Smart Card Alliance

Smart Card Case Studies and Implementation Profiles

A Smart Card Alliance Report

Publication Date: December 2003

Publication Number: SC-03005

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 1-800-556-6828

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, health care, retail and entertainment industries, as well as a number of government agencies. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. For more information, visit **www.smartcardalliance.org**.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Smart Card Alliance members: Members can access all Smart Card Alliance reports at no charge. Please consult the member login section of the Smart Card Alliance web site for information on member reproduction and distribution rights.

Government agencies: Government employees may request free copies of this report by contacting info@smartcardalliance.org or by joining the Smart Card Alliance as a Government Member.

Table of Contents

Introduction

Organizations worldwide are increasingly using smart cards in secure identification (ID), retail, financial, transit, health care, telecommunications and other applications. The Smart Card Alliance has developed case studies and profiles of successful smart card implementations and compiled them in this report.

Enterprises and government organizations are implementing new or upgraded ID systems to improve the accuracy of individual identity verification and to add new capabilities that will improve the ID system's security, functionality, or convenience. Smart cards are increasingly being used in new ID systems and accepted as the credential of choice for securely controlling physical and logical access. Included in this report are case studies or profiles of the following smart ID card implementations:

- California Independent System Operator
- Federal Deposit Insurance Corporation
- National Aeronautics and Space Administration Smart Card Project
- Rabobank
- Schlumberger
- Shell Group
- Sun Microsystems Java Badge
- Transportation Security Administration Transportation Workers Identification Credential (TWIC)
- U.S. Department of Defense Common Access Card
- U.S. Department of Homeland Security Identification and Credentialing Card
- U.S. Department of State Access Control Smart Card Implementation Project
- U.S. Navy DENCAS

Health care organizations are actively looking for ways to lower administrative costs, increase security and make their information systems easier to use. "Smart" health cards can be used to support HIPAA compliance, increase security, simplify system access and deliver new clinical and administrative benefits. Included in this report are profiles of the following smart health card implementations:

- French Sesam Vitale Health Card
- German Health Care Card
- Mississippi Baptist Health Systems
- Taiwan Health Care Smart Card Project
- University of Pittsburgh Medical Center

The **financial and retail industries** are all abuzz over the latest payment trend - contactless payment devices. Included in this report are profiles of the following contactless retail payment implementations:

- American Express ExpressPay
- MasterCard PayPass
- Visa Contactless Payment in South Korea

Mass transit agencies have been using stored value, pre-paid cards for electronic ticketing since the 1970's. Through the 1990's this market steadily began transitioning from magnetic stripe technology to contactless smart cards. Today, virtually all new transit fare payment systems either in the delivery or procurement stages involve the use of contactless smart cards as the primary ticket media. Already, major deployments are up and operational in a variety of cities worldwide, including Hong Kong, Seoul, Pusan, Washington D.C., and Shanghai. Many of these transit deployments are also planning to use the same contactless smart payment card across multiple modes of transportation in a region and with retailers who could benefit from fast, convenient contactless payment. Included in this report are profiles of the following transit smart card implementations:

- Hong Kong Octopus Card
- London Oyster Card
- San Francisco Bay Area TransLink
- Ventura County Transit Smart Card
- Washington Metropolitan Area Transit Authority – SmarTrip

Enterprise and Government Case Studies and Profiles

California Independent System Operator[1]

In 1996, California lawmakers enacted historic legislation allowing consumers to choose their energy suppliers in order to create a competitive marketplace for public utilities. The California Legislature conceived the not-for-profit, public benefit organization, the California Independent System Operator (California ISO), to manage the power transmission grid and to facilitate markets for electricity reliability products. Created by PG&E, Union Gas and Electric, and Southern California Edison, the California ISO is the "air traffic controller" of the electrical grid. They oversee the path, routing and sale of energy across 80 percent of the grid of California.

The power grid, a transmission system made up of high-voltage power lines, delivers enough power to serve the annual energy needs of over 30 million current customers of investor-owned utilities. In addition, the grid will transport significant amounts of power for others in the region.

In 1996 the California ISO created a specialized team whose task was to define their information security requirements. The resulting plan was required in order to satisfy federally mandated tariffs that defined the business requirements regarding a public key infrastructure (PKI) deployment. The Cryptographic Universal Design Architecture (CUDA-ISO™) team was created. The CUDA-ISO team spent two years of research, due diligence, policy development, and security architecture development before the deployment of the PKI and smart cards began. By 1998, the overall security architecture, PKI policy and practice statements, subscriber requirements, and subscriber education and training deliverables were complete.

To deploy their newly defined security plan, California ISO chose SPYRUS Inc. to provide the PKI, Rosetta™ smart cards, and the LYNKS™ high assurance cryptographic tokens to satisfy these information security requirements. In the spring of 1999, the California ISO began to deploy their PKI and issue smart cards to their user base, with nearly 2000 California ISO smart cards issued by mid-2001.

Project Overview

The California ISO was created to monitor power generation facilities, manage the transmission grid, manage the buying and selling of electricity, and provide the e-business framework necessary to ensure commercial equity across business areas. A specialized organization was created and chartered with architecting, developing and deploying a secure information framework that could accommodate the varying levels in information assurance required to operate the diverse components of their business.

Energy systems are a National Critical Infrastructure component, and the development of a comprehensive security package for protection of physical

[1] This case study, published in April 2002, was developed by the Smart Card Alliance Digital Security Initiative with the assistance of Bryan Ichikawa and SPYRUS Inc. Rosetta™ and LYNKS™ are trademarks of SPYRUS Inc. CUDA-ISO™ is a trademark of the California Independent System Operator.

and logical assets is essential. California ISO assembled a team to implement the network's firewall security and to plan security for the network's eventual move from a dedicated private network to the Internet. During the next 15 months, the CUDA-ISO team developed criteria, selected vendors, and began to deploy a master security solution across the California ISO network.

The California ISO security solution had to have open standards and be non-proprietary. The CUDA-ISO team identified confidentiality, ease of use, scalability, and a life expectancy of at least ten years as the essential system requirements. Confidentiality was vital because unauthorized access to privileged trading information could give an unfair advantage to energy auction participants. Ease of use was essential to California ISO's many and diverse clients, including utility, generator and transmission companies and energy traders. Scalability of the online security system was essential to accommodate additional electrical generating plants and traders over time.

Charged with managing the power transmission grid and coordinating the flow of electricity throughout the state, California ISO quickly recognized its critical need for a high-assurance security infrastructure. The California ISO system is currently operational across a number of different applications. High-assurance applications, including power generation, use high capacity PCMCIA hardware tokens; medium assurance applications, such as secure scheduling and dispatch operations, use smart cards; and basic assurance services, including invoice submission, use browser software certificates. This combination of secure tokens is utilized to provide a robust and comprehensive security solution.

