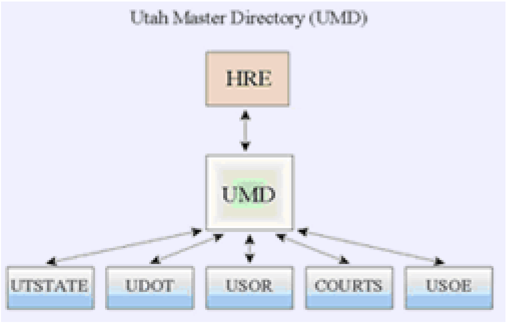
UMD: UTAH MASTER DIRECTORY

EXECUTIVE SUMMARY



The Utah Master Directory (UMD) is an identity management system for all State of Utah employees and approved citizens. It is the touchstone for all applications requiring authentication and authorization, providing a single, up to date database of consistent user information as well as a single sign on solution when a user ID and password are required for access.

Prior to UMD, the State of Utah had many authorized user directories; one for almost every online application. The application administrator had to create dedicated accounts for the users, and the users had to remember an ID and password for each secure application they accessed. In addition, application administrators were not consistently notified when there was a change in an employee's status. A single Enterprise Authentication Directory seemed to be the answer; one that used the Human Resource database as its "source of truth", providing the most accurate and up to date user profile available. An application was designed, programmed, and tested. The completed Utah Master Directory was placed into production in July 2002 and has proven to be very stable.

UMD has proven to be a fast, accurate employee provisioning and de-provisioning solution. Now, each State employee has only one user ID and password to remember to all the participating State applications they access, and when an employee terminates State employment, accounts with all associated systems are automatically disabled.

Associated systems allow enterprise collaboration and improve reliability and security. Just a few of these applications include a white pages application to view employee information, including organization charts, phone numbers, and work addresses; instant messaging applications; and, employee time sheets.

DESCRIPTION OF PROJECT

Descriptions of the Business Problem

With the State having multiple user stores, it was determined that there was a need to create a single Enterprise Authentication Directory; a user store for both State employee and citizen user accounts. Almost every time a new application was added into the system an administrator had to create accounts for the new user. And users had to remember a unique user ID and password for each system they accessed.

Before UMD was implemented, we used the existing statewide resource directory for single sign-on. Accessing authenticated sites was often difficult, as user IDs were deep in the tree (directory) and often could not be located before the login attempt timed out.

New web applications were being created were users had to create new ID’s to access these systems.

Administrators were not consistently notified when new employees were hired nor when employees were terminated or transferred to another agency.

Business owners and users wanted to be able to login to multiple protected sites using the same user ID and password as they used to access the main State network.

Business owners, rightfully demanding better security and wanted their application to be somewhat separated from the other applications and yet did not want to create their own user store. They also wanted to be able to enter an attribute (such as a license number), or part of a user profile, and have it displayed accessible only to their application.

Application developers and stakeholders felt that it would be beneficial to create an “identity vault” of users which would be tied directly to Human Resources and the HR directory trees to have a single source of user identity. This system would communicate to other systems, providing a source of truth; the one location with the most accurate all around user profile information. This system would then share this information with connected systems as needed.

Purpose and Objectives

UMD provides an identity store of all employees and many citizens where applications requiring authentication and authorization can look to one directory (data) store for consistent user information as well as providing a single sign on solution, giving users one user ID and password for all participating systems.

Solution Description

The State of Utah has a unique situation, where employees can be in one of five different file and print directories (which we refer to as “resource directories”), depending upon which agency they work for. UMD was implemented to work with this existing infrastructure, and was designed to use HR as the authoritative source for the user profile information. HR's system sends the user information to UMD, which, in turn, sends it on to resource directories.

The system infrastructure is based on publish and subscribe channels, where data is passed in XML (DirXML) format from one system to the other as appropriate. Information is sent only when the other system needs it. Only modified information is sent keeping the synchronization process as efficient as possible.

When an action on a user occurs in HR, it triggers an event to UMD. This then initiates the change in UMD (whether it is a new user, a change, an update, or a termination). UMD then makes that change in the UMD directory and passes needed information along to the resource directory. All components of the system are connected at the user account level, providing an automated approach to maintaining a consistent and updated user profile within the identity vault.

With the identity vault in place, an authentication and authorization system can be connected, enabling a SSO approach to accessing protected applications. This is accomplished with two additional components: SiteMinder, and a custom application called AppProfile. Together these enable an application owner to have their application protected behind an SSO system which allows them to read and write user attributes to and from the identity vault. This approach also allows us to delegate the task of managing authorization and access control for individual users on specific applications to the application administrators.

Length of Time in Operation

The directory for UMD was put into production in August 2002. The authentication and authorization components were integrated into production in November 2003.

Significance to Improved Government Operation

Operational Maturity

The UMD infrastructure has proven to be very stable and advantageous to automating tasks that had been previously been handled through manual processes.

