Customer Need
O’Neill needed to provide their remote workers with secure access to their corporate resources and sensitive data, in particular their designs and collections which are developed for up to 2 years prior to launch. O’Neill wanted to ensure that their staff had the flexibility to work remotely whilst enabling them to access key applications and intellectual property (designs, materials, production details, etc) securely, minimising the potential risk and financial loss from data breaches. O’Neill wanted to strengthen their security and to evaluate and purchase a range of authentication solutions that would meet both their current and future business needs. The solution needed to offer:

- **Flexibility**: A comprehensive and flexible authentication back-end solution that could support a broad range of authentication methods and advanced security applications.
- **Usability**: The ability to offer their employees a variety of different authentication methods based on their role in the organization.
- **Mobile Authentication**: The ability to offer strong authentication on smart phones and mobile devices
- **TCO**: The ability to streamline authentication operations using a cost-effective, low maintenance solution.

O’Neill has been a satisfied SafeNet customer for over 5 years having initially purchased 350 SafeNet authenticators for their remote workers. O’Neill has an extensive Citrix deployment, using their technology at the Gateway. They were advised by Citrix to evaluate SafeNet’s technology as the two solutions are easy to deploy and integrate, enabling O’Neill to extend and maximise their existing investment in Citrix – an important consideration as the chosen solution needed to be cost-effective and represent value for money. In addition, SafeNet’s ease of use and deployment was a key factor in the recent decision to evaluate the SMS Authentication solution, enabling O’Neill to deploy a strong combination of hardware and software authenticators.
Solution

After completing the technical evaluation, O’Neill selected the following SafeNet solutions:

- **SafeWord 2008** - an “out-of-the-box” OTP two-factor authentication solution that provides secure remote access to sensitive data and confidential resources. Offering both hardware and software, and supported by user-friendly management software and maintenance tools, SafeWord 2008 all-in-one OTP authentication solutions are easy to install, use and manage.

- **MobilePASS** - a software-based two-factor authentication solution that generates OTP passcodes on users’ mobile phones. MobilePASS supports a broad range of mobile handsets, including iPhone, BlackBerry, Android, Java and Windows Mobile platforms.

O’Neill wanted to be able to keep control of their data and liked the idea of self-provisioning and token management from a single console. They chose SafeNet’s Authentication solutions based on:

- Flexibility and centralised management
- Ease of use, deployment and installation
- Low TCO and value for money

By implementing SafeNet solutions, O’Neill has been able to maximise their existing investment with Citrix whilst deploying a proven technology and scalable solution for future business needs.

Installation and implementation was very straightforward, taking only a few hours with minimal training. The solution has enabled O’Neill to enforce their corporate security policy more effectively as well as increasing security awareness amongst its employees. Feedback from users is very positive – the solutions are easy to use, require almost no maintenance and provide an extra layer of security.

SafeNet’s strong authentication solutions have provided a scalable platform that can extend into other parts of the business as the mobile workforce grows and the need for a “Buy Your Own Device” approach to IT increases.

Solution Benefits

- **Ease of Management**: SafeWord 2008 is recognized as the easiest solution to administer, manage and deploy for Windows environments. It installs in minutes, right out of the box, ensuring ease of use and deployment.

- **Support for multiple authentication methods**: Safe Word 2008’s support for hardware and software authentication solutions has enabled O’Neill to seamlessly extend its existing hardware-based solution to include software mobile solutions without having to change its authentication back end.

- **Support for multiple mobile clients**: MobilePASS supports a broad range of mobile clients including iOS, BlackBerry, Android, Java and Windows Mobile 7. This has enabled O’Neill to easily implement and centrally manage secure access in a heterogeneous end-point environment.

- **Simple installation and activation**: MobilePASS’s support for over-the-air installation and activation translated into an easy and fast deployment process

- **Convenience for employees**: MobilePASS for iPhone, iPad, tablets and other mobile devices offers convenience, flexibility and security when accessing sensitive data

- **Lower TCO**: SafeNet’s single server solution enables O’Neill to consolidate its authentication infrastructure in one platform. This, together with the fact that SafeWord is easy to maintain and requires no dedicated technical staff, has significantly reduced help desk calls and operational IT costs, ensuring a lower TCO.

- **Integrates with Microsoft Active Directory tools** to provide easy and intuitive administration

- **Ensures regulatory compliance**

“Innovation and technology are core values at the company. We’re constantly evaluating new technologies to help drive business efficiency whilst ensuring flexible working and secure remote access to sensitive data. Recent data breaches highlighted the need for a multi-layered approach to security with robust policies and strong authentication when accessing resources from mobile devices. The deployment of SafeWord 2008 and MobilePASS across the company was very straightforward and the ability to centrally manage our authentication solutions is essential in maintaining control of our data. With Citrix and SafeNet’s authentication platform we have a solid foundation and scalable solution for future secure remote access needs – we’re confident that our investment in these proven technologies will safeguard our business-critical data for many years to come.”

Peter Maljaars,
Global IT Service & Infrastructure Manager