California ISO began to deploy their PKI infrastructure and issue end user smart cards in March 1999.

Project Background

When the California energy market was broken up and the California ISO created, a "clean slate" was provided on which to create a new operating environment. State-of-the-art technology was selected to satisfy the many requirements defined by several factors. Newly defined tariffs defined rules for information confidentiality, liability, indemnification, and dispute resolution. Existing control networks were predominantly leased line networks, and the move to open network standards would result in significant costs savings. There was the need to remove barriers to market participants. If future trading of transmission rights were to include different players, those organizations would have had to install dedicated lines connecting them to the California ISO networks. These tremendous barriers to participation would need to be resolved by implementing a secure system that could provide highly secure, authenticated access.

Application Description

When California ISO became operational, the network consisted of a statewide virtual private network (VPN) that ran Internet Protocol (IP) over dedicated lease lines. California ISO assembled a team to implement the network's firewall security and to plan security for the network's eventual move from a dedicated private network to the Internet, which would lower costs and allow for easier system expansion. To reduce the cost of expensive dedicated leased lines, California ISO wanted to use the Internet wherever feasible.

The California ISO PKI deployment supports multiple levels of assurance. The high assurance system operates the power generation and transmission grid facilities. These systems use a high assurance PCMCIA token to support the cryptographic functions. The medium assurance systems support the various trading and metering applications, and use smart cards. Basic assurance systems use software certificates to manage basic information flows.

In enabling business to operate in open network environments, the power entity successfully implemented a number of secure e-business applications, including the following:

Online trading. Over an extended Internet/extranet network, buyers and sellers of power are authenticated using software certificates before being allowed to access an online auction of transmission rights.

Online power generation control. This service is secured through the use of high-assurance LYNKS™ Privacy Cards.

Online meter access. Access is secured while enabling online meter access by third parties of the kilowatts supplied to customers throughout the transmission system.

Online invoicing submission. Access is secured using a web-based certificate.

Online problem management. Smart cards are used to secure remote access while tracking problem resolution quickly and efficiently. More than 500 California ISO users also use smart cards to secure online network load balancing, supporting real-time power trading services to cover spot imbalances of power.

Scheduling notification. Another smart card-based application, scheduling notification automatically alerts electric generation facilities to outstanding bids to purchase energy and prompts them to respond to the request. By responding, the facility commits to produce a specific number of kilowatts of electricity. This step guarantees that electric generation plants across the state have the opportunity to compete fairly in the open market.

Around California, more than 800 scheduling coordinators use their smart cards to conduct transactions with the California ISO. The CUDA-ISO team implemented an Internet-enabled application that allows participants to securely manage the bid submission process online.

All of the applications are securely managed by the PKI, composed of four certification authorities (CAs) and two registration authorities (RAs), with additional expansion planned at all levels within the network. The smart cards deployed in the California ISO system are SPYRUS Rosetta smart cards. These cards are 16K crypto-controller smart cards running the SPYRUS SPYCOS™ chip operating system. These highly secure smart cards have received the Federal Information Processing Standard (FIPS) Level 2 certification, representing the highest possible security level available for smart cards today.

Implementation Overview

In 1997, California ISO began to construct a private ATM network secured with state-of-the-art firewall technology. This network would provide the backbone upon which all California ISO business would be conducted. Authentication was to the network, and once an end user gained access to the network, all resources became available. All of the newly developed energy management systems and marketing databases would tie control of the grid to the market, and all of these systems operated on a single private line network.

By 1998, once the initial backbone was in place and operational, California ISO began the task of conceptualizing a new approach that would support higher levels of security, reduce network costs significantly, and be able to scale in functional capability as well as numbers of users supported. In addition, criteria for the new capabilities had to follow open standards, be non-proprietary, and sustain long life spans.

An RFI was issued to collect input, and the decision that followed reflected that a PKI would be the only solution that could meet all of the requirements. Multiple RFPs and RFQs were issued, and the final team selection process occurred in January of 1999.

The CUDA-ISO team managed the entire process. Final partner selection resulted in SPYRUS providing the PKI and hardware tokens, with SAIC selected to be the integrator. By March of 1999, work to build the California ISO PKI had begun, and within six months, three certification authorities running separate policies had been created and smart cards were being issued to end users. The CUDA-ISO team created a fourth certification authority, allowing them to test new security releases before releasing them to the field.

Program Management and Support

The California ISO deployment was managed entirely by internal resources. SAIC provided the development and integration support services necessary to bring the applications online. A client support services organization was created within California ISO to provide the help desk, trouble ticket generator, and problem management functions. The Remedy database provided a web-based tool that was accessible by end users who, by using their smart card, could track the status of disputes, network connectivity issues, or any other network, user, or business issue involving the new California ISO systems. Training was provided by internal organizations and web-based information systems supplied additional reference data to end users.

Smart card issuance involved in-person registration authorities that performed the checks necessary to ensure the identity of the recipients of the digital credentials. In the event a card was lost or stolen, certificate revocation and credential (smart card) re-issuance processes ensured that work flow disruption was kept to a minimum.

Cost/Benefit Analysis

It is a gigantic task for California ISO to securely manage the generation and sale of $50 to $100 million of electrical energy each day. From its headquarters in Folsom, near Sacramento, California ISO's automated command and control network regulates the generation and metering of power from remote generators located throughout California.

The CUDA-ISO team's initial efforts concentrated on defining California ISO's security architecture and application requirements and then implementing a VPN with proxy management. The flexibility of the deployed security policy has enabled California ISO to develop and deploy network applications rapidly. All future California ISO applications must conform to CUDA-ISO specifications and will migrate to the new security policy.

The CUDA-ISO team at California ISO has successfully deployed a PKI infrastructure solution into a pre-existing critical infrastructure, enabling the organization to offer a broad range of services and add levels of security not previously available to the energy industry in California or anywhere else in the world.

E-business is a reality in today's marketplace. California ISO entered this new environment with the highest level of confidence, knowing that their mission-critical transactions would be tightly secured. Not only did the California ISO eliminate security concerns in a cost-effective manner, the solution also allowed them to implement innovative e-business applications that reduced operational costs.

The cost/benefit analysis would reflect that the deployed solution was the only viable alternative that would provide the necessary framework for network, information, and transaction security. In the end, California ISO realized significant savings through reduction of California ISO's dependence upon dedicated private line networks. In addition, the successful deployment of the PKI and smart cards allowed the CUDA-ISO team to completely eliminate a migration step, one that entailed the deployment of a VPN using authenticated proxies. This efficiency resulted in a costs savings of hundreds of thousands of dollars and many months. Web-enabled security applications sped deployment schedules significantly as new online applications easily replicated the security architecture.