Predictable Results

The UMD infrastructure has proven to be very stable. Early on, as with most applications, the programmers had to make adjustments periodically to correct minor issues. Alert modules were added to send messages to the application administrators when a component of the infrastructure was not functioning properly. This happens rarely, and when it does, the operations team generally has the application back on line before users are impacted.

Agencies appreciate the fact that they do not need to have their own on-call staff for user support. The DTS Help Desk is able to handle the tasks of assisting users with authentication and password issues.

In addition, the infrastructure was built to tolerate system failures by providing automatic failover. The login components utilize Layer 4 network technology for load balance and failover, including the policy, profile, LDAP, and directory servers. This results in a completely redundant system.

Cost Effective Development

Cost savings is sometimes hard to determine, but it appears that there is a 20% to 25% decrease in the application development costs by using this enterprise authentication and authorization system. This is based on not having to code these features into every application.

There is also a cost savings in the reduced number of user stores that must be maintained and managed. For the larger application there is usually at least one FTE required to manage the user store, update information, and reset passwords. Business owners appreciate the fact that by using the enterprise system they do not need to allocate resources in this area.

Users, allowed to use a single user ID and password, saved an incalculable amount of time and frustration by not having to remember multiple sets of access information.

Reliability and Timeliness

Some of the advantages achieved by UMD include an increased speed for integration of an application into production. Developers no longer need to write code for authentication nor user store for their applications. Applications can be built and “plug-in” to the authentication module and rely on this existing infrastructure. Authorization is still a business management task, but this can also be automated in most applications. Other tools have been created to simplify the authorization process.

Applications that utilize JAAS are especially easy to attach to the UMD system, while off the shelf applications are sometimes a little more difficult to integrate. However, most applications have been successfully integrated.

Public Value of the Project

Stakeholder Participation

Several State agencies use UMD for applications that are public facing. UMD supports access for citizens, and citizens can create their own account when initially attempting to access a protected application. The citizen is then able to use this same account for any other protected application for which they have been granted access. A password reset feature has also been implemented so State employees and citizens can reset their own password, following the standard challenge and response process.

Public Policy Benefits

Using SSO solutions has been helped with the increased rate of adoption by agencies. When agencies witness the benefits of reduced development time and the benefits of a connection to the identity vault for a single source of truth, they have chosen to implement this in their processes. They also appreciate the fact that they can grant existing users access to their applications rather than requiring that everyone create a unique account just for their application. This is especially advantageous for public facing applications.

State and Agency Benefits

Since implementation into the production environment, UMD has enabled a faster and more accurate employee provisioning and de-provisioning solution. Now, when an employee terminates State employment, accounts with associated systems are disabled. Also, connected systems have been implemented to allow enterprise collaboration and improve reliability. These applications include a white page application to view employee information (including agency, organization charts, phone numbers, and work addresses), the enterprise instant messenger application; and, the enterprise employee time sheet application; among others.

Realized Return on Investment

Adoption

Adoption of UMD was slow at first, as application developers finished projects underway and did not have the resources or the time to change existing processes. Meetings were arranged with each agency to explain the concept and infrastructure and to share the documents and plans as to how their agency would benefit from the enterprise system.

For UMD directory, adoption was immediate, affecting each agency and every employee. For the authentication components, adoption was slower and took about a year and a half to get development cycles in line to utilize the new infrastructure. It is difficult to know exactly how many sites there are, but currently there appear to be over 190 Web resources (both applications and sites) using UMD Authentication, several of which are public facing. A solid 94% of all State employees have accessed the system. Additionally, several thousand citizens have created accounts and accessed resources protected by the system.

Savings and Cost Avoidance

The savings realized and avoided from implementing UMD have not fully been calculated but the areas have included;

- Reduced cost to help desk for password resets.
- Reduced development time and cost because a new user database is not needed for every application.
- Reduced development time and cost because authentication does not need to be developed for each application.
- Reduced need for user administrators for each application.
- Consistent user data.
- Profile and rights administration simplification.
- Single sign on for quicker access to applications.
- Users account creation automation. Instant notification of de-provisioning of terminated users to security administrators.
- Provides a means for public citizens to do business with the State using a one identity.
- Pre-filling forms at the time of login for users so they don't have to enter their information multiple times.
- Users can reset their own password using the challenge and response process without contacting the help desk.
- Provides a central place for role-based provisioning.

Return on Investment

The overall project costs over the past years are as follows:

Consulting	320,000	Initial Software	430,000
5yr Software maintenance	280,000	Hardware	120,000
5yr Hardware maintenance	1,160,000	Personnel	212,000
		Total Cost	**2,522,000**
41 Large Applications	190 Total Applications	**Total Benefit over 5 years**	**Exceeds $13,583,000**

Based on average data, the total benefit of the Utah Master Directory exceeds cost by over $11 million. Savings have also been realized in application development. Additionally, personnel who would have developed and supported authentication and login services for the 190 applications have been directed at other critical tasks.   Single sign-on capability has saved an unknown number of service calls and reduced time to created user ID's.

Continuing Operational Benefits

The time and money not spent on developing and maintaining a separate user database for each application is applied to the development of other projects. Thus the quality and timeliness of new applications is increased overall.