DIGITAL SECURITY INITIATIVE

CASE STUDY

Smart Card Alliance

Schlumberger deploys smart cards and PKI corporate-wide in effort to protect corporate and customer data

In 1999, Schlumberger Limited (www.slb.com) inaugurated a global initiative to deploy smart cards and PKI to its entire workforce. While a successful deployment would create a product and capabilities showcase for the corporation, Schlumberger's motivation soon turned pragmatic, and protecting vital corporate and customer information assets soon took over as the primary driving factor.

Schlumberger Limited is a global technology services company consisting of two segments, Schlumberger Oilfield Services and SchlumbergerSema. Schlumberger Oilfield Services, headquartered in Paris, is the leading provider of services, solutions and technology to the international petroleum industry.

SchlumbergerSema, with headquarters in New York, is a major IT services company providing information technology solutions to the telecommunications, utility, finance, transport and public sectors, and is the leading supplier of smart card technology. Schlumberger Limited acquired Sema plc in April 2001. Schlumberger employs 89,000 people in 160 countries around the world.

Schlumberger Network Solutions, a Schlumberger Oilfield Services division, not only plays a key role in the upstream oil and gas industry, but also provides network, network security and associated services to both internal and external customers. This organization was called upon to architect an information security infrastructure and issue smart cards to all PC users.

In 2000, Schlumberger Network Solutions (SNS) began to deploy the global PKI and rollout the first smart cards. Based upon an Entrust Authority‰ PKI and Entrust Entelligence‰ security layer, the initial deployment encountered obstacles that made the SNS organization rethink their deployment strategy. The lack of platform uniformity for both hardware and OS coupled with the high cost of upgrading individual PCs to enable the smart cards and PKI began to raise costs to unacceptable levels. Additionally, a corporate-wide rollout to upgrade and standardize PC and server platforms was just beginning.

With a new PC platform strategy in place, coordinated with the smart card and PKI initiative, the corporate rollout restarted in the spring of 2001. The new plan has increased deployment output from 500 per month to 3000 per month. In 2002, the rollout is expected to be complete for Schlumberger Oilfield Services. SchlumbergerSema plans to complete their rollout once their IT-infrastructure integration and PC-platform upgrade programs are complete.

PROJECT OVERVIEW

The original drive for the Schlumberger smart card project was to create a technology showcase that demonstrated the feasibility of utilizing smart cards in a global corporate security infrastructure. With real world requirements for protecting Schlumberger corporate and customer information assets growing, the showcase rationale soon changed.

Schlumberger processes tremendous amounts of customer data. The oilfield operations generate large volumes or proprietary information, card operations manage extremely sensitive card personalization data, and the newly acquired Sema organization processes critical billing information. Schlumberger itself is a technology driven company, with over 700 sites worldwide, operating a global IP based network and several Extranets. Protection of business information and managing access to networked computing resources became a top priority.

The project initiation occurred in 1999, and the R&D effort lasted into the year 2000. The Schlumberger smart card project was an interesting deployment as the customer and the provider were both the same company. The decision to pursue such a complex and large undertaking was made at the highest corporate levels, and the Network Solutions organization became the provider organization, delivering technology, program management, training, and corporate policy support into Schlumberger corporate entities.

OPERATING ENVIRONMENT

Schlumberger Limited employs 89,000 employees in 160 countries around the world. They occupy more than 200 facilities and 400 office locations worldwide. Until standardization efforts took effect, computing platforms reflected a wide variety of vendors and operating systems.

Access to the Schlumberger network was conducted via remote dial-up processes secured primarily by userID/password systems. Help desk costs for managing the userID/password systems were significant and cost reduction became a significant issue. Smart card technology had not been used for logical access to any Schlumberger network resource.

Building access was based mostly upon old magnetic stripe technology. Simple swipe readers were installed at individual entry/exit locations. The exception was access to bankcard manufacturing facilities, where stringent security requirements were implemented to obtain certification by financial institutions.

A worldwide directory (LDAP), accessible by all employees through a browser or e-mail client provided contact information for all employees worldwide.