Lessons Learned and Recommendations

Deploying state-of-the-art technology requires extreme diligence on behalf of the owning organization. The fact that California ISO spent over a year investigating the technology alternatives is testament to this fact. It is extremely important that the deployed technology meet the operational requirements of the system.

Fully architecting a security solution as an *entire* system is critical. An effective security solution cannot be an assembly of numerous components that may or may not adhere to a unified policy. This architecture must also be supported by the requisite certificate policies and certificate practice statements.

Scalability is also an important factor. Scalability must be viewed as the number of objects supported by the system. Usability for the different types of certificates, including the smart card form factor, is another key element that needs to be considered when deploying security solutions. Very often, issues surrounding scalability and usability are closely related.

One-time provisioning was also a key element of success in the California ISO deployment. The security team did not have the luxury of a second chance. Once deployed, the security architecture had to work.

Finally, performance and application impact were categories that required considerable diligence in the planning cycles. System performance impact had to be kept to a minimum, user interfaces to applications had to reflect little or no change, and deployment transparency became a key objective.

By employing personnel possessing considerable expertise, conducting a thorough due diligence cycle, exercising a complete RFI/RFP/RFQ cycle, and applying sound program management principles, California ISO was able to meet their objectives in enabling the new California energy marketplace to confidently conduct business within a new security framework.

Federal Deposit Insurance Corporation[2]

The Federal Deposit Insurance Corporation (FDIC) was the subject of a comprehensive business case study directed by the General Services Administration and executed by Booz Allen & Hamilton. The goal of the project was to document a business case approach that can be used by Federal agencies considering an investment in public key infrastructure (PKI) on smart cards for government-wide applications.

The Federal Deposit Insurance Corporation's mission is to maintain the stability of and public confidence in the nation's financial system. FDIC has about 7,800 employees, including approximately 3,500 field representatives who were included in the initial PKI/smart card pilot.

FDIC generated its first certificate policy and certification practices statement in 1998. The FDIC's Electronic Travel Voucher (ETV) system was its pilot program. ETV made use of encryption and digital signature technology. FDIC issued 3,500 certificates in fiscal year 2000 and planned to issue about 5,000 more in fiscal year 2001 to complete the PKI-enabling within the corporation.

In addition, FDIC used Entrust profiles on Datakey 330 smart cards. FDIC used smart cards, combined with photo identification proximity badges, to perform PKI administration. FDIC also implemented secure extranet applications using digital certificates for FDIC external clients. This is a low assurance PKI used for authentication purposes only. FDIC maintains the PKI in-house because it will be used for the core functions of the agency. FDIC spent $5 million in fiscal year 2000 and planned to spend $2.5 million in fiscal year 2001.

FDIC is currently working on developing a high-level application programming interface (API) to make the system PKI-consistent irrespective of which PKI product is used. This will facilitate development and wide deployment of PKI-enabled applications.

The FDIC mission and vision statements are shown in Figure 1. The FDIC has insured deposits and promoted safe and sound banking practices since 1933.

The implementation of PKI and smart cards promotes both the FDIC mission and vision by:

- Addressing potential risks due to security breaches.
- Ensuring only authorized personnel gain access to sensitive data.
- Improving the ability to track and detect suspicious activity across FDIC systems.
- Ensuring the confidentiality, integrity, and availability of FDIC information are maintained.

[2] This case study, released by the Smart Card Alliance Digital Security Initiative in April 2002, was derived from a comprehensive business case produced for the General Services Administration by Booz Allen & Hamilton.

Figure 1: Federal Deposit Insurance Corporation

FDIC’s Mission and Vision Statements

FDIC Mission

“The FDIC, an independent agency created by Congress, contributes to stability and public confidence in the nation’s financial system by insuring deposits, examining and supervising financial institutions, and managing receiverships.”

FDIC Vision

“To assure that the FDIC is an organization dedicated to identifying and addressing existing and emerging risks in order to promote stability and public confidence in the nation’s financial system.”

Background

FDIC has successfully combined picture identification badges with smart card chips mounted on the badge. The badges, controlled by the security office, are issued after an employee has participated in the FDIC personnel security program. Unlike a generic token, these are registered to a specific user.

To implement these badges, a product search was undertaken that was limited to those devices capable of operating within the FDIC’s PKI. Datakey 330 smart card chips were selected and have been tested. The new Datakey 330 cards have undergone Federal Information Processing Standards (FIPS) 140-1 level 2 verification. FDIC is currently using smart cards, combined with photo ID proximity badges, to perform PKI administration.

Following pilot testing, it is expected that FDIC will begin using smart cards for all high-risk electronic transactions that require a digital signature. When this technology is combined with a picture badge, the FDIC will be able to satisfy user cryptographic requirements associated with General Accounting Office (GAO) authorization.

Low Assurance PKI

FDIC uses a low assurance PKI for a number of SSL web-based applications on its extranet with its member institutions and other parties that are external to the agency, such as other state or federal agencies. Browser certificates are used to control access to the extranet Web server. The extranet PKI uses 128-bit RSA encryption via SSL and employs Entrust WebCA software. The extranet PKI has about 2,000 certificates issued from the medium assurance PKI. The extranet uses software-based protection mechanisms (Web browser certificates). It provides authentication only.

Electronic Travel Voucher System Pilot

FDIC has approximately 3,500 field representatives with laptops. All field representatives will have to use ETV to get reimbursed. The electronic system is interfaced with the National Finance Center (NFC). Previously, it took up to two months for field employees to be repaid, but after the implementation of smart cards, it now takes two days for a direct deposit to reach the employee’s account. The paper reimbursement process used to cost about $50 per transaction to process; the new process costs less than $10. FDIC processes approximately 80,000 to 100,000 vouchers every year. This results in savings of approximately $3.2 to $4.0 million.

In addition to quantitative advantages (such as cost savings), qualitative advantages to using the ETV include:

- Quality of data check.
- Expedience of service.
- Use of direct deposit to a checking account for reimbursement.

ETV uses digital signatures and some encryption. Although the transition to PKI was a significant change for employees, the expedience with which they are reimbursed has led to this technology being welcomed by the field representatives. As a result of the success of the ETV pilot program, FDIC expanded the program to a fully operational, on-going cryptographic smart card endeavor.

PKI Enabling within FDIC

FDIC generated its first certificate policy (CP) and certification practices statement (CPS) in 1998. Development of the version 1 policy took approximately one month and underwent OIG review. FDIC is planning that future development and revisions should take no more than 3 months. A single CP is being generated to address four assurance levels. This will use the Department of Defense (DoD) CP as a template. FDIC is reviewing the Federal Bridge Certificate Policy for cross certification purposes. Each certification authority (CA) will have a certification practices statement. Each of the assurance levels will have a separate certificate profile. Specifically, the approach is to use Federal Information Processing Standards (FIPS) 140-1 validated hardware cryptographic modules for the CA. High assurance digital signatures will also become part of the smart card capabilities.

