AUTHENTICATION AS A SERVICE: SINGLE SIGN-ON
CUSTOMER AUTHENTICATION

Category: Improving State Operations

State of Utah

NASCIO 2011
**Executive Summary**

The State of Utah has over 950 online services, many of which require authentication, and varying levels of security and trust. These services are provisioned by nearly all government agencies without a well designed Single Sign-On (SSO) approach. Authentication is provided by a number of different approaches with little in common. The intent of this project is to provide Authentication as a Service with an SSO approach that allows agencies to establish multiple levels of trust and integration with other State directory services such as the Utah Master Directory (UMD).

The architecture of the project has been designed to be used by all State agencies that wish to allow users to leverage OpenID as an authentication mechanism for public facing services.

The Utah Department of Workforce Services (DWS) provides a host of one-stop services to job seekers, employers and other workforce partners through the online portal [http://jobs.utah.gov](http://jobs.utah.gov).

For the job seeker, key DWS services include job matching, claims filing and benefits case management. Access to these online services requires customer authentication through an online application/system; UWORKS, CUBS and myCase respectively.

Historically, authentication to each of these primary systems required separate and distinct credentials from the customer. To access UWORKS for job matching, an email address and password was required. To complete a weekly filing for unemployment in CUBS, a social security number and pin was required. And, to report changes to a food stamp case in myCase, 6 separate pieces of personal information were required.

Consequently, customers wishing to access multiple systems had to first remember and then enter the unique credentials for each system they accessed. Equally unique and arduous for the customer was the process of credential recovery; often requiring the support of front-line staff.

To simplify the process of accessing multiple systems, the department developed *Single Sign-On Customer Authentication*.

Customers are now able to authenticate with DWS systems using an account with Google, Yahoo or Facebook. Authorization is still required up front with each of the applications to connect the DWS customer with their sign-on account but, once established, the customer is then granted access to multiple systems with a single sign-on.
DESCRIPTION OF THE BUSINESS PROBLEM AND SOLUTION

The broader context for this project on a Statewide basis is implementation of Authentication as a Service (AaaS). The Department of Workforce Services (DWS) has a large public user audience where authentication is required. Citizens tend to prefer authentication vehicles that are familiar to them and easily remembered. Single Sign-On Customer Authentication is an enterprise system of AaaS that allows DWS customers to sign-on with multiple online systems using a single authentication. Authentication is made through one of three Open ID providers; Google, Yahoo or Facebook. The project is also designed to support the Use of Utah ID for those citizens that prefer to use a State assigned ID. DWS was the proof of concept for this Statewide service offering.

Problem Statement
The premise behind a one-stop operation is that customers are able to access multiple services under the same roof; whether that roof is brick and mortar or a virtual roof. Customer access to DWS online services has been challenging due to the varying authentication requirements of our different systems. Customers accessing multiple systems were required to maintain separate credentials for each system. Forgotten usernames, passwords and pins were also handled differently by each online system.

Barriers, Challenges, and Opportunities
The department faced several significant barriers in moving from unique authentication systems to a Single Sign-On Customer Authentication.

1. Creating agreement among business partners was the first critical step to the overall success of the project. Without agreement, we wouldn’t have a “single” sign on system. Reaching an agreement focused on two primary areas; security and ease-of-use.

   Security was the primary concern for all business partners. All agreed that authentication alone was not enough to grant access to customer data. In addition to authentication, each online system would continue to require one-time authorization. Authorization ensured that customers who authenticated through Google, Yahoo or Facebook were in fact known to DWS.

   Given the volume of work being conducted online, ease-of-use was also a critical factor in gaining partner agreement. No partner was willing to implement such a significant change to the sign-on process if it meant a disruption in online workflow. Even a moderate disruption online would have caused major setbacks in the processing of weekly unemployment claims, job matching and benefits management. Patterning our work after private sector examples, we were able to develop and test a process that minimized customer impact.

2. Technically, one of the more challenging barriers we faced was the process of connecting an existing or “legacy” authentication with a new Single Sign-On
Customer Authentication. This required the use of an association screen. Here, after selecting a single sign-on provider, customers would identify themselves to DWS by 1) entering their legacy credentials or 2) entering personal data. Once completed, the customer would not have to revisit the association process on subsequent visits.

3. Changing customer behavior was also a barrier, and an opportunity. While many customers were comfortable with the existing DWS interface, others were missing out on the opportunity to stay connected with other, related DWS services. Some of those missing out on the benefits of single sign-on included select populations of DWS customers, those receiving certain types of benefits or unemployment insurance, who were required to participate in multiple online systems, namely job matching services.

4. Building the customer interface or sign-in screen for Single Sign-On Customer Authentication became even more challenging with the decision to maintain, for a period, the existing customer’s legacy sign-on while introducing single sign-on.

