access to externally hosted applications. Single sign-on (SSO) enables centralized storage of sensitive user profile information through the use of standards-based identity federation, and this information remains under Intel's sole control. Users appreciate that a single password allows them access to both internal and external Web sites. This type of enhanced data security is especially important for closed communities, as it helps ensure customer privacy and Web security for all external Web sites. SSO also reduces maintenance costs and increases productivity, because there is no need to update user ID information in multiple places.

Brandon Wiens and Ajaya Agarwal, Intel Corporation

January 2009

IT@Intel

The Channel Community has given us the ability to engage with our customer more frequently and more intimately. Inevitably these community engagements lead to stronger relationships and, ultimately, more sales. And to that end, the single sign-on project has greatly helped in making the community logon process totally seamless.

—Scott B. Palmer
Senior Web Strategist
Intel Corporation

Executive Summary

Intel IT developed a single sign-on (SSO) strategy and process that provides seamless user access to both internally and externally hosted applications, improving the security of sensitive user profile information, reducing maintenance and costs, and simplifying the user experience. Through the use of standards-based identity federation, our SSO solution allows us to store and maintain confidential user authentication information in a single location. Additionally, we can integrate outsourced applications into the user's environment so that all applications, both external and internal, appear as one homogenous entity. Internal and external users can access multiple applications with a single logon.

In order to provide the most flexible, cost-effective solution, we carefully researched what our customers needed before we began implementation, defining trust models, use cases, and high-level requirements. Our implementation of SSO uses Security Assertion Markup Language (SAML), a security markup language standard based on Extensible Markup Language (XML). We tested our SSO strategy and process through a limited proof of concept (PoC) with our Americas Sales and Marketing Organization social media Web site, also known as Channel Voice.

Our SSO strategy provides numerous benefits, including:

- **Improved security of sensitive user profile information.** User data is stored in one place and is maintained by Intel.
- **Reduced maintenance costs and increased IT productivity.** There is no need to update user ID information in multiple places.
- **Enhanced user experience.** Users do not have to remember and enter multiple user IDs and passwords.
- **Added value for Intel's network of partners.** An Intel-provided SSO service simplifies access for all users, internal and external.

Based on our initial success with identity federation and SSO, we plan to expand the solution in several directions, including rolling it out to other groups at Intel.

Contents

Executive Summary	2
Business Challenge	4
Solution	5
Developing a Single Sign-on Process.....	5
Expected Benefits.....	9
Next Steps.....	10
Conclusion	10
Authors	11
Acronyms	11

Business Challenge

With the growth in social media and externally hosted services, people often log on to multiple Web sites in the course of their daily work. Each site requires a user name and password, creating a burdensome list of logon credentials users must track—often leading to password fatigue.

For example, one way for the Intel Web marketing team to better connect to members of the Intel® Channel Partner Program on the Intel Reseller Center Web site was to use Web 2.0 technologies, such as a social media application, within the Intel Reseller Community. This presented a challenge, however, because the social media application was hosted on an external site. To access this site, community members were tasked with multiple logon procedures, user IDs, and passwords.

In addition, user authentication information had to be maintained on multiple servers, which posed data maintenance problems:

- Storing and maintaining duplicate copies of user information is imprecise and wasteful.

- Account clean-up after worker status changes is hard to enforce, especially for delegated administrators.
- Keeping unnecessary, sensitive information records on external servers—especially personal or credit data—is risky.
- Off-network access to outsourced or enterprise applications requires resource-intensive virtual private network (VPN) connections.

Figure 1 illustrates the multiple logon model.

To simplify users' logon routines and data maintenance, Intel IT developed a single sign-on (SSO) strategy and process to help improve communication and collaboration between the Intel Web marketing team and members of the Intel® Channel Partner Program.

