Title of Nomination: Government to Government – Easy Government Access through Identity and Access Management

Project/System Manager: Ann Garrett and Brent Roberts (representing multi-disciplinary team involved in this project)

Job Titles: Ann Garrett, Chief Security Officer
Brent Roberts, Identity Access Administrator
Address: 4101 Mail Service Center, Raleigh, NC 27699-4101
Telephone: 919-981-5310
Facsimile: 919-981-5043
E-Mail: Ann.Garrett@ncmail.net
Brent.Roberts@ncmail.net

Category: Digital Government – Government to Government

Person Nominating: George Bakolia
Job Title: North Carolina Chief Information Officer
Address: 4101 Mail Service Center, Raleigh, NC 27699-4101
Telephone: 919-981-2680
Facsimile: 919-981-2548
E-Mail: George.Bakolia@ncmail.net

Executive Summary

North Carolina's Office of Information of Technology Services needed a simpler and more secure way of managing user accounts in state government: a method that would allow a large number of users to access necessary services through a centrally managed system. Such a process would have two immediate benefits: 1) it would reduce the potential for insider attacks through better controls on system usage and also by promptly deprovisioning employees when they left public service; and, 2) it would streamline government expansion of services to the public using information technology by providing citizens with a centralized log in.

To meet this need, the Identity and Access Management System (IAMS) was born. The first offering of the service has begun with the state's 60,000 employees. IAMS will be expanded to citizens and businesses that need to communicate securely over the Internet with government. IAMS users are able to sign on to multiple systems and applications using their single account. While streamlining access to multiple systems, IAMS increases the security of the state's network by requiring an authorization process, including self-registering, before an individual is authorized to access systems and applications. IAMS also reduces the workload of the help desk by allowing self-registration for an account and allowing individual users to reset their passwords using their secret pass phrase.

As designed, IAMS:

- Allows users to self-subscribe, self-register, and self-administer accounts through a platform independent administration facility.
- Reduces the burden of account administration and the number of redundant entries in the various agency directories.
- Provides a secure electronic approval process for the creation and alteration of user accounts.
- Provides for role-based authorization.
- Reduces the number of IDs a user is assigned.
- Creates audit trails for all processes.

Today, businesses can use IAMS to help them file their quarterly sales and use taxes on-line with the North Carolina Department of Revenue. This allows the taxpayer to file effectively and safely. It also brings funds to the state treasury more quickly. Agency information technology security representatives use IAMS to access the state's Security Portal to retrieve the latest information on cyberthreats. Agencies use IAMS to provide controlled access to their intranets. Tomorrow, IAMS will allow parents to securely view their children's report cards through their school's web pages. Ultimately, IAMS will provide secure centralized Web access to a broad, disparate range of government services, channeling services through a single authentication and authorization directory, and allowing citizens and businesses a more streamlined way to pay taxes, renew their motor vehicle registrations, and purchase state fair tickets.

A. Description of project

The North Carolina Office of Information Technology Services (ITS), as the central information technology provider for state government, was approached three years ago by several agencies seeking centralized identity management and Web-based access control solutions. The agencies wanted a central entry point to government services, with security policies built in that mandated compliance with rigorous security standards for authentication and authorization.

The North Carolina Criminal Justice Information Network (CJIN) needed a secure way of providing access to federal, state and local records housed in a multitude of data files to a wide variety of criminal justice organizations, all of which were geographically distributed throughout the state. In addition to making certain the data was secure, CJIN required that the system provide information or access only to authorized personnel, who, in turn, had different access requirements based upon their roles and responsibilities.

The authentication of personnel and authorization for access to records had to be accomplished quickly and the administration of privileges had to be sound, reliable, and easy to perform. IAMS had to satisfy stringent access requirements for criminal justice data.

The statewide authentication and authorization project created a new central lightweight directory access protocol based directory (LDAP) that is automatically synchronized with certain agency directories for enabling statewide authentication and authorization.

Profiled in the May 2003, edition of Information Security Magazine[1] and the January 2003, edition of Government Technology[2], the ITS IAMS has six key features:

- Self service registration: A user can register through a central web site and be issued an identity after the user is authenticated by a third party, such as a supervisor.
- Delegated administration: Instead of requiring a network administrator to change user information the user can do so, following the built-in security checks that ensure the user is who he says he is.
- Identity life cycle management: The system provides one-stop shopping for issuing, modifying and terminating user IDs. A user with access to several applications can be quickly terminated from those applications with a single action.
- Auditing: Successful and unsuccessful attempts to protected systems are monitored, as are changes to IDs and authorizations. IAMS has intrusion

[1] Roiter, Neil, "Who Are You? Identity Management" Information Security May 2003, http://www.infosecuritymag.com/2003/may/whoareyou.shtml

[2] Brown, Justine K. "Positive ID" Government Technology January 2003, http://www.govtech.net/magazine/story.phtml?id=36406

detection system capability that can proactively send alerts to system administrators.

