ELM

ELM Manages Identities of 4 Million Government Program Users with

WSO2 Identity Server

http://wso2.com

WSO2

ELM Implements Single Sign-on With WSO2 Identity Server to Streamline Administration, Improve Productivity, and Reduce Costs

In Saudi Arabia, ELM is a trusted provider of secure electronic services. Providing deep expertise in innovative and specialized e-services for government transaction and e-government initiatives, it is the first company in Saudi Arabia to have successfully launched a fully compliant e-government process.

Recently ELM architected and implemented a system to manage a range of processes for the Saudi national Unemployment Assistance Program. Today, ELM relies on WSO2 Identity Server to manage some 4 million users of the Unemployment Assistance Program and ensure secure online transactions.

Accommodating Unemployment Assistance Program Growth

In 2011, the Unemployment Assistance Program launched to provide an allowance for all Saudi citizens who were currently unemployed and searching for a job. ELM had implemented the system, which included a portal where citizens could submit their requests, as well as applications running in the background that managed all the processes for qualifying the users and handling any payments.

Initially, the project just covered one program. However, a year later, as the Saudi government expanded services to include several programs, ELM recognized the need to streamline the administration for managing the user identities of everyone involved with the program.

The ELM Unemployment Assistance Program team decided that the best solution would be to implement single sign-on (SSO) between a set of relying party vendors. The next step was determining the right technology provider to help deliver that solution.

"We evaluated identity management options from all the large vendors," recalled Abdullah Al Tahhan, a senior project manager at ELM. "Out of all the solutions we tested, WSO2 had the most flexible solution. We liked that it was customizable and could be modified to fit our needs."

> "WSO2 had the most flexible solution. We liked that it was customizable and could be modified to fit our needs."

OpenID Vs. SAML 2.0 for Single Sign-on

To support the implementation of WSO2 Identity Server, ELM obtained a two-month consulting engagement with WSO2's engineers. As the ELM and WSO2 developers began outlining the architecture, they realized that the first decision would be whether to use OpenID or the Security Assertion Markup Language 2.0 (SAML 2.0).

OpenID and SAML 2.0 are the two most widely used standards for single sign-on across the Web, and both offer a platform-agnostic approach that allows enterprise architects to implement a uniform security layer with existing assets. Furthermore, WSO2 Identity Server supports both standards. However, there are significant differences in the standards.

1. SAML 2.0 supports single sign-out. OpenID does not.

2. SAML 2.0 service providers are coupled with the SAML 2.0 identity providers. OpenID relying parties are not coupled with OpenID providers. Instead, OpenID has a discovery protocol, which dynamically discovers the corresponding OpenID provider once an OpenID is given.

3. With SAML 2.0, the user is coupled to the SAML 2.0 identity provider, so a user's SAML 2.0 identifier is only valid for the provider that issued it. By contrast with OpenID, users own their identifiers and can map them to any OpenID provider they wish.

4. SAML 2.0 offers different bindings while the only binding OpenID has is HTTP.

5. SAML 2.0 can be either service provider-initiated or identity provider-initiated, but OpenID is always service provider-initiated.

6. SAML 2.0 is based on XML while OpenID is not XML-based.

After weighing the differences between OpenID and SAML 2.0, the ELM and WSO2 engineers decided to proceed with OpenID in directed identity mode to support both dumb and smart relying parties. With OpenID dumb mode, relying parties would not have to worry about handling signatures themselves, hence the load on client is less. With smart mode, each client has to process signatures and the load on the server and the network traffic are less . WSO2 Identity Server supports both OpenID dumb and smart modes simultaneously with an option to disable dumb mode.

“We like the fact that with the OpenID directed identity mode, users do not have to remember lengthy URLs,” Mr. Al Tahhan explained. “Users are simply redirected automatically to the Unemployment Assistance Program OpenID provider for authentication, and then they can just login with their Unemployment Assistance Program user name and password. It is a simple and elegant approach.”

Implementing the SSO Solution

With the architecture solidly in place, ELM was ready to put the project into action, and with two WSO2 engineers working onsite side by side with the ELM technical team, the system was up and running within two months.

“WSO2 has provided great, around-the-clock support. They are the most available support team we have worked with.”

“WSO2 has provided great, around-the-clock support. They are the most available support team we have worked with. When we ask for technical service, we get a response in no time,” Mr. Al Tahhan observed.

In production since April 2013, the Unemployment Assistance Program SSO system manages about 4 million users with 2,000 login requests per second.