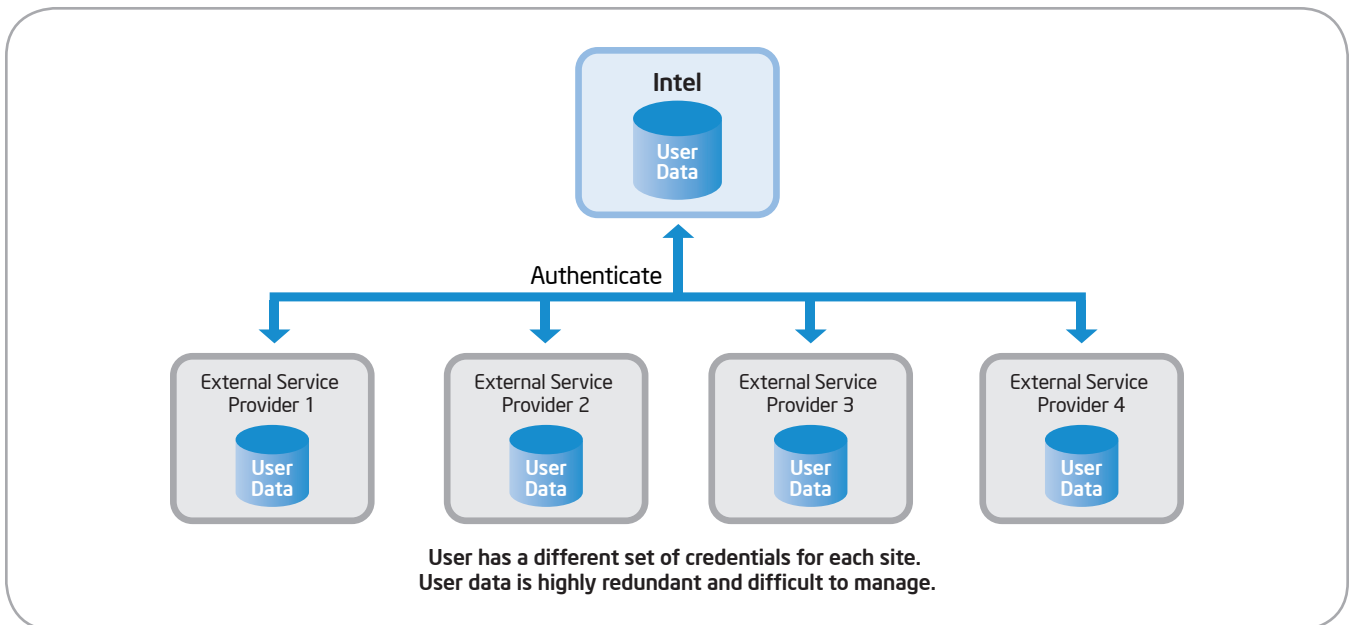


Figure 1. The multiple sign-on approach has many problems.

Solution

We created a centralized identity management solution using Security Assertion Markup Language (SAML)-based identity federation to implement an SSO strategy. SSO allows users to connect to multiple applications across an environment using a single logon identity. Federation standards extend the SSO solution to external sites, giving users the ability to logon to internal and external sites using one user identity.

Our SSO strategy allows us to store and maintain confidential user authentication information in a single location, known as the identity provider (IDP). A third-party Web site, the service provider (SP), requests a user's credentials from the IDP and then, based on the authentication and authorization results, serves the appropriate service, application, or information.

SSO has allowed us to integrate outsourced applications into the user's environment so that all applications, both external and internal, appear as one homogenous entity. Users, both internal and external, can access multiple applications with a single logon. They don't need to remember multiple passwords, and their sensitive user profile information remains in one secure place rather

than on a number of servers. Figure 2 diagrams how the SSO process works.

Developing a Single Sign-on Process

In 2006, Intel IT set up the initial environment for external and internal customers to access outsourced applications. We then began to research which tools to use for user authentication, authorization, and profile management. Once we had the tools in place, we tested them in a limited proof of concept (PoC) environment—more than 250 users in the Americas Sales and Marketing Organization—before rolling out the solution to the entire user community.