Through a competitive bid process, FDIC selected the firm Entrust as its PKI provider. Within FDIC, the PKI is run internally (not outsourced) and managed by the people who manage the issuance of passwords. The implemented architecture consisted of an Entrust Manager (version 3.0c1) and an ICL X.500 version 7B Directory Service. The client software deployed to the user is the Entrust Client v3 for desktop users and Entrust Entelligence v4.2a (with Entrust ICE/True Delete/Secure Delete) for the laptop users. The infrastructure is currently being upgraded to Entrust Manager v4, with the hopes of increasing it to Entrust Authority (version 5). Additionally, the hosting CA platform will support a FIPS 140-1 level 4 cryptographic module to contain the CA signature keys, once upgraded.

Entrust provided free toolkits that enable the Secure Communication Manager (SCM) to interface with a high-level cryptographic application programming interface. SCM is an FDIC-developed middleware application that is intended to reduce the complexity of the underlying mechanisms while facilitating service requests through simple service calls. The SCM was modified to recognize hardware tokens.

The FDIC is working with other government agencies in defining a high-level application programming interface (API) that would work with developed government off-the-shelf (GOTS) applications. This interface will be PKI-consistent regardless of which PKI product is used. This will facilitate the development and wide deployment of PKI applications and will make support across multiple PKI products less difficult. FDIC has established links with the Department of Energy, Department of Treasury's Financial Management Services Division, National Institute of Standards and Technology (NIST) and

GAO. FDIC has also had some contact with the Environmental Protection Agency and feels that the Department of Army may show interest.

Certain client software upgrades need to be made before migrating to Entrust 5.0 Manager. FDIC is testing the build for a corporate desktop upgrade that will bring everything up to version 4.X. FDIC is also procuring the software necessary for establishing a full PKI for the extranet. FDIC will shadow the internal directory to the extranet border directory and cross-certify with customers. FDIC expects to cross-certify with the Federal Bridge CA at the low assurance level using this interface.

Phase 1 of the PKI enabling will involve 2,500 examiners who are in the field most of the time. These examiners need assurance that there is only one key set. This cannot be accomplished with a floppy disk that can be copied; whereas it can be accomplished by a smart card. The issuance of smart cards will be coordinated with the badge issuance office. The badge issuance vehicle will also be the issuer of smart cards.

Phase 2 will include the rollout of PKI on all desktops. This phase was expected to commence in early 2001.

The smart card will also be used for physical access except in places where office space is leased and it may not be possible. In other staffed access-controlled areas where the badge is presented to the reader, the image of the bearer of the card is scanned and provided as physical verification to the guard. The computer room where the CA is located has a guard posted, and access is limited, by card key badge, to authorized personnel. There are still areas within the FDIC where five-button security (cipher locks) will continue to exist.

Program Management and Support

Program management and support are on-going throughout the lifecycle of the project. Program management activities include the following:

- Training
- Help desk
- On-going maintenance
- Audit

Training within the FDIC is an on-going process based on a “train the trainer” model. FDIC has numerous help desk facilities. The on-going maintenance contract FIDC has with Entrust is its Silver program, which costs 18 percent of the contract value per year. Administrators and government oversight personnel perform auditing to ensure contract compliance.

Certificate Life Cycle Management

The on-going certificate lifecycle management process is clearly defined within the FDIC and is explained in detail below.

Certificate Issuance. The core users have been issued certificates. The FDIC opted to develop an automated registration tool to support the ETV rollout. In contrast, the use of smart cards will eventually require a human in the loop to issue a key because FDIC will use high assurance cards that require that a human validate the cardholder.

Certificate Renewal. Certificate renewal is automated within Entrust. The certificate policy specifies the validity period. When the certificate nears expiration, it is automatically renewed unless explicitly denied.

Certificate Distribution. Certificates are distributed within the Entrust product to the client. Encryption certificates populate the X.500 directory and the signature certificates are concatenated with the signature of the CA.

Certificate Backup and Recovery. The Entrust Manager is backed up daily. Recovery requires registration authority (RA) intervention. The RA must establish that the user is who they claim to be. There is also an information security officer reporting system that is used to make recovery requests.

Testing and Maintenance. New software versions must be tested in lab and test environments. Older versions of the software are not supported by the vendor and therefore need upgrading.

FDIC Timeline

FDIC was able to successfully complete PKI enabling of its pilot project at the scheduled time. It plans to roll out PKI/smart cards to all employees and some contractors by March or April 2001.

FDIC had planned to complete the rollout by January 2001, but a delay in deploying Windows 2000 software had delayed the full implementation by a few months. As explained earlier, FDIC decided to keep the PKI endeavor in-house and did not contract out any portion of it. FDIC had established the timeline shown below for implementing PKI and smart cards.

Figure 2: Major FDIC PKI and Smart Card Implementation Timeline

Needs Study	January 1997
Low Assurance PKI	January 1998
Certificate Practices	August – September 1998
ETV Decision	Early 1998
ETV Cut Over	December 1999
Issuance – 3500 Cards	November 2000
Full rollout	March – April 2001

Decision To Not Outsource

The crux of FDIC's decision to not outsource relates to the future vision for PKI and smart cards. FDIC will use smart cards for its high dollar value obligations in the future. Such a critical and core function should not be outsourced to an outside vendor because the potential for significant losses is high. By keeping this function in-house, FDIC retains control of the function and can take appropriate steps to protect against losses.

The other deciding factor was that a GAO sanction will not allow for this core function to be outsourced, and FDIC is obtaining this GAO sanction. Because many financial obligations will be made with digital signatures, it can be expected that the GAO will become involved. The concern is that data integrity could be compromised. GAO will sanction only a high level of assurance that will require a person in the loop for face-to-face identity proofing.

Costs

Thus far, the cost of PKI enabling within FDIC has been $1 million for the program management of the infrastructure alone. The $1 million does not include CA contract support, FDIC contract support or government personnel time.

The costs of planning and project review were not assigned to the PKI and smart cards endeavor. Rather they were subsumed in the overall operations cost of the agency.

As an agency, FDIC had the advantage of being able to include the costs of hardware with its enterprise-wide laptop upgrade. Only the costs for the tokens and the readers were assigned to the PKI and smart cards project. This meant that the only costs were those for implementing the PKI, which included $1 million in program management costs. FDIC did not incur middleware costs as the SCM was developed in-house, so that in-house applications can call a high-level API.

