



CASE STUDY

Client: Company name available on request
Industry: Government Organization/Insurance Services
Solution: AnyWare Group Engineering Team Experience

Business Challenge:
Organization required 2 different user authentication options be offered to users when logging into the ROAM portal.

BACKGROUND

As organizations move their business processes to the Internet to give employees, customers and partners greater access to information, they need to protect themselves from security risks. This is particularly true of organizations that work with their clients' private information – like health and financial records. In order to access private information, a username and password must be used. Commonly, lists of users and their passwords are stored on the company Intranet in a secure directory (e.g., Active Directory).

Headquartered in Central Canada, an injury and disability insurance organization turned to ROAM for remote access. Employees and partners of the organization interact with the private information of their clients and the company must ensure the privacy of their clients. The organization planned to provide authorized employees with remote access to network resources.

CHALLENGE

With the use of a public-key encryption (SSL VPN), an organization can allow authorized users to remotely access secure data – a process that circumvents the need to install proprietary encryption software in each machine, but which naturally requires its own directory of usernames and passwords.

This insurance organization wanted a reliable, simple and highly secure means of verifying a user's identity before granting access to network resources.

In order to meet this requirement internally, the organization's IT manage-

ment concluded that they needed to setup two different levels of authentication. The first based on the existing Active Directory server for users who access one level of information. But, the organization also had a second level of user who would access network resources using a higher level of authentication controlled by an RSA Server and a small, portable, RSA "token," similar to a key fob. This token displays an authentication code at fixed intervals based on the built-in clock and the card's factory-encoded random key (the "seed"). The seed is different for each token, and is stored on the RSA server.

After thoroughly researching the available solutions for remote access, the organization chose to avoid the capital costs and overhead (hardware, licensing, training and manpower) associated with a do-it-yourself remote access solution. They concluded that AnyWare Group Inc.'s ROAM Platform made more business sense. ROAM (Role Oriented Access Management) is a managed service, that reduces the cost of remote access through shared infrastructure and does not require any software licenses or capital expenditures.

The insurance organization had one requirement that was unique to their ROAM installation – the login page leading to the personalized ROAM portal had to offer two authentication options. Users were to be given the choice between simply providing a username and password (which would be authenticated by the Active Directory server) – or – read their personal hand-held token display and enter ROAM using RSA server authentication.

SOLUTION

The company's Network and Systems Infrastructure Specialist worked directly with AnyWare Group's team of engineers to work out a method to integrate ROAM with the RSA Server.

"Several challenges were encountered and resolved along the way thanks to the team's persistence and hard work," said Joe Tilley, Customer Services Engineer at AnyWare Group. "Once integrated, a quick update to our portal servers presented end users with the choice of authentication mechanisms that the customer desired."

RESULTS

Particularly gratifying for the ROAM engineering team was this email from the infrastructure specialist in July, 2008:

"Sweet!!! You should see the big smile on my face. Thanks, man! You guys are the best."

Over time, the RSA server method proved so effective that the insurance organization adopted it for all remote access users.

"This solution can now be used with other ROAM customers as well," says Tilley. "Without the need to repeat the research and development this particular customer required."