



Overview

Country or Region: United Kingdom
Industry: Defence

Customer Profile

The Ministry of Defence (MOD) in the United Kingdom is responsible for homeland security, as well as promoting international peace and security.

Business Situation

The MOD wanted to give its military and civilian staff secure access to its line of business applications via the Internet starting with 10,000 people working in remote locations.

Solution

Microsoft® Gold Certified Partner Capgemini used Government Gateway to verify users and Microsoft Certified Partner Sapphire chose Microsoft Intelligent Application Gateway 2007 as security management

Benefits

- Expenses settled quickly
- Automation cuts costs
- Greater security
- Simple integration
- Consolidates information

Self-Service Online HR to Save MOD Millions of Pounds Over 10 Years

“Our remote staff now feel much more in touch. For example, the IAG expense claims that once took up to three weeks in some instances will be processed in just 24 hours.”

David Longhurst, an Adviser to the Chief Information Officer, Ministry of Defence

The U.K. Ministry of Defence (MOD) wanted to provide secure remote access to its line-of-business applications starting with 10,000 “orphaned users” who work remotely and had no means of accessing internal administrative services. MOD approached Capgemini and Microsoft® to examine the use of existing services and off-the-shelf products to deliver its Internet Access to Shared Services (IASS) project. Taking advantage of new technologies such as Intelligent Application Gateway 2007, Microsoft and Capgemini delivered a proof of concept in the Microsoft Technology Centre. Capgemini subsequently implemented IASS into the MOD Defence Electronic Commerce Service using the Government Gateway to check user identities before connecting them to the right HR system. The self-service HR system using Chip and PIN authentication will save taxpayers millions of pounds over the next decade.



“From the time we were confident that there might be a solution to security to the point when it went live was just a year,”

David Longhurst, an Adviser to the Chief Information Officer, Ministry of Defence

Situation

As one of the United Kingdom's largest government departments with 320,000 personnel including 40,000 reservists, the Ministry of Defence (MOD) is responsible for defending the country and promoting international peace and security. Of those, around 10,000 military and civilian staff work in remote locations where they cannot easily access MOD line-of-business applications, such as human resources (HR) systems.

David Longhurst, an Adviser to the Chief Information Officer at the MOD, says: “We wanted to bring all our military and civilian staff into the 21st century by changing from paper-based HR systems to an electronic service. The MOD, in line with all government departments, is under an obligation to the Treasury to achieve efficiency savings and secure best value for the taxpayer in any major procurement. In particular, managers saw that if expenses claims and more than 20 other routine HR processes were automated—by turning them into self-service functions—huge savings could be achieved over the long term. This was achieved several years ago, but we were left with around 10,000 staff who we regarded as “orphans” because they are unable to access our internal ‘self service HR systems from their place of work. Typically such staff are seconded to other government departments, to Industry, or are serving with other Defence departments overseas.

“For many of the ‘orphan’ staff, who were unable to access the internal electronic system prior to IASS the alternative was a paper-based form. This could take weeks to process and we needed additional employees in the HR organisation so we could dual run paper and electronic HR. Even processing an expenses claim could sometimes take weeks. In other instances, soldiers in the field or reservists on training might have to queue to use a single computer. We wanted to give all

of them secure access to the MOD systems from any industry or home based browser, from an Internet café, or even an i-Touch phone or personal digital assistant.”

As a result, in 2005 the MOD launched its Internet Access to Shared Service (IASS) project, which will eventually extend to all employees who need access to MOD corporate systems. However, the MOD knew it would take some time to find an acceptable solution for security and the IASS project had to offer its users a high level of security, without the expensive re-development of existing services in the back office. The aim is to give the user of an unsecured device access to services that are usually only available from a secure location inside the MOD's electronic boundary. “If you are accessing MOD services, it is imperative to provide a strong identity validation of that individual's right to access his or her personal information,” says Longhurst.

The project began to move forward in mid 2007 with a Microsoft® demonstration in October of that year. The service was switched on in October 2008. “From the time we were confident that there might be a solution to security to the point when it went live was just a year,” adds Longhurst.