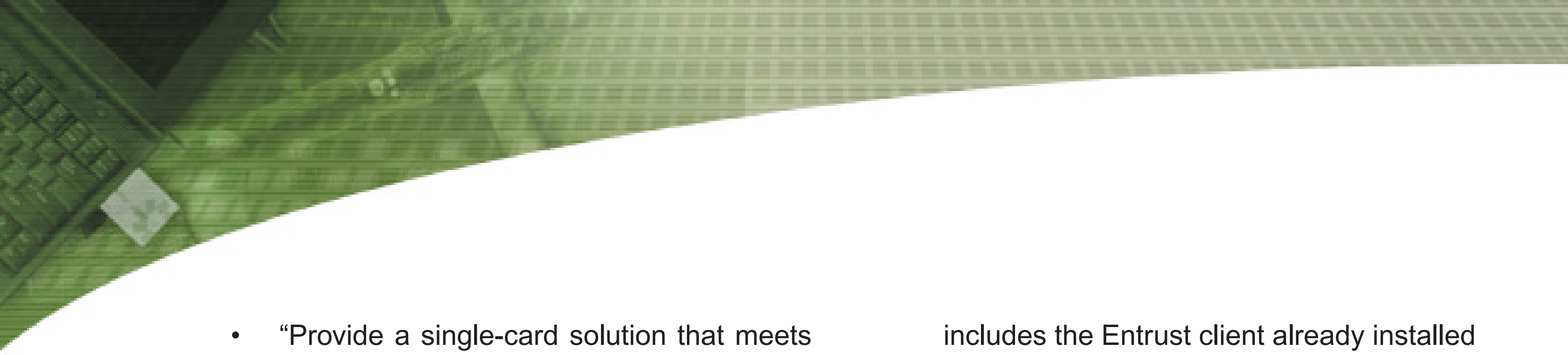
Schlumberger operates one of the largest private networks worldwide. The ability to leverage this network to provide significant cost savings through integration of new technologies and services was to become a cornerstone accomplishment for the Schlumberger Network Solutions Group.

OBJECTIVES

Schlumberger recognized that the Internet and mobile services were vital tools in empowering employees with the ability to remain in communication with customers and fellow employees when on travel. Additionally, Schlumberger employees are often in remote locations to support customers on a local basis. In these cases Schlumberger corporate offices are not centrally located, however, the employees still need to access the corporate network to continue the flow and management of critical information.

The primary objectives for the Schlumberger smart card project were:

- “To provide a solution that allows for secured access to physical locations and logical access to corporate networks and critical corporation information while ensuring no interruption to current operations”.



- “Provide a single-card solution that meets the overall smart card-based PKI and Corporate Badge objectives”

APPLICATION DESCRIPTION

The Schlumberger smart card project integrated legacy physical access technology and PKI based authentication technology onto a single card platform and deployed the cards in concert with a corporate-wide venture to standardize PC platforms. In addition, new business processes required guidance for use, and thus “usage standards” were created and communicated to employees. These usage standards defined the circumstances under which information was to be encrypted or emails were to be signed

Schlumberger developed a relationship with one of the largest PC manufacturers to develop a “Schlumberger specific” PC configuration. The PC configuration, includes the following components:

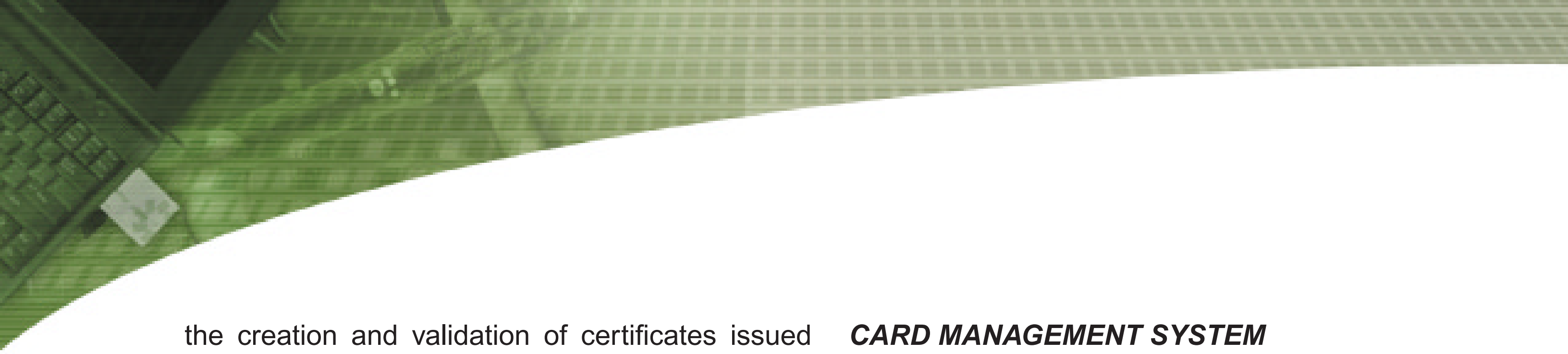
- Windows 2000 OS
- Smart Card Reader – Laptop users receive with their PC an integrated PCMCIA smart card reader. Desktop users receive either a serial or USB compatible smart card reader.
- PKCS#11 software module: provides smart card integration with Netscape browsers and the Entrust software.
- CSP (Cryptographic Service Provider): provides smart card integration with Microsoft Applications (built into Microsoft Windows 2000)
- Entrust Secure Desktop Client software (Entelligence): Schlumberger chose the Entrust PKI solution. Each PC that ships with the Schlumberger configuration includes the Entrust client already installed on the employee PC The Client software provides Windows Sign-on, seamless integration of PKI in e-mail and browsers, encrypted folders, and functions for creating and managing PKI certificates.
- Checkpoint VPN client - The VPN solution provides smart card based authentication for a highly secure yet cost-effective support for telecommuters or employees based in customer premises needing access to the Schlumberger Network.