The entire architecture implemented by ELM sits behind a firewall to ensure secure, authorized access. F5 application networking software manages incoming requests from users and authenticates these users through the four WSO2 Identity Server instances that have been installed. WSO2 Identity Server then checks user information, which resides in a Microsoft SQL Server that sits behind a second firewall.

Key features in WSO2 Identity Server, such as the role-based access control (RBAC) convention, fine-grained policy based access control, and SSO bridging, help to reduce identity provisioning time, guarantee secure online interactions, and deliver a reduced single sign-on environment.

Realizing Single Sign-on Advantages

Since implementing single sign-on through WSO2 Identity Server, ELM has been able to significantly streamline the administration of user identities, as well as improve the overall user experience. The benefits delivered by SSO include:

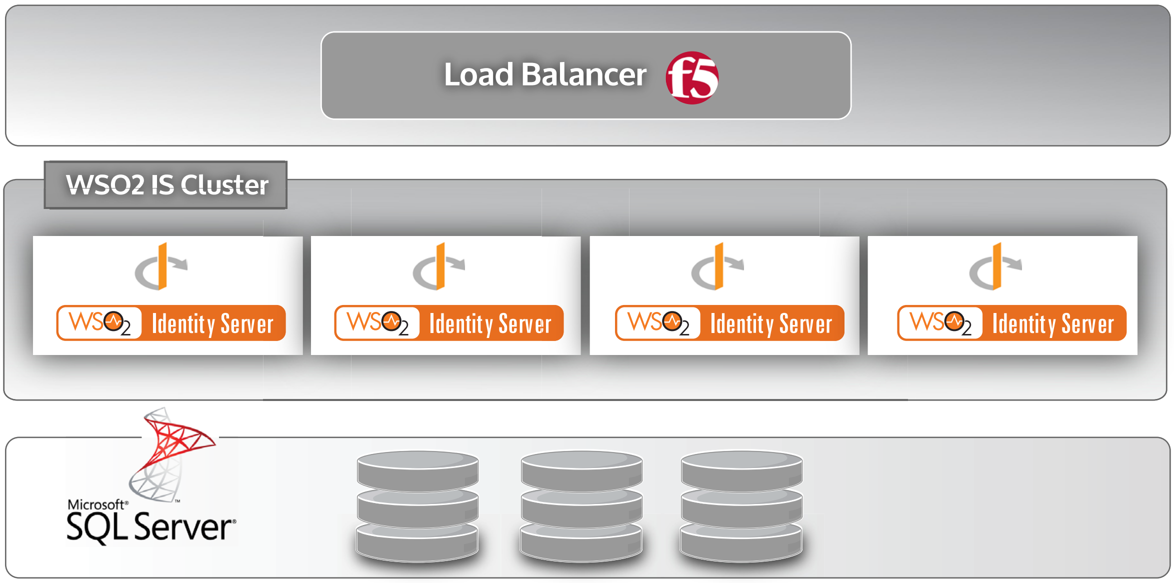
Improved productivity. Single sign-on eliminates the need to enter a password each time users log in to a resource, which saves around 20 seconds and increases productivity. Also, users only have one password to remember and update, and only one set of password rules to remember, reducing the frustration of multiple log-on events and forgotten passwords. Additionally, SSO facilitates adoption, since it reduces the barriers to using resources and applications.

Centralized management and reporting. Using a single registry of user identities with a centralized management interface enabled the quick and easy provisioning and deactivation of users. There is also an improvement in reporting and monitoring, and having a single repository for auditing and logging access to resources provides streamlined regulatory compliance.

Increased security. Having implemented a secure, enterprise-wide infrastructure with common password and security policies, ELM allows user identities to be managed and secured centrally. Since OpenID is platform-agnostic, it adds a uniform security layer. Moreover, users are less likely to write down their passwords when there is only one to remember.

Reduced helpdesk costs. Because SSO provides an easier way for users to authenticate their identities, there are fewer helpdesk calls for password resets, resulting in bottom-line savings.

“The SSO environment implemented with WSO2 Identity Server has fully met our expectations and is enabling us to realize the goals we set out for simplifying our user identity administration,” Mr. Al Tahhan says. “We are quite pleased with WSO2’s technology, but more than anything, when we think of future engagements, we are going to think of WSO2 because of the great support.”



Unemployment Assistance Program Single Sign-On Solution Architecture

Figure 01