CAT OTP Implementation

Westforce Credit Union Case Study

Internet Banking Implementation

Mega AS Consulting Ltd.
P.O.Box 55227, Mission Bay, Auckland, New Zealand
Tel: +44 7972 111149
E-mail: sales@megaas.co.nz support@megaas.co.nz WWW: http://www.megaas.co.nz /

Background

The Westforce Credit Union is a financial mutual co-operative registered as a credit union under the Friendly Societies and Credit Unions Act 1982 ("Act"). The objects of the Credit Union are essentially the promotion of thrift amongst its members by the accumulation of their savings, the use and control of the members' savings for their mutual benefit and the training and education of the members in the wise use of money and in the management of their financial affairs .

The Credit Union's primary activity over the past five years has been to provide a co-operative savings facility for members, through the issue of shares, to form a loan fund.

The Westforce Credit Union was created in 1981. At the beginning of 2005 Westforce Credit Union had a membership of 7600+ and serves Members from North Cape to the Bombay hills. The potential for further growth in this area proves a big challenge, but certainly not an insurmountable one. With the technology and resources available, Westforce Credit Union is realising that getting from it's inception to today is but a small step compared to the whole journey before us.

Problem Being Addressed

Westforce have been using RSA hardware tokens to secure the internal network and remote access via VPN. The tokens were distributed to VIPs in the organization and few customers. Westforce could not deploy the strong authentication to a wider range of users due to the costs involved.

Westforce have had a history of problems with the implementation of the RSA tokens. In addition, Westforce had a requirement to increase the number of used tokens which proved to be an expensive venture taking into account the number of hardware tokens and their costs.

With these concerns Westforce started looking for alternatives.

The Approach Taken

Westforce looked at the available options in the New Zealand market. They have learned from the ASB experience with the SMS based authentication, that using SMS as an alternative was again a costly venture as there are hidden costs and at the same time the SMS mechanism is not stable and does not ensure that the user will get the SMS and on time. SMS was also deemed insecure as it was exposed when going through third party providers (the telcos)

It was recognized that the market standard for strong authentication is - TFA OTP tools. A list of requirements was prepared based on the immediate needs and projected growth plans.

The requirements were:

- Integration with the existing Intranet infrastructure
- TFA OTP token with time based algorithm to reduce the "phishing" risk
- Take into account possible extension of the security to other areas such as additional servers and services
- Ease of use
- Costs, Hidden Costs
- Tokens Management overheads
- Support
- Maintenance and tokens replacement
- Ability to customize
- Conducting a Pilot

The CAT was one of the options in the market that ranked high at the requirements list. But the final decision was made after the product had a pilot at Westforce.

The CAT fitted into the infrastructure with its Radius support. Once installed, the system was running without a problem.

During the pilot Westforce raised few requirements to the CAT development team, such as stronger integration with the Windows Server Services. These requirements were addressed promptly and included in the next release of the product. Westforce was able to finalize its decision after using the CAT during the pilot with all its functionality.

Benefits

Once the final selection was done, Westforce had immediate benefits and a change of paradigm. Westforce could now plan for a wider deployment of strong authentication.

The immediate benefits included:

- Affordable Strong Authentication. With the CAT tokens used deployed for free, and no management and deployment costs, Westforce could now increase the number of tokens used.
- The past problems that used to occur with the RSA tokens have gone. The new CAT system merged into the existing infrastructure with its Radius support and was immediately fully operational.
- As with most enterprises, Westforce paradigm was that delivering strong authentication to its thousands of users would be a costly and almost impossible. With the CAT, that paradigm was gone. Now, Westforce realized that they could plan for deployment of strong authentication to ALL their users and not just the few VIPs. That is perceived as a strong competitive point in an aggressive banking and loans market.

Evidence of Success

Within a short time of using the CAT, Westforce have increased the number of users and extended the deployment of the CAT Authentication Server.

Initially, the CAT was used to protect the VPN. The next step was implementing the CAT as a strong authentication for the OWA at Westforce server.

Currently, Westforce are planning the deployment of CAT strong authentication to their Internet Banking services over the Internet.

Things We Would Do Differently

During the pilot stages, users were using the CAT to access the VPN from remote locations. While the CAT worked fine and produced the OTP, the users could not login until they realized that their Cellulars had not the correct time. Once the user adjusted the clock of the cellular to the correct local time, the OTP was accepted.

The conclusion was to follow the developers' advice and have the Server clock on the Login window. In addition, the users were made aware that they should keep their Cellulars' clock adjusted correctly to their local zonetime.