Computing platforms configured to a corporate standard would ease the level of interaction with support organizations. The upgrade task to bring legacy desktops to the required standards was extremely expensive in materials and time.

The Schlumberger network was also required to meet several objectives to support the smart card project. SNS established an integrated LDAP directory solution as a managed service. The LDAP directory provides worldwide access to employee information, including office phone numbers, e-mail address, office location and other pertinent information.

The SNS project team integrated the Entrust Profile Manager with Schlumberger’s current worldwide LDAP directory. At the time of badge issuance, employee digital credentials were generated and loaded onto the smart card. The employee’s public certificate information was loaded into the LDAP directory for access by other Schlumberger employees and business associates worldwide.

Schlumberger chose to leverage its existing private network infrastructure for hosting the server requirements for this implementation. Schlumberger implemented a “secure room environment” at one main location as well as establishing two redundant facilities. The “secure room” includes a vault that contains the CA/RA based services for



the creation and validation of certificates issued to employees. The vault may only be accessed by select individuals who must use a combination of smart card and biometric technologies.

SMART CARD TECHNOLOGY

Schlumberger selected the Mifare technology for fulfilling the requirements for physical access security. This technology integrated with the Schlumberger Cryptoflex‰ and Schlumberger Cyberflex‰ smart card platform, deployed on high quality plastic that was able to support post card issuance printing. The encoding of the Mifare cards was defined and implemented as a Schlumberger Corporate Standard.

PHYSICAL ACCESS READER TECHNOLOGY

Schlumberger developed a relationship with several suppliers (IOLAN in the USA, Custom Group in the UK) for sourcing contactless readers compatible with the Corporate Standard. These readers interface with the Physical Access control systems using “industry standard” protocols. The reader “translates” the Mifare communication to the “Wiegand format”, for example, sending the appropriate message back to the physical access software tracking the user and their authorization for entry. The readers are able to withstand exposure to inclement weather conditions.

ACCESS CONTROL SYSTEM BACK-END

Large varieties of Physical Access Management systems were in place within Schlumberger. In many instances, these systems were upgraded for the new corporate badge by exchanging the reader modules only. For new sites implementing Physical Security Systems a list of approved suppliers with demonstrated ability to address the Corporate Badge is maintained centrally.

CARD MANAGEMENT SYSTEM

The card management system (CMS) that Schlumberger deployed was a functional subset of their production CMS product. Issuance processes were changed to ensure cards were never out of employee’s immediate control once the cryptographic keys were generated. The CMS was adapted to allow multiple printing stations to interact with the back office system. In addition, interfaces that allow existing Physical Access systems to interact with the CMS and the LDAP directory are being implemented to provide global control over Access control badges

IMPLEMENTATION OVERVIEW

Initial deployments for the Schlumberger smart card system took place while a corporate-wide PC upgrade campaign was about to start. At first, qualified IT personnel would spend at least 30 minutes at employee workstations upgrading the existing systems to be able to accept and utilize smart cards. They installed smart card readers, hardware drivers, middleware, and client software.

Schlumberger realized that this time spent on a computer that was soon to be replaced was incurring tremendous cost, and the initial rollout was delayed until it could be combined with the PC upgrade campaign. The coordinated effort created immediate benefit as end-user platforms no longer required upgrading. They were smart card and PKI ready coming out of the box.

Web based support tools were developed to facilitate the enrollment and scheduling of PKI deployments at a site. The employees would submit a photograph that triggered the sending of the employee smart card to the local registration authority. Employees would be required to present formal identification in order to receive their cards, and would immediately initiate the process to generate their digital identities via an online system.