The ETV pilot, which has been described in detail previously in this report, cost approximately $2.75 million to implement. All of these costs were incurred in fiscal year 2000. The cost of issuing cards and readers was $357,000 for approximately 3,000 tokens and is expected to be $678,300 in fiscal year 2001 for approximately 5,700 tokens. A one-time testing cost of $100,000 was incurred in fiscal year 2000.

Ongoing help desk support that is staffed by contractors from Computer Associates is expected to be approximately $300,000 for the first two years when the PKI and smart cards are being put in place. When proficiency has increased, help desk costs are expected to decline. System administration, including auditing and training, is expected to require three full-time equivalent staff and have a recurring cost of approximately $300,000 per year. Ongoing maintenance is provided under the Entrust Silver program, which is 18 percent of program management costs or approximately $200,000 each year throughout the life of the project.

Figure 3 summarizes the costs of the FDIC PKI and smart cards project.

Lessons Learned

This case study demonstrates that it is possible to implement PKI/smart cards irrespective of the size of the agency. Although there is currently no uniform methodology of implementing PKI and smart cards, there are three different methods that an agency can use. An agency can either outsource the activities or decide to conduct all of the operations in-house, as FDIC decided. The advantages and drawbacks of both have been discussed. A third method involves a combination of government-owned and contractor-operated ownership, where a user owns the PKI, but a contractor provides customized PKI services.

Benefits Versus Risks

The FDIC was aware of the general risks posed by use of PKI and smart cards and the obstacles to successful implementation. However, FDIC believes that the benefits outweigh the risks and have, therefore, proceeded with the implementation of cryptographic smart cards. In fact, discussions with agency personnel from FDIC reveal that they believe there is no better option for security available and that implementing PKI and smart cards is an inevitable decision.

Figure 3: FDIC Project Costs

	Year 1 (FY 2000) Total Costs	Year 2 (FY 2001) Total Costs
Number of New Certificates	**3000**	**5700**
PROJECT REVIEW		
PLANNING		
Policy Development		
Implementation Plan		
Test & Acceptance Plan		
Bid Evaluation Strategy		
Bidder Communications		
Bid Review		
Award Negotiations		
APPLICATIONS ENABLING		
Program Management	1,000,000	1,000,000
Toolkits		
Application Upgrades		
Application Installation/Modification		
Smart Cards	66,000	125,400
Card Readers	291,000	552,900
Issuance Stations		
Test and Evaluation	100,000	
Support		
Upgrade/Product Improvement		
TOTAL APPLICATIONS ENABLING	**$1,457,000**	**$1,678,300**
OPERATIONAL CAPABILITY		
Program Management		
Concept Exploration (Pilot)	2,750,000	
Training – System Administrator		
Training – End User		
Documentation		
Auditing		
Help Desk Support	300,000	300,000
System Administration	300,000	300,000
Vendor Relations Management	200,000	200,000
TOTAL OPERATIONAL CAPABILITY	**$3,550,000**	**$800,000**
CERTIFICATE LIFE CYCLE MANAGEMENT		
TOTAL COSTS BY YEAR	**$5,007,000**	**$2,478,300**

Notes:

1. **Planning and project review costs were not directly assigned to this project.**
2. **Certificate life cycle management is part of vendor relations management costs.**
3. **Year 1 costs include the cost of the ETV pilot, which is $2.75 million.**

Costs Versus Benefits

FDIC incurred substantial costs in implementing PKI and smart cards. The incremental costs of each added layer of security should be analyzed against the extra benefit that the added security feature provides. FDIC used PKI to enhance their security and realize higher levels of authentication, data integrity, non-repudiation, and confidentiality. They also purchased smart cards due to the added benefits of portability, scalability, and interoperability. Although biometric technologies offer a higher level of security, they felt that the currently high cost of biometric readers makes this option not feasible for now.

Preparing for Implementation

The implementation of the PKI and smart card infrastructure requires significant planning and consideration throughout an agency. Below is a checklist of some of the important factors that an agency should consider before implementing cryptographic smart cards. This checklist is distilled from literature review and is based on lessons learned from the case study and interviews with both PKI and smart card subject matter experts.

1. Prepare a Certificate Policy and a Certificate Policy Statement

A certificate policy is a bare minimum requirement that has to be prepared before operating a PKI infrastructure in a disciplined environment. A certificate policy will provide the map for the agency's business model for electronic transactions. Additionally, a certificate policy statement should be prepared if the agency is going to operate its own CA or have a contractor operate the CA on behalf of the agency. This certificate policy statement defines the operating procedures for the CA, namely, key management.

2. Determine the Agency's Need for Interoperability

If the agency has a high need to transact business with other agencies, the Federal Bridge Certification Agency (FBCA) is a very efficient mechanism to provide the interoperability required for this interface. The advantage of linking with the Federal Bridge is that an agency enters into one certificate management arrangement with the bridge and has access to all other Federal Bridge users rather than having to draft bilateral agreements with every agency with which the agency conducts business. If the agency chooses to operate with the FBCA, it should consider the certificate policy of the bridge in framing its own certificate policy. Additionally, the GSA Smart Access Common ID Program contract is a means of obtaining interoperable smart cards that can used between agencies.

3. Consider Phasing-In Implementation

Discussions with agencies about their PKI enabling efforts indicate that it is more practical to adopt a phased-in approach to PKI. This incremental implementation allows the agency to learn from and deal with any mistakes that may be made in the pilot process and allows for the scaling up of such activities as program management and help desk capabilities. It also allows the cost of implementation to be spread over more than one fiscal year, which could prove beneficial in securing necessary funding.

4. Department-wide Implementation and Policies

The substantial infrastructure investment and ongoing certificate-issuing costs of PKI suggest that a department-wide approach be taken to achieve centralization of infrastructure and economies of scale. The substantial marketing efforts that will be required to establish incentives and to encourage adoption of PKI digital signatures by users and constituents suggest that a centralized marketing campaign would be more effective and economical. A number of commonalities could exist among agency functions and users that will have to be established. Although each agency has a different mission, the commonalities would suggest that a unified approach could be taken to meeting information security requirements. Several PKI solutions are being tested in pilot projects within specific departments that use certificates from several vendors. It is possible that any PKI applications going forward can be met by an enterprise approach to PKI within each department. The same is true of smart cards, as all agencies within a department could issue the same smart card with the same amount of memory.

5. Define the Registration Process

The agency may decide to incorporate the certificate registration process into the existing personnel or facility office business practice of issuing identification cards. For most agencies, the smart card will replace identification cards; therefore, this step is really streamlining PKI into an existing business process, resulting in a nominal cost impact to the agency. For example, when a new employee is hired, the subscriber agreement that is required to obtain a digital certificate and a smart card can be part of the rest of the hiring package. The smart card can be issued as part of the normal processing of new employees.