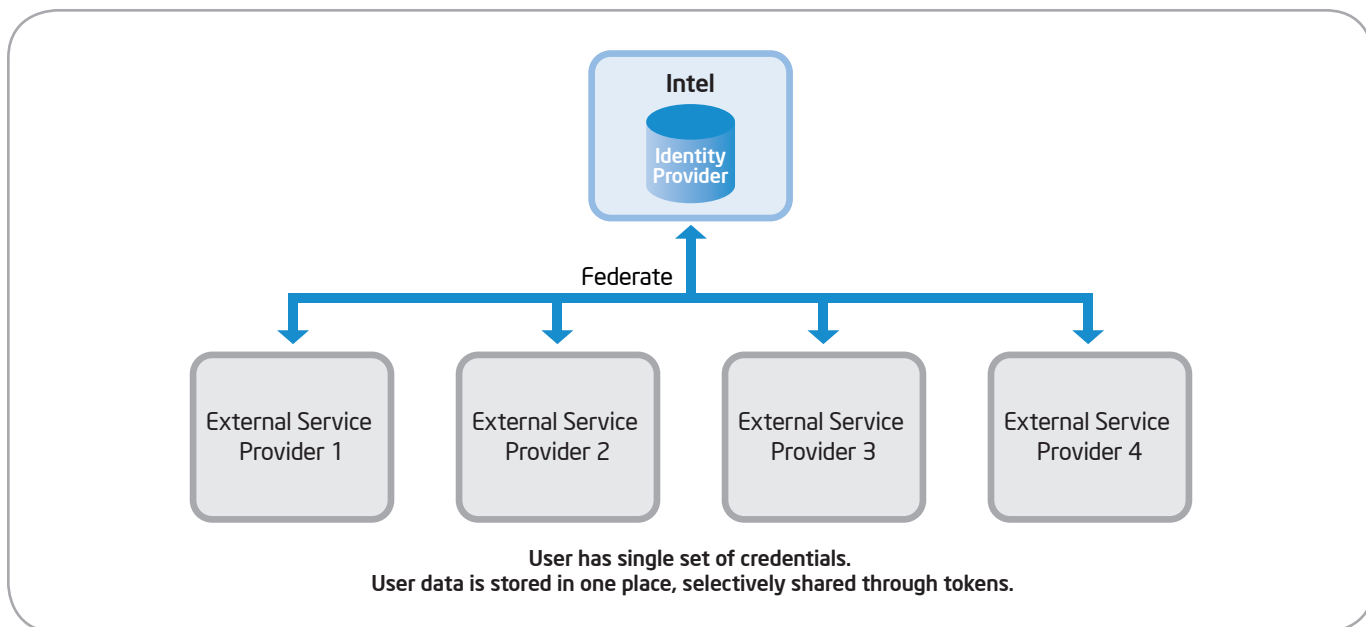


Figure 2. Federation and single sign-on enable seamless, secure access to service providers.

Table 1. Trust Models and Use Cases

Trust Models	Use Cases
1. Intel as the worker identity hub. In this case, the Intel intranet serves as the identity provider (IDP).	<ul style="list-style-type: none"> ▪ Employee is logged on to the Intel network and accesses an enterprise application. ▪ Employee is logged on to the Intel network and accesses an outsourced service provider (SP). ▪ Employee is outside the Intel network and accesses an outsourced SP.
2. Intel as an identity spoke.	<ul style="list-style-type: none"> ▪ An external partner, such as a supplier, serves as the IDP, and through federation-based single sign-on (SSO), accesses an Intel service application.
3. Intel as an external identity host.	<ul style="list-style-type: none"> ▪ An external user such as a supplier accesses an outsourced application, and the user authentication and authorization is handled through a demilitarized zone (DMZ) IDP located on an Intel server.

Defining the Proof of Concept

In order to provide the most flexible, cost-effective solution, we carefully researched what our customers needed before we began implementation.

Trust models and use cases

Our first step was to envision how the SSO solution would be used by both internal and external customers. We identified three main trust models and use cases, as shown in Table 1.

