DIGITAL SECURITY INITIATIVE

CASE STUDY

Smart Card Alliance

Shell Group's info security initiatives center around 85,000 smart cards with PKI and single sign on

EXECUTIVE SUMMARY

In the winter of 1999, the Royal Dutch Shell Group (www.shell.com) looked at the high cost of ownership for their desktop environment and decided it was time for a change.

High total cost of ownership (TCO) for managing the IT environment motivated Shell to seek a new approach, one that would have a positive effect on the bottom line while also improving security. In addition, they required that their new approach be simple, user-friendly, and offer a clear path to e-business capabilities in the future.

The Hague-based energy corporation went to the Schlumberger Network Solutions Infosec group to see if they could deliver a global IT solution that utilized smart cards integrated into Windows 2000. The project definition required a solution that would eventually touch 85,000 Shell employees at 1,200 sites across 134 countries.

Shell wanted a unified security offering integrating physical, thin client and desktop access. Smart cards offered the best solution, allowing all of these services to be offered on one platform while providing the additional benefit of support for existing physical access systems.

At the same time, the Microsoft Windows 2000 platform provided smart card support in its native Public Key Infrastructure (PKI) offering an integrated single sign on (SSO) capability using Kerberos.

Through careful and thorough planning and commitment to consistent technologies, Shell has been successful in this technically and logistically complex undertaking.

Shell is on target to meet Shell's Group Infrastructure/Desktop project goal of reducing TCO by 50%.

PROJECT OVERVIEW

Faced with ever-escalating costs for password management, Royal Dutch Shell embarked upon a smart card project that would be an important component of their Group Infrastructure/Desktop (GID) initiative. The GID was tasked with, among other things, reducing the support costs for PCs. To reduce those costs, Shell looked to reduce password management costs which industry estimates at $100 per user per year. By adopting a variety of technologies, such as thin clients, smart cards and PKI, Shell hoped to reduce their desktop TCO by 50%.

Shell turned to Schlumberger's DeXa.Badge solution to help with Shell's smart card endeavors. This solution is integrated with the native security features found in the Windows 2000 platform. In addition, a thin client authentication solution and a user-friendly web-based card management system were developed. This unique system provides a low-cost, convenient and secure solution.

The smart cards and associated software represent a significant undertaking. Shell began the deployment in the beginning of 2001 and plans to complete the initial distribution of smart cards to 85,000 employees by the end of the first quarter, 2002.

PROJECT BACKGROUND

Operating Environment

The Shell environment is predominately Microsoft applications running on Compaq hardware. The Windows 2000 platform is the operating environment for both servers and desktops. Shell also deploys thin client technology using Citrix Metaframe technology.

Physical security is supported by a number of proximity sensor and mag-stripe technologies. All smart cards issued by Shell have at least one alternate technology integrated onto the card, making the smart card form factor an attractive one.

Decision Process

The driving factor within Shell was Total Cost of Ownership. Shell wanted to lower their IT costs by 50%, so decisions were made to standardize on Windows 2000, Compaq computing platforms, Citrix thin client solutions, and smart cards. Through a standard competitive bid process, Shell first awarded the project in the winter of 1999-2000. Work began in mid 2000, but by the end of the year, the project was not proceeding as anticipated. Shell then decided to change vendors and asked the Schlumberger Network Solution Infosec group to assume project ownership in the winter of 2000-2001.

Business Issues

As mentioned above, total cost of ownership was THE driving economic factor that led to the establishment of this initiative.

With the massive proliferation of networks, the Internet, thin clients and PCs, Shell faced a very fundamental problem: how to know who was really on their network. In the past this was managed with passwords, but at a cost of around $100 per user per year and the fact that passwords provide very little security in return, a new, cost effective solution was required. Smart cards can provide true, strong authentication of end-users. Manageability and security of both the network and physical environment is improved while costs are reduced and business opportunities are expanded. Smart cards can be used in ways passwords cannot—for example, they can be used to electronically sign and encrypt documents and email. Businesses can conduct legally binding business online and via email, without having to fax or courier documents back and forth. In many countries, such as the United States and all members of the EU, electronic signatures are as binding as handwritten ones. Shell utilizes this approach to authenticate their users, bring down support costs and leverage their investment in network equipment and IT personnel. Using one card, Shell employees will have physical access to their facilities, be able to log in to their network from any device (whether a Compaq PC or a thin client), and be able to sign and encrypt documents and email. Using the web-based card management system, those cards will be very easy for Shell and their employees to manage.

Shell is just one of many large firms looking to reduce support costs and bolster security by providing employees with smart cards for network access. When used as part of an infrastructure that incorporates public-key cryptography, smart cards can provide tamper-resistant storage for PIN codes, private keys, digital credentials, and other personal information. Companies can use PKI and smart cards to authenticate users requesting network access, to digitally sign and encrypt documents, and to achieve nonrepudiation. The card

itself can be used for physical access to the facilities as well as for a corporate badge, including photo ID. The Shell deployment initially supports the Win2K Logon facility, but the smart card form factor was chosen because of its ability to support the legacy applications that exist in a card form factor.

APPLICATION DESCRIPTION

The Shell program uses smart cards to provide physical access, network access and corporate ID all on one smart card. The cryptographic capabilities of the smart card are used to authenticate end users, digitally sign and encrypt documents and email, and provide nonrepudiation for digital transactions. The Shell solution works seamlessly with Microsoft Windows 2000 and with all major PKI vendors to provide flexibility in the design of their security platform. In addition, a user-friendly system provides card and digital credential management capabilities. The Shell solution provides smart card authentication to thin clients—a solution which is unique in the industry today. Shell employees will be able to roam the company, log in anywhere on any device, be authenticated and receive their proper level of authorization.