Further economy requirements in line with the government's modernisation drive were for IASS to use commercial off-the-shelf (COTS) technology. The requirement was to access the HR systems without any change to the MOD's line-of-business applications. Longhurst adds: “To keep costs down, we wanted to reuse a lot of our information and needed a solution that would integrate easily with our existing IT assets. We wanted a context sensitive front end. This is to ensure that the same back office application is accessible internally and externally, but at the same time can exhibit slightly different behaviour without having to reconfigure it.

“Using the Government Gateway fitted well with the government shared service agenda, which encourages the reuse of one department’s capability by another to avoid buying duplicate solutions.”

David Longhurst, an Adviser to the Chief Information Officer, Ministry of Defence

This was achieved using the Microsoft Intelligent Application Gateway software, which provides security management through secure socket layer-based application access.”

Solution

Microsoft® Gold Certified Partner Capgemini worked jointly with Microsoft to design and implement IASS using the Government Gateway for authentication and the Microsoft Intelligent Application Gateway (IAG) 2007. It uses Active Directory® Federation Services on the resource side for identity management with Microsoft Internet Security and Acceleration Server 2006 as part of the firewall. A significant component—the card and user provisioning service—was designed by Microsoft Consulting Services (MCS), Avaleris, and Gemalto and was implemented by EDS Defence. Capgemini—the project leader—has been working since 2000 with the MOD on a managed services contract to provide and manage the Defence Electronic Commerce Service framework.

Cliff Evans, Vice President of Defence and ID Management, Capgemini, says: “We pride ourselves on our collaborative approach to complex projects and IASS was no exception. Capgemini ensured that all the parties involved in the integrated project team—including the Government Gateway, EDS, Microsoft, Avaleris, Gemalto and the MOD—worked together effectively to deliver an end-to-end solution.”

IASS provides an identity and access solution—designed by MCS together with Microsoft Partner Avaleris and implemented by EDS—that assures identities for government employees who need to access internal applications from anywhere at anytime. The identity management component—called the card and user provisioning service—provides an important component of the “defence in depth”

principle to protect the MOD’s networks while at the same time facilitating access to essential information. One-time password technology with strong two-factor authentication was selected over to avoid the need to change the software stack on remote computers.

The Government Gateway, which helps businesses, citizens and government employees, to communicate and transact with government departments electronically, is central to the solution as the independent authentication provider. It was considered particularly appropriate because the information is sensitive, requiring a high level of identity assurance, data protection, and filtering.

Longhurst says: “Using the Government Gateway fitted well with the government shared service agenda, which encourages the reuse of one department’s capability by another to avoid buying duplicate solutions. This was the reason why we used the Government Gateway—a Cabinet Office and Department of Work and Pensions facility—for user authentication rather than the MOD building one of its own.”

The Microsoft products used included Microsoft Identity Lifecycle Manager 2007 integrated with customised Gemalto .NET smartcards and Microsoft Identity Lifecycle Manager 2007 identity synchronisation. “The overall solution has many moving parts,” St John Williams, Head of Defence, Microsoft UK, notes, “and to de-risk the solution, Microsoft provided the resources of its Technology Centre in Reading and in less than six weeks, a small team of MCS Consultants working closely with MoD and partners had proved the end-to-end solution”.

Longhurst adds: “The experience for our staff will be similar to using an ID card as they would a credit card at a shop or restaurant.

“The EMV standard, smartcards, and the implementation model had been provided across Europe, but Microsoft offered a proof of concept for the Chip and PIN authentication, which gave us confidence to go ahead.”

David Longhurst, an Adviser to the Chief Information Officer, Ministry of Defence

Our people insert their Chip and PIN card into a portable standalone smartcard reader. The reader displays a dynamic password generated by the card chip. The password is valid for a single time when accessing the HR service via a Web portal. With this service, civilian and military staff can access numerous HR services anytime from anywhere.”

Support from Microsoft Partner Ecosystem

Microsoft approached Sapphire, Microsoft Trusted Security Advisor of the Year 2008, to provide several proof of concepts relating to the installation of the IAG within the MOD and various other government departments. Sapphire also provided technical advice, support, and guidance in relation to the IAG to the MOD People Pay and Pensions Agency and the newly formed Service Personnel and Veterans Agency.

Benefits

The MOD is commoditising Internet remote access to its HR systems for all its employees using secure Chip and PIN password access with authentication through the Government Gateway. The implementation is destined to save the MOD several millions pounds over the next decade once manual processes have been fully automated and made available online for self service by all MOD personnel and civilians. Staff will all benefit from having equal access to HR services wherever they are and nobody will feel disadvantaged or excluded.