This paper focuses on Trust Model 1; even more use cases, based on Web service federation (WSF), are possible, but are currently less in demand than SSO access to outsourced service providers.

High-level requirements

Based on these trust models and use cases, we defined the following high-level requirements for the SSO process:

- Intel will be the IDP and the external site will be the SP.
- Both Intel and external users, after successful authentication and authorization from the main logon page, should be able to access the external site seamlessly.
- Users directly trying to access the external site will be redirected to the main logon page for authentication and authorization. After successful authorization, the user will be allowed to view the initial target URL at the external site.
- Users who register directly at the external site will not be part of the SSO process and cannot expect a seamless logon.

- Existing Intel employees or customers already logged on through the main logon page should have seamless logon to the external site. If the user doesn't have a user ID, then they will need to go to the registration page to log on.
- SSO functionality is achieved through the browser-post profile using an SAML 1.1 token.
- Secure Sockets Layer (SSL) will be enabled.

User authentication and authorization requirements

We also identified several specific requirements for the user authentication and authorization component:

- Secure authentication and authorization
- Centralized security management
- Single sign-on
- Policy-based access control
- Support for multiple and different authentication mechanisms
- Support for multiple and different user directories
- Scalability with load balancing and fail over

- Customization through application programming interfaces (APIs) and software development kits (SDKs)

Implementing Single Sign-On

Our implementation of SSO uses SAML 1.1. Produced by the Organization for the Advancement of Structured Information Standards (OASIS), SAML is a security markup language standard written in Extensible Markup Language (XML).

The SSO process consists of the following main steps:

1. A user logs on using either the main Intel logon page or the SP logon page.
2. A user is prompted to provide logon information.
3. The logon information is redirected to the IDP—the Intel site—for SAML processing.
4. The Intel servers access the data store to produce and encrypt the SAML file, which is an XML document that contains user profile information, along with security features including an authentication section.

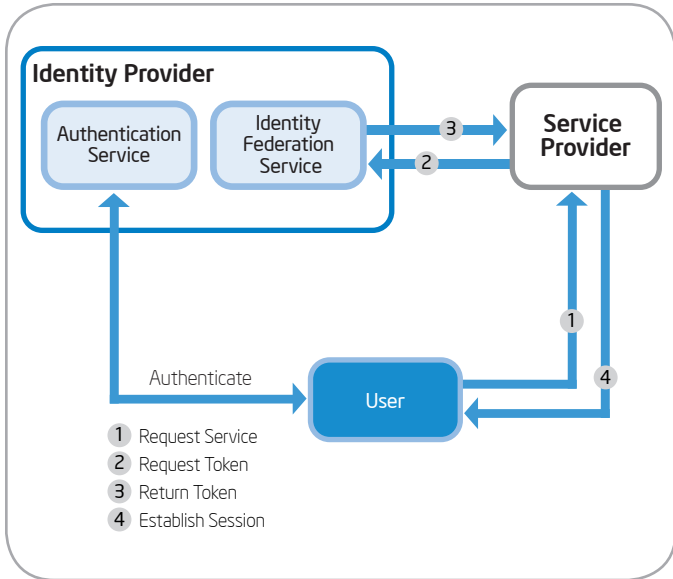


Figure 3. Using single sign-on, identities authenticated by an identity provider are trusted by a service provider.

5. The SAML file is sent to the external site.
6. Assuming the user is authenticated, the SP serves the application to the user.

Figure 3 illustrates the basic process; Figure 4 provides more detail.

SAML security features

To further enhance security, the SAML file is signed by a federation server certificate, which essentially says, “this file was created by this server and is intended for this consumer server.” There is a one-to-one relationship between the SAML file and its intended endpoint. If the SAML file is intercepted, it is invalid for any other endpoint. Also, the SAML file must be consumed within two minutes, or it is invalid.

Troubleshooting

As we developed our SSO solution, we encountered and solved several problems. The biggest challenge was integrating our authorization and authentication component with third-party endpoints. In particular, the SPs must be able to process the SAML file. Each situation is different, and we worked with vendors to find work-arounds and solutions as problems arose.