The Shell smart card platform utilizes:

- Smart cards - Cyberflex 16k and 32K Smart cards
- Readers – Keyboard (Available Jan 2002), PCMCIA, USB, Serial
- Schlumberger Self Service Module - User friendly, web based, card management system
- Schlumberger Virtual Channel solution - Allows thin client users to strongly authenticate via smart cards to thin client sessions.

Most companies use passwords for authentication, which, as previously described, are expensive and lack sufficient security. The solution deployed by Shell will vastly reduce password and helpdesk costs. Shell's deployment is also one of the largest Windows 2000 deployments in the world and also one of the largest private sector smart card deployments in the world. The smart card also provides an avenue to single sign-on, especially in a Windows 2000 environment. Shell found a number of single sign-on solutions available but these typically rely on passwords—which means that if the password is compromised, the intruder will have access to all applications. Single sign-on without smart cards is a risky proposition. Single sign-on with smart cards provides improved security and improved manageability while reducing helpdesk calls.

Deploying in the Workforce

Shell relies on Microsoft's Active Directory technology to identify candidates who will receive the Shell secure card. Coordinated activities ensure that targeted employees receive appropriate technology upgrades, specifically the smart card readers and/or computing platforms that can accept and work with smart card technology. End-user platforms are either equipped with new keyboards that contain a smart card reader, or are upgraded to newer equipment that have smart card reader support already integrated. Laptop computers are equipped with both PCMCIA and USB readers so end-users can have optimal speed when they are at home and PCMCIA connectivity when they are traveling.

IMPLEMENTATION OVERVIEW

Initial deployments of the smart card system began at Shell in April 2001. Smart cards were issued to

employees at the same time a global infrastructure upgrade was taking place. New servers, desktops, laptops, and thin client workstations were being deployed worldwide as the supporting infrastructure was rolled out. This large, coordinated, effort is expected to take about a year to complete.

The initial phase included the design and rollout of the fundamental infrastructure, platform upgrades, and smart card issuance. Subsequent phases of the deployment introduce enhanced functionality and expanded applicability, such as chaining and Unix support. Chaining is a technology that provides employees with authorized access to Citrix meta-frame servers located remotely via credentials passed through local servers.

By the fall of 2001, 53,000 smart cards are expected to be issued. By the spring of 2002, Shell expects to have deployed smart cards to all employees worldwide who require access to network computing resources.

PROGRAM MANAGEMENT AND SUPPORT

Shell and Schlumberger both contribute equally to the system development and deployment team structures. Overall project management comes out of Shell headquarters in the Hague, while day-to-day program management is performed by the Houston office of Shell Information Technology International.

Shell provides direct customer support through three help desk facilities deployed around the world. Shell provides all levels of support with Schlumberger on call for escalation support.

Shell provides the introduction and training to their end-users to ensure smooth deployment, use and continuing operations of the system.

Card Management System

For management of the cards themselves, Shell required a system that would allow end-users to manage their own credentials in a simple, error-resistant way. A new application called the Self Service Module, or SSM, provides this management function. The SSM, as its name implies, provides a very simple means by which Shell employees can initialize and manage the smart card and its contents right over the Web.

In the event a card is lost or stolen, employees call one of the global help desks and their lost card is rendered inoperative. The certificate will be revoked and physical access permissions turned off. Temporary cards allowing short-term access to logical and physical facilities will be issued until the employee can obtain new permanent credentials. The permanent digital credentials are loaded by employees themselves, following simple, Web-based directions.

COSTS BENEFIT ANALYSIS

Total Cost of Ownership was the initial motivating factor in coming to the decision to deploy the new desktop infrastructure, including the use of smart cards across the corporation. The specific goal was to lower TCO by as much as 50% - which would be partially achieved by replacing legacy userID/password technology with smart cards. While the project rollout is just crossing the halfway point, initial TCO reduction figures are extremely encouraging. Initial results indicate the 50% TCO reduction target will be met.

LESSONS LEARNED/RECOMMENDATIONS

Although the post mortem has yet to be conducted as the deployment is still in progress, initial man-

agement reaction to the program is extremely favorable. Early on, responsibilities and expectations were clearly identified and documented. Well-executed program and project management offices ensured that the business requirements of the Shell smart card project were met. Of course, ongoing and accurate communications were essential to managing change.

When Shell made the decision to deploy a Windows 2000 PKI, the date was 1999. For a technology decision of this extent to be made at that time meant that Shell had tremendous depth of knowledge for network infrastructures, security models, PKI, smart cards, physical security, and security management principals.

Programs such as the Shell smart card initiative will introduce fundamental change to the operating processes of a corporation. And perhaps this is the most important lesson to be learned from the success of this deployment; corporate commitment to comprehensive IT modernizations must be top-down, comprehensive, and driven by competence in understanding technology and the impact it has on the workforce.

This case study was developed by the Smart Card Alliance's Digital Security Initiative with the assistance of Martha Jones, Schlumberger, and Bryan Ichicawa.
For more information on this and other case studies or to obtain additional no-cost resources on the use of smart cards in digital security,
contact the Alliance at www.smartcardalliance.org; info@smartcardalliance.org.