Remote Worker Expense Claims Settled in 24 Hours Instead of Days or Weeks

The implementation will bring online self service for HR applications to 10,000 staff who currently do not have access to them. As a result, morale is destined to improve, especially for employees serving their country in remote locations cut off from home comforts.

Longhurst says: “There are many reasons why people operate outside the electronic boundaries of the MOD. It might be because they are seconded to another U.K. Ministry or working in another country’s MOD. Our remote staff now feel much more in touch. For example, the IAG expense claims that once took weeks in some instances will now be processed in just 24 hours. The internal processing is instant with payments made to staff by automatic bank transfer at the end of the working day.”

Automation Saves Taxpayers “Many Millions of Pounds” Over 10 Years

The MOD is responding to the Treasury’s challenge to dramatically improve its levels of efficiency and accessibility by modernising public services. The IASS project is a major contribution. Started in 2005 and live since October 2008, it is forecast to make significant savings over the next 10 years by automating once manual processes and cutting down the need for clerical workers.

Longhurst says: “With all our HR services now online, there will be savings in the back office which could amount to many millions of pounds over 10 years. The savings will far outweigh the cost of the implementation.”

Chip and PIN Authentication Provides Safe and Secure Service

At a time when identity theft is widespread and the press carries reports of lost personal data in the public sector, the MOD was looking for a cutting-edge solution to provide strong two-factor authentication. The solution needed to be built from COTS, with as little coding as possible, to build security-enforcing functions acceptable for defence networks.

Longhurst adds: “The EMV standard, smartcards, and the implementation model had been provided across Europe, but Microsoft offered a proof of concept for the

For More Information

For More Information

For further information about Microsoft products and services, please visit www.microsoft.com/uk

or call 0870 60 10 100*

For hearing impaired customers with a Minicom, contact: 0870 50 30 400*

*Lines are open 8am–6pm, Monday to Friday. Please note, numbers prefixed 0870 will be charged at national call rates. For details of national call rate charges, please contact your telecommunications provider.

For more information about Capgemini products and services, visit the Web site at: www.uk.capgemini.com

For more information about Sapphire products and services, visit the Web site at: www.sapphire.net

For more information about Ministry of Defence products and services, visit the Web site at: www.mod.uk

Chip and PIN authentication, which gave us confidence to go ahead.”

In addition, the U.K. E-Government programme with the Government Gateway authentication service provided an easy to use existing infrastructure and trust fabric without the need to create a custom-built framework for the MOD alone.

When users in remote locations access the MOD HR application the screen blanks out sensitive information known only to the user, such as his or her precise bank account number, so as to avoid any risk of the information being seen “over the shoulder.”

Microsoft Technology Integrates with Existing HR Systems

According to Evans, Capgemini carried out a critical review of the platform about 18 months before completion. “We looked at an alternative solution for comparison purposes, but it was too expensive and didn’t achieve anything more than the Microsoft technology,” he says.

Microsoft technology integrates easily with the existing MOD HR applications, which run on Oracle, and no changes to the applications have been necessary due to the low-cost re-useable elements in the solution. Longhurst

says: “Microsoft software works well with Oracle applications and that makes our operations more efficient so we have the best of both worlds.”

Consolidates Multiple Forms of Digital Identity

IAG ensures granular access control, authorisation, and deep content inspection from a broad range of devices and locations to a wide variety of line-of-business resources. The software consolidates many forms of digital identity, including SecureID, local building passes, and individual passes for service and civilian staff.

This is just one of the value-for-money aspects of the project. By using its Microsoft Enterprise Agreement for low-cost volume licensing of software, the MOD is also saving money on operating costs and is benefiting from an ongoing business partnership with Microsoft. Longhurst adds: “Our relationship with Microsoft is second to none.”

Microsoft Server Product Portfolio

For more information about the Microsoft server product portfolio, go to: www.microsoft.com/servers/default.mspix

Software and Services

■ Products

- Microsoft BizTalk Server 2006
- Microsoft Intelligent Application Gateway 2007
- Microsoft Identity Lifecycle Manager 2007

- Microsoft Internet Security and Acceleration Server 2006

■ Technologies

- Microsoft .NET Framework
- Microsoft Active Directory Federation Services