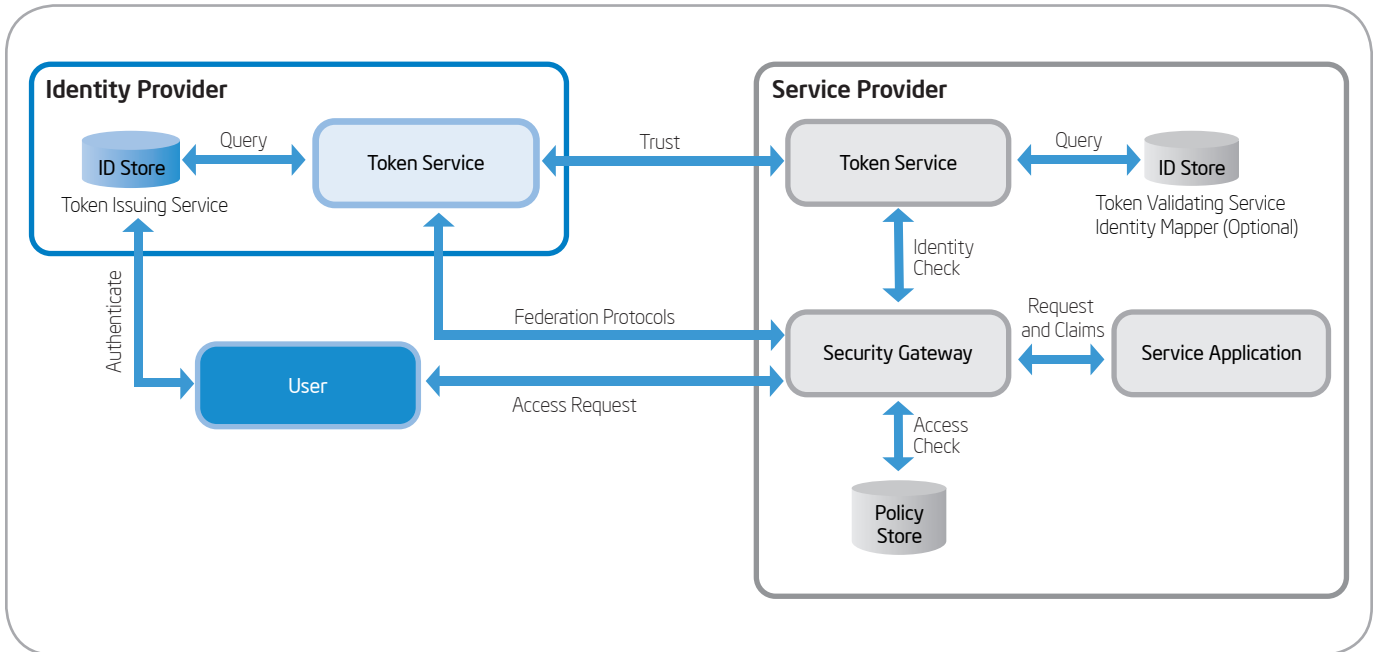


Figure 4. By passing secure tokens, Security Assertion Markup Language (SAML) enables seamless user authentication and authorization.

For example, on one external Web site, we found that if a user created a bookmark, closed the browser, and then attempted to use the bookmark in a later session, the user was returned to the site's home page after logging on, not to the bookmarked page. We worked with this ISV to modify the information being sent to the IDP server, so that the user landed on the correct page.

While troubleshooting these sorts of problems, we found it very helpful to enable the logging feature on the federation servers and to use a header browsing plug-in on the client browser, which allows a trace of the federation as well as the ability to capture the SAML response.

Systematic diagnosis

We used the following troubleshooting approach to diagnose problems when they occurred:

1. Verify the user is authenticated successfully on the IDP side.

2. Verify the SAML file is being posted successfully on the SP Assertion Consumer URL.
3. Verify the SAML file is consumed and processed successfully on the SP side.
4. Make sure the requested SP application is served to the user.