6. Establish a Certification Revocation Policy and Validation Procedure

Several options are available to establish a certification revocation policy that disables certificates if the smart card is stolen or inoperable, or when an employee terminates. The revocation of certificates ensures that security remains intact. Two common certificate revocation approaches are Certificate Revocation Lists (the most common today) and the Online Certificate Status Protocol (OCSP) approach of “Validation Authority.” One key decision that should be made in establishing the revocation policy is how stringent the policy will be. A very stringent policy leads to a number of revocations, while a less stringent policy results in fewer revocations. It is extremely important for the agency to put in place validation procedures, expired certificate procedures, and Certificate Revocation Lists. Also, the agency should decide who has the responsibility of providing long-term signature validation services.

7. Forecast Liability Issues

The agency should determine upfront what liability, if any, it will assume for failures in the certificates it issues and under what conditions it will assume such liability. It may be better for the agency to posit the use of PKI as a method of preserving trust rather than creating trust.

8. Determine the Use of the Smart Card

A smart card has several potential uses, including physical access, logical access, electronic purse, transit payment, and medical information storage. Every agency will not require every one of these functions. Therefore, an agency needs to consider how the smart card is to be used in support of its mission and vision. An agency could first implement a card with a few applications and add new applications after the initial set of applications are deemed stable; however, it is important at the outset to develop a vision for how the card will be used both in the near-term and long-term. This allows agencies that plan multiple applications to buy smart cards with the appropriate amount of memory at the beginning so that new cards will not have to be issued later. Rather, the new application can simply be added to the existing card thereby reducing re-issuance costs.

National Aeronautics and Space Administration[3]

The National Aeronautics and Space Administration (NASA) plans to implement a multi-application, multi-technology smart card program with a user base spread across the agency. The NASA smart card deployment will provide users with a single identification credential to use for visual identification, physical access control, and logical access control.

The first phase of the NASA smart card program includes adopting the emerging Government Smart Card Interoperability Specification (GSC-IS) V2.1, which includes a specification for contactless smart cards to be used in physical access applications. The NASA smart card will include both contact and contactless proximity technologies. In the initial phase, the principal development activities will include engineering integrated solutions for current physical access control systems and integrating logical access control for multiple platforms including Windows®, Macintosh®, UNIX®, and Linux.

A distributed-issuance, centralized card management system modeled after the Department of Defense Common Access Card RAPIDS stations and issuance portals will be deployed in the initial phase. New identification badges that include both contact and contactless smart card technologies are planned.

NASA's primary areas of endeavor are space science, earth science, biological and physical research, human exploitation and development of space, and aerospace technology. Its core structure consists of a headquarters in Washington, DC; 10 field centers located in Maryland, Virginia, West Virginia, Florida, Ohio, Alabama, Mississippi, Texas, and California; and various facilities across the nation. The agency has a workforce of approximately 18,000 full-time civil service employees, supplemented by academic and commercial contractors.

[3] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force as part of the report, "Using Smart Cards for Secure Physical Access," July 2003.

Rabobank[4]

With 33,000 of its 50,000 worldwide employees serving 9 million customers in the Netherlands, Rabobank Group is the largest Dutch retail bank, operating nearly 1500 offices and 380 local banks. From its roots as a Dutch agrarian cooperative providing credit to farmers more than one hundred years ago, Rabobank today has grown to a position of world leadership as a wholesale bank to the global Food and Agriculture (F&A) and other emerging markets. Rabobank Group's specialized banking businesses are market leaders in virtually all financial services – from leasing and trade finance to insurance, venture capital and private banking. Its century-proven customer focus and rock-solid practices have earned Rabobank Group the coveted AAA rating only bestowed upon a few banks worldwide by major credit rating agencies.

Time-honored banking principles – trust and security – take on new significance in electronic age

Customer demands for trust and security have remained constant while revolutionary changes in banking practices and technologies over the past century have completely changed the culture of the industry. An increasing number of technology-savvy financial customers around the world expect to initiate secure transactions via the Internet or by phone anytime, anywhere. As a result, large financial organizations such as Rabobank Group have put security strategies in place, both internally and externally, to keep pace with the technology requirements of electronic banking.

Rabobank Group has stayed several steps ahead of these increasingly complex technology challenges by consistently investing in a security infrastructure and strategy it calls Rabo Web Security (RWB), deployed enterprise-wide by its Zeist-based ICT Group. Working in close cooperation with Rabobank marketing and listening to the specific local needs of its independent cooperative banks, Rabobank ICT is driven by the new market realities of electronic banking – declining numbers of bank offices and growing numbers of customers who opt for the independence and freedom of conducting increasingly complex transactions online.

"The bank's way of working today is quite different from the past and much more distributed," says Ad Bezemer, Project Manager of Infra Services at Rabobank ICT headquarters in Zeist. "Financial services have become much more complicated, as integrated products and several distribution channels are emerging. In the past, security meant shielding off hackers and intruders, but today, it means building the highest levels of trust right into our systems and communications."

Smart cards – security enablers in Rabobank's distributed environment

To build the highest levels of trust into its systems as it moves closer toward the future vision of 'anytime, anywhere banking,' Rabobank ICT has applied its forward-looking security strategy on several fronts, including its internal communications and channels. Since 1997, Rabobank ICT has been moving all applications, which in the past had disparate security and required multiple passwords, to the intranet in order to make them available on all distribution channels. "This move enables us to centralize the security around these applications," explains Ad Bezemer.

[4] This case study, released in August 2002, was developed by the Smart Card Alliance's Digital Security Initiative with the assistance of Datakey.

To control access to these centralized applications and ensure strong authentication of its internal bank employees, Rabobank is deploying 33,000 smart cards combined with PKI (public key infrastructure) technology that enable a new level of security and efficiency for its internal employees. The cards are provided by Datakey, Inc., a North American-based developer of smart card technology for securing e-business. Datakey smart cards enable security in transaction- and communication-based domains such as finance, government, health care and telecommunications around the world.

At Rabobank, the deployment of smart cards is eliminating the risks inherent in a "knowledge only" system based on multiple passwords. This is accomplished by providing two-factor security – *something that is owned* (the smart card) and *something that is known* (the user's password). In e-business security language, the smart cards provide 'non-repudiation' – two-factor security authenticates unequivocally that users truly are who they claim to be – and therefore integrity and security. In addition, the selected smart card technology has FIPS 140-1 validation, an independent U.S. government certification of cryptographic strength and security.

The smart card technology deployed at Rabobank provides role-based access for users, which is particularly important at Rabobank because there are 55 different roles for its 33,000 employees in the Netherlands. The roles define what kind of transactions each user is able to conduct online. According to Rabobank's security policy, each application is classified with an internal classification system using the criteria *availability*, *integrity* and *confidentiality* (abbreviated in Dutch as the BIV code). On the highest security level, the BIV 3 classification, the smart cards are also used to add digital signatures to transactions. The smart card's 32 kilobyte storage capacity easily allows it to store digital certificates with each internal user's role, as defined by the specific job level, as well as a high volume of updates.