An extensive training program was required to support the many groups affected by this deployment. A management-training course was designed to create awareness at the top levels. The management teams needed to fully comprehend the impact and benefits of usage of the new corporate security technologies. They also needed to understand how and when to apply this technology and guide their employees in its proper use. The SNS global help desk organization needed to learn about all aspects of the system. They would become the first level of support the rest of the corporation would go to for questions and problem resolution. Local support organizations responsible for level 2 support would also require extensive training. Security guidelines were written to provide the necessary usage standards. Finally, end user training provided employees with the details regarding enrollment, usage, procedures for lost/stolen cards, etc. There was also an Entrust computer-based training module installed on every employees PC, enabling end users to access an immediate source of assistance right at their desk.

Support was obtained through the existing global help desk. Additional support was available through self-help dialogues available on the PKI web pages

PROGRAM MANAGEMENT

Program management for the entire project was managed by Schlumberger Network Solutions. The SNS program management team was assisted by peer employees at the serviced locations. The customer-side program managers would be able to provide more direct workforce assistance, and help increase the communication channels necessary for success.

Global project management was reduced from six regions to three; North and South America, Europe and Africa, and the Middle East and Asia.

COST BENEFIT ANALYSIS

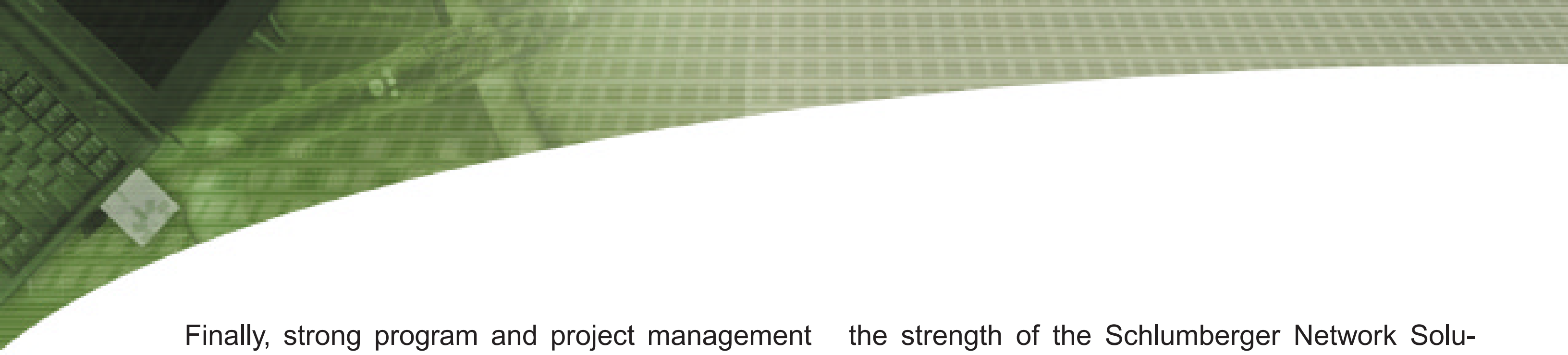
The Schlumberger smart card program is still in the process of being deployed. At the time of this writing, the cost benefit analysis had not yet been formally conducted. It was mentioned that a significant cost benefit component was security – or perhaps awareness. The awareness of the cost associated with a corporate information security breach, estimated at approximately $15M, provides an immediate recognition of the benefits such a program can deliver.

Another unqualified benefit was reduced help desk costs. The high cost of password support will easily be reduced through deployment of the smart card system with a Win2K logon or single sign-on solution.

LESSONS LEARNED / RECOMMENDATIONS

While the Schlumberger smart card project is still in its rollout phase, several points have already crystallized. Instead of lessons learned, perhaps lessons confirmed is a more appropriate term, for the commitment that was received from the highest levels of management. Without the corporate dedication to success, complex and capital-extensive programs such as this would be destined for failure.

A consistent and long-term platform strategy was also a key factor contributing to the success enjoyed thus far in the deployment cycle. The early deployment cycle was hampered, even slowed, by the lack of uniformity in platforms subject to the rollout schedule. This plan did not only address personal computing platforms, but also defined server, back office, OS, and network guidelines that would be followed for years ahead.



Finally, strong program and project management disciplines contribute heavily to the ongoing success of the program. Clear objectives, well-defined responsibilities, and well-managed expectations supported by strong communications are perhaps the strength of the Schlumberger Network Solutions team. The evidence can be seen by the success in the deployment of this large and ambitious project.

This case study was developed by the Smart Card Alliance's Digital Security Initiative
with the assistance of Matt Radcliffe, 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.