Steps 1 and 2 can be verified from logs on the IDP side, whereas Steps 3 and 4 must be verified on the SP side.

Expected Benefits

As we have only just begun to expand the PoC to additional users, we haven't started measuring user experience and satisfaction yet. However, as outlined in Table 2, we expect our SSO solution to provide significant benefits in several critical areas.

Table 2. Expected Benefits of the Single Sign-on Solution

Benefits	Details
Improved Security	<ul style="list-style-type: none"> ▪ User identity information is better protected because it is under Intel's control. ▪ Only required personal information is sent in the Security Assurance Markup Language (SAML) token, reducing unnecessary exposure of sensitive data. ▪ Release of employee profile information is controlled by policy and employee opt-in. ▪ Reduced requirements for storing extra information for external users means reduced identity theft liability. ▪ Off-network access can be safely processed on borrowed networks or low-functionality systems. ▪ Keyboard logger attacks are less of a concern. ▪ Accounts can quickly be disabled from one central point as needed.
Improved IT Efficiency and Cost Savings	<ul style="list-style-type: none"> ▪ A huge reduction in password maintenance effort lowers costs. ▪ A single, cross-domain and Internet-capable user directory reduces infrastructure requirements and minimizes necessary administration. ▪ Fewer remote synchronization problems occur. ▪ Personal information necessary for business logic is still accessible in real time. ▪ Internal authentication systems can be used to control off-Internet access.
Enhanced User Productivity and Experience	<ul style="list-style-type: none"> ▪ Users no longer have to remember multiple user IDs and passwords. ▪ Users spend less time repeatedly logging on. ▪ Universal single sign-on (SSO) to heterogeneous application environments provides users with a more consistent, unified experience.
Added Value for Partners	<ul style="list-style-type: none"> ▪ Intel manages access to partner sites. ▪ Intel provides SSO services for a network of business partners.

Next Steps

Based on our initial success with federation and SSO, we plan to expand the solution in several directions.

- Roll out the SSO solution to additional sales and marketing organizations.
- Upgrade from SAML 1.1 to SAML 2.0.
- Extend our use of user attributes by pulling information from a separate customer profile management (CPM) database, so we can further customize the user experience.
- Possibly implement more trust models and use cases, based on user demand and industry acceptance of relevant standards

Conclusion

Security, operational efficiency, and enhanced user experience are three critical focal points for IT organizations. Implementing a federated SSO solution has enabled Intel IT to address all three of these issues.

By storing sensitive user profile information in one place and maintaining it ourselves, we can assure our closed community members that we value customer privacy and can provide Web security for all external Web sites with which they interact through our communities.

By storing user profile information in one central place, we are no longer forced to maintain multiple user directories and redundant passwords. Data synchronization is much easier. These improved

efficiencies reduce data maintenance costs and increase IT organizational productivity.

By freeing our users from multiple user IDs and passwords and providing them with easy, seamless Web site access, our SSO solution creates a one-stop portal to the tools and information users need. In addition, the authentication and authorization process allows us to customize the user experience, based on user profile information.

Authors

Brandon Wiens is a systems programmer with Intel IT.

Ajaya Agarwal is an application developer with Intel IT.

Acronyms

API application programming interface

CPM customer profile management

DMZ demilitarized zone

IDP identity provider

ISV independent software vendor

OASIS Organization for the Advancement of Structured Information Standards

PoC proof of concept

SAML Security Assertion Markup Language

SDK software development kit

SP service provider

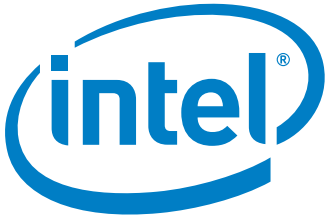
SSL Secure Sockets Layer

SSO single sign-on

VPN virtual private network

WSF Web service federation

XML Extensible Markup Language




www.intel.com/IT

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.
Copyright © 2009 Intel Corporation. All rights reserved.

Printed in USA
0109/JLG/KC/PDF

 Please Recycle
320559-001 US