- Authentication: IAMS allows for inclusion of two-factor identification, including passwords, PKI, biometrics, and hard token.
- Authorization: Users are assigned access privileges based upon the roles they play within groups, such as teachers within a group of educators.
-

B. Significance to the improvement of operations of government

From a security perspective, IAMS establishes a proven, scalable, and repeatable process for securing resources and providing ease of access to those resources for users who qualify. IAMS frees up technical support for technical activities. No longer are systems administrators called upon to reset user IDs: the users can reset their own. Further, user IDs are managed centrally, allowing IDs to be modified or terminated easily and avoiding the possibility that users retain access to a system when their duties change or they leave government service.

IAMS also provides a way to map business processes and resource allocation to electronic systems through the work flow process. This means that an agency can take what's done manually on paper and turn it into an electronic process, allowing approvals to be done electronically rather than chasing a paper trail to ensure the approvals are obtained.

C. Benefits realized by service recipients, taxpayers, agency or state.

An often frustrating side effect of information technology is the multitude of user names and passwords that must be remembered in performing routine tasks. IAMS removes the frustration by allowing one user ID and password for multiple systems. And, when the password is forgotten, the system lets the user reset the password by correctly answering the secret question with a pass phrase that the user previously provided.

Other benefits include:

- Password synchronization – allows use of a single password for multiple systems. When a password is reset, all are updated automatically.

- Password policy enforcement – ensures passwords comply with the state and agency security standards for password creation, including length and characters.

Another real benefit is the cost savings that come from accessing government services through a centrally managed system, as shown in Section D.

D. Return on investment, short-term/long-term payback

The IAMS features that simplify sign on and management of user IDs have immediate payback because of the reduced need for system administrators to work with user IDs. Further, allowing users to reset their passwords reduces the need for help desk support. Jonathan Penn, a research director for Giga Information Group, says the provisioning features can save as much as 50 percent of all IT time spent on user account management, such as creating new accounts, changing accounts and disabling accounts. Help desk costs for password resets are estimated at $25 per incident, according to Giga. [3]

ITS has paid $2.5 million for IAMS and the license to provide every citizen, business and state government employee with a user ID – over 8 million in all. The cost for each user ID is less than 32 cents.

ITS use of IAMS is relatively new, but based on survey data, Meta Group has modeled the savings that a typical organization with 10,000 employees can expect[4]:

- The average user spends 16 minutes a day signing in to systems and being authenticated. For a 10,000-user organization, this is equivalent to 2,666 employee hours a day.
- About 45% of help-desk calls are requests for password resets. Automating the reset process and letting employees service themselves would reduce the help-desk call volume by a third and result in an estimated annual cost savings of $648,000.
- Respondents predicted that time savings from the centralization and consolidation of user database management would be more than 1,200 hours a year. Managing users, users databases, authentication, and access control would result in an estimated 54,180 hours per year. Even a 25% improvement in efficiency in this case would result in a savings of more than 13,500 hours.

Assuming the average government employee is paid $15 an hour, the immediate savings, based upon Meta Group's research, is $39,990 a day or $9,597,600 a year. Help desk savings, as noted above, run about $648,000 a year. The savings from the centralization and consolidation runs a conservative $202,500, using Meta Group's calculations at a 25% improvement in efficiency. Even reducing the sign on savings to 10% of the $9,597,600 figured on an annual basis, the ITS investment in IAMS results in a savings of more than $1,810,000 a year. A conservative return on investment, therefore, means that the state pays for the IAMS system in less than a year and a half.

Another measure for return on investment is the cost of a security breach because a user's credentials aren't terminated appropriately. In a competitive environment, the failure to

[3] Levinson, Meridith, "Who Goes There?" CIO Magazine December 2002.
http://www.cio.com/archive/120102/et_article_content.html
[4] Byrnes, Christian. "Who Goes There?" Optimize Magazine. October 2002.
http://www.optimizemag.com/issue/012/roi.htm

terminate a vendor's access to an agency's calendar system after his work is completed, for example, could give rise to that vendor gleaning agency activities with regard to possible contracts and negotiations. The access, in turn, could give that vendor an unfair competitive advantage – all because a simple application was overlooked when the agency terminated the vendor's access to its system. With IAMS, the access would have been terminated for all applications – in one simple step.