"The Datakey smart card is the enabler for Rabobank security," explains Ad Bezemer. "We are going from 10 to 12 different passwords, each application with its own authorization, to ONE smart card. The smart card meets our requirements for security, compliance with standards, role-based access, and they're ready to go – what is called 'plug-and-play' in the industry. In a highly distributed environment like ours, the smart cards are an efficient security solution."

Because Rabobank's cooperative banks decide independently on their local needs and requirements, some are using the smart cards for physical access. To meet the specific requirements of those banks, the smart cards are delivered custom-formatted with magnetic stripes and proximity technology. The Datakey technology supports different kinds of readers, and the smart cards can be used with the Compaq keyboard readers already installed at Rabobank. Whatever 'flavor' of smart card the individual banks prefer, employee uses include network access, Microsoft Windows™ logon, and digital signatures.

Rabobank has given several hundred additional smart cards to large customers for special transactions. In international scenarios, for example, the smart card is used for 'dealing room' currency transactions. The customer is able to do an immediate buy or sell in the exact dollar (or other currency) amount without incurring the risk of losing funds through currency fluctuations. "By ordering the currency transaction directly with the smart card, the customer is able to side-step the process of calling the bank and arranging a transaction which may take a month or two to complete," says Ad Bezemer. "The usually 10-second confirmation makes the transaction almost real-time, versus the risky delays with the old process. The smart card offers our currency-trading international customers speed, cost-efficiency and transactional security."

Rabobank expects ROI from technology investments in trust and security

Rabobank is planning to move its web security strategy forward with several technology enhancements in the near-term. Once every user has a smart card, this card will be the only authentication device for employees and can be used in other areas such as remote access, virtual private networks (VPNs) and secure mail. Approximately 10 percent of Rabobank users work in small offices or are mobile. They use the Citrix concept of server-based computing, and will also use smart cards for remote access and digital signatures.

According to Ad Bezemer, "Our role here at Rabobank ICT is to be enablers of methods and technologies that are vital to our business. The advance of e-commerce means a continued focus on the security of all transactions. Deploying the smart cards internally has been one important aspect of our security strategy. Now that we have laid the foundation, we can cash in on that and deploy on a larger scale. That's the nature of our business as a bank – to pay off, our communication has to be rock-solid, built on trust and security."

Schlumberger[5]

In 1999, Schlumberger Limited (www.slb.com) inaugurated a global initiative to deploy smart cards and public key infrastructure (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[6]. 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 operating system (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 using 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.

[5] This case study, published in April 2002, was developed by the Smart Card Alliance's Digital Security Initiative with the assistance of Matt Radcliffe, Schlumberger, and Bryan Ichikawa.

[6] Now Axalto.

Schlumberger processes tremendous amounts of customer data. The oilfield operations generate large volumes of 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. Protecting business information and managing access to networked computing resources became a top priority.

The project started in 1999, and the research and development 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 user ID and password systems. Help desk costs for managing the user ID and 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 bank card 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 in the world. 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 traveling. Additionally, Schlumberger employees are often in remote locations to support customers locally. 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.
- To 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 operating system.
- 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, providing smart card integration with Netscape browsers and the Entrust software.
- CSP (Cryptographic Service Provider), providing 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 virtual private network (VPN) client. The VPN solution provides smart card-based authentication for 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 certification authority and registration authority 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 is integrated with the Schlumberger Cryptoflex™ and Schlumberger Cyberflex smart card platform and 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

Many different 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 use 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 benefits 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 that 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, and procedures for lost/stolen cards. There was also an Entrust computer-based training module installed on every employee's PC, enabling the end user 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 dialogs 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 cost. 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 and 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, a complex and capital-extensive program 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, operating system, 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.

Shell Group[7]

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 used 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 supporting 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 planned to

[7] This case study, published in April 2002, was developed by the Smart Card Alliance's Digital Security Initiative with the assistance of Martha Jones, Schlumberger, and Bryan Ichikawa.

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 magnetic 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, 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 considering a cost of around $100 per user per year and the fact that passwords provide very little security in return, a new, more 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 are 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 uses this approach to authenticate users, bring down support costs and leverage the investment in network equipment and IT personnel. Using one card, Shell employees will have physical access to their facilities, be able to login 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 personal identification numbers (PINs), 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 non-repudiation. 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 non-repudiation 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 the 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, login anywhere on any device, be authenticated and receive their proper level of authorization.

The Shell smart card platform uses:

- Smart cards - Cyberflex 16K and 32K smart cards.
- Readers – Keyboard (available January 2002), PCMCIA, USB, serial.
- Schlumberger Self Service Module – User-friendly, web-based card management system.
- Schlumberger Virtual Channel solution - Allowing 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 help desk costs. Shell's deployment is also one of the largest Windows 2000 deployments in the world and one of the largest private sector smart card deployments in the world. In addition, the smart card 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 s risky proposition; single sign-on with smart cards provides improved security and improved manageability while reducing help desk 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 MetaFrame 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 operation 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, the employee call one of the global help desks and the 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.

Cost/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 user ID/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 and Recommendations

Although the deployment is still in progress, initial management 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 infrastructure, security models, PKI, smart cards, physical security, and security management principles.

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.

Sun Microsystems Java Badge[8]

”At Sun Microsystems we created a new smart card solution for network security and physical access control called Java™ Badge," said Chris Saleh, marketing manager and program manager for Java Badge. "We've rebadged every Sun employee in the United States and we're on track to finish all 35,000 employees worldwide in 128 countries by July 2003. We are using Java Cards manufactured by Schlumberger and readers from SCM Microsystems as well as our own embedded ones. The cards have a magnetic stripe for access control today, and MIFARE™ contactless chip we plan to use for access in the future. We chose a Java Card because it offers the important advantage of being able to dynamically add applications in the field in real time."

One application of the card is building access, but the main reason Sun adopted smart cards was to implement logical access to the company's network using Sun Ray™ appliances, the thin clients deployed at Sun. "We have flexible offices for 25,000 employees, meaning you do not always work at the same office," said Saleh. "Sun Ray delivers IT services in a very cost effective manner, because all sessions reside on servers. The smart card is the key to the system, because it lets people bring up their own sessions and user environment."

"For example, say you want to leave for the gym. You pull out your Java Badge from the Sun Ray appliance, which powers down to save energy. When you return from the gym you go to another office and use your card to get your session back up again. Once you insert the Java Badge into the appliance it powers up, gets your personal session from the Sun Ray appliance and takes you right back to your personal session where you left off. Sun calls it 'Session Mobility,' which is being able to carry your user environment from one area to another," explained Saleh.