Through our analysis of customer behavior, we determined that many customers would not immediately embrace a system of single sign-on; particularly those without a need to access more than a single system. It was therefore determined to allow customers for a period of time to continue using their existing or “legacy” credentials while also having the option to sign-on with an Open ID provider.

Issue or problem context
The main challenge of the project other than implementation logistics was to architect the DWS solution for statewide applicability and integration with the State’s existing master directory infrastructure.

Solution Description
The project presents the user of DWS services with a login screen that allows the user to leverage OpenID providers for their login. User ID data is synchronized with other Utah directory resources such as the UMD and internal DWS resources that track trust levels for specific applications. In June 2011 the State of Utah will be adding a fourth OpenID provider, for customers that prefer a State source.

Length of Time in Operation
Single Sign-On Customer Authentication has been in operation since November 2010. The project timeline was as follows:
• June 2010 Business Requirements
• July 2010 Business Case
• August 2010 AaaS SSO Requirements and Architecture
• September 2010 Prototyping and Testing
• October 2010 Coding and Implementation
• November 2010 Product Release
Innovative Characteristics
Innovative to the DWS Single Sign-On Customer Authentication is the use of Facebook as an authentication source. To work with Facebook as a source of authentication required a slightly different set of programming rules than those followed with Google and Yahoo. However, the addition of Facebook is seen as significant, based on our observed use of Facebook by DWS customers.

Still, some customers expressed reservations about using Facebook for the purpose of signing on with DWS; fearing that DWS would obtain their personal Facebook information. For this reason, DWS restricted the interface with Facebook to only allow for the sharing of information required for authentication.

Leverage and Transferability
The DWS Single Sign-On Customer Authentication system is seen as an enterprise solution for the state of Utah. DWS continues to work closely with the state Department of Technology Services to ensure steps taken within the department coincide with the direction of the state in building statewide citizen access to online services.

Communication Plan
Throughout the implementation of Single Sign-On Customer Authentication customers have been notified through online messaging of pending changes. Great care had to be taken to ensure a smooth transition for customers from multiple “legacy” sign on accounts to a “single” sign-on account.

The language used in online messaging was tested with customers in a beta environment over the course of several weeks. Test results were then used to modify messaging.

Front-line employees were also used in the testing and messaging with customers to ensure those working with customers would be able to support the process.

Training was also provided to DWS community partners; recognizing the important role of our partners in helping customers gain access to DWS services.

Significance
The potential impact of Single Sign-On Customer Authentication is as great as the number of customers being served by the department. Though not all customers choose to go online, all primary DWS services have a home on the web with one of our online applications/systems.

In April 2011, the department issued benefits on more than 292,000 cases. Each month the department issues roughly 700,000 job referrals and takes nearly 175,000 weekly claims for unemployment insurance.

All of these services are supported online and accessible through single sign-on. Many of these users also access many other State services and will benefit from an AaaS SSO approach.
**Description of Beneficiary/Stakeholder Groups**
The principle groups impacted by the DWS project are citizen users, and DWS agency personnel responsible for providing access to DWS online services.

**Policy, Strategy, Goal Alignment**
The project aligns DWS and State goals for authentication and access to on-line services with varying levels of trust requirements, while at the same time minimizing the number of sign-ons required for citizens to use State services.

**Benefit of the Project**
Citizen users of public facing services that require authentication generally seem to prefer using user ID and passwords that are frequently used, such as Google, Yahoo, and Facebook. State specific passwords are harder for users to remember and require more State password maintenance. A single sign-on solution for multiple applications is a large potential benefit for public users.

**Description of impact of the project**
The DWS project impacts 575,000 unique visitors per month and impacts a broad cross section of users of State services. Success with DWS services enables many other agencies to use this same kind of service on their public facing sites that require authentication.

**Description of types of benefits and the impact of the benefits on both the agency nominating the project and the groups which benefited from the project**
Primary benefits include:

1. Single authentication through a known provider; Google, Yahoo or Facebook—Many DWS customers already have accounts with one or more of these providers.

2. Credential recovery through the same, known provider—A familiar process to most customers who have an account with one of these providers. Username and password recovery is handled exclusively through the Open ID provider—No involvement or impact on the department and its staff.

3. Utah Master Directory (UMD) integration and provision for the State of Utah to become an OpenID provider.

**Non-Financial Return on Investment**
The chief non-financial ROI to DWS is a sign-in process in line with industry standards and familiar to our customers. Though difficult to quantify in terms of dollar savings, online access to DWS services is paramount in meeting the service needs of our customers; particularly in difficult economic times when budgets are tight and demand for services is high.
Measurements
117,690 DWS customers have opted to create a single sign-on account. Many of these are accessing multiple systems.

**Figure 1.** Single Sign On User Accounts

**Figure 2.** DWS Customers Accessing Multiple Systems