"We're entering a new phase with Java Card to issue certificates on smart cards," said Saleh. "We'll have three applications secured by a public key infrastructure (PKI): authentication/single sign-on, signature, and encryption for secure email transmissions. For the highest levels of security we want dual-factor authentication – what you have and what you know. The card is what you have and the personal identification number (PIN) is what you know in order to log in to services. Down the road, maybe we'll use three-factor authentication with addition of biometrics."

In addition to Sun Ray appliances, there were many reasons for Sun to go to smart cards. "It's technically safer to store PIN and key information on smart card hardware tokens than on a computer hard drive in some server room. It eliminates the inefficient use and inherently weak security of passwords. We were motivated to go to smart cards for legal reasons too. To move commerce to the Internet we needed a robust system that offers non-repudiation, and Europe dictates smart cards and PKI to achieve this. Finally the smart cards enabled us to consolidate four or five credentials into one card," stated Saleh.

"The user reaction is extremely positive. The consolidation of cards, not having to remember passwords, mobility and increased sense of security are huge pluses and convenience for them. We are a big proponent of smart cards," he

[8] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force as part of the report, “Using Smart Cards for Secure Physical Access,” July 2003.

concluded.

Sun, Sun Microsystems and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Transportation Security Administration Transportation Workers Identification Credential (TWIC)[9]

The Transportation Security Administration (TSA) is mandated by federal legislation to develop an identification system for individuals requiring access to secure areas of the nation's transportation system. The Transportation Worker Identification Credential (TWIC) is intended for each worker requiring unescorted physical or logical access to secure areas of the nation's transportation modes (maritime, aviation, transit, rail, and other surface modes).

The TWIC will allow implementation of a nationwide standard for secure identification of transportation workers and access control for transportation facilities. Current estimates are that 12 to 15 million workers will require the TWIC to gain access to secure transportation sites. Each individual enrolled in the TWIC system will be positively matched to his or her credential via a reference biometric (or multiple biometrics) and will have undergone a standard background check.

The program infrastructure carefully balances security, commerce, and privacy requirements. The TWIC is to be universally recognized so that workers will not require redundant credentials or background investigations to enter multiple secured work sites and will allow facilities to better manage site access. Additionally, the credential will have the capability to be used within a facility to meet multiple levels of secure access requirements.

The TWIC system will contain sufficient technologies to be compatible with Government Smart Card Interoperability Specification (GSC-IS) while maintaining access to and within local facilities. This will enable the TWIC to leverage existing access control system investments, rather than require replacement of these systems at considerable expense. Additionally, the TWIC system will serve as the standard platform for future technology purchases at transportation facilities.

The TWIC program has received authorization to conduct two regional multi-modal pilot projects. The Los Angeles/Long Beach and Philadelphia/ Delaware River areas have been selected as the TWIC regional pilot sites based on the broad range of facility types (e.g., mode, size, infrastructure), organization structures, transportation mode inter-relationships, and policy issues in each region.

The TSA completed a technology evaluation in late 2003 and determined that smart card technology is the most appropriate for TWIC's requirements. TWIC program personnel is in the process of planning a seven-month prototype phase which will begin in early 2004.[10]

[9] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force as part of the report, "Using Smart Cards for Secure Physical Access," July 2003.

[10] "Transport Worker ID Almost Ready To Roll," Card Technology, Dec. 10, 2003.

U.S. Department of Defense Common Access Card[11]

On November 10, 1999, the Deputy Secretary of Defense (DEPSECDEF) issued a memorandum directing the integration of efforts to improve information assurance and reduce fraud associated with the current Armed Forces identification (ID) card. In response to this memorandum, the Department of Defense (DoD) began rolling out the Common Access Card (CAC) in October 2000. The resulting CAC program addresses the need to expand the functionality of ID cards as well as provide a strong digital ID for increasing the protection of sensitive DoD information assets.

The CAC was designed to serve as a standard DoD ID card, as the primary card to enable physical access to buildings and other controlled spaces, and as a card to grant logical access to the Department's computer networks and systems. The DoD's challenge was designing an interoperable secure multi-application smart card that could function as a military ID card compliant with the Geneva Conventions. To address this challenge and establish a satisfactory balance with cost, the DoD sought to adopt industry best practices and commercial off-the-shelf (COTS) products adapted to the DoD environment versus creating a military-specific card system. The most economic way to accomplish this task was to use a smart card platform to serve as a token for digital certificates. The certificates on the Common Access Card are compliant with the U.S. digital signature law and guidance.

The existing infrastructure of more than 1,500 military ID card issuance workstations worldwide is being expanded and upgraded to issue the more secure, higher assurance cryptographic hardware token CACs. Up to 200 additional registration workstations will be added to provide issuance to the military, as well as to DoD civilian and contractor personnel that currently are not served by the existing card issuance workstations.

Approximately 4 million participants, including active duty military, selected reserve personnel, DoD civilian employees, and approved contractors, will receive the CAC initially. Not included in the initial roll-out are retirees, family members, or inactive Reserve personnel that will continue to receive the non-CAC ID card. The potential population served by this program (specifically those receiving ongoing medical and other economic benefits) is approximately 13 million.

The first beta site was established on October 2, 2000 at Quantico, Virginia. As of mid-2001, the CAC card was operational at 70 beta sites. As of September 2003, DoD had issued 2.8 million smart cards on the way to 4 million, a goal that they expect to achieve by early 2004.

Operating Environment

DoD ID cards are produced on-demand at more than 900 locations worldwide. An infrastructure of equipment, trained verifying official personnel and supplies are managed through a global network that provides ID cards to all uniformed service members (active duty and guard/reserves) from the U.S. Army, U.S. Air Force, U.S. Navy, U.S. Marine Corps, U.S. Coast Guard, Public Health Services (PHS), and National Oceanographic and Atmospheric Administration (NOAA). In addition, ID cards are provided to family members eligible for benefits as well as retirees. Each facility has its own procedures for providing separate ID cards for building access purposes.

[11] This case study, published in April 2002, was developed by the Smart Card Alliance's Digital Security Initiative with the assistance of Virginia Uelze, DAL.

The smart card technology is being integrated into the Defense Enrollment Eligibility Reporting System (DEERS) and the Real-Time Automated Personnel Identification System (RAPIDS), which are two established independent – but closely coupled – systems providing eligibility information for DoD benefits.

Originally, the DEERS database was developed by the DoD in response to a Congressional mandate to improve the control and distribution of military health care services. The system provides a computerized information service for the enrollment of individuals who are eligible for benefits within the Uniformed Services. The database holds 23 million records and offers accurate and timely information on all eligible members of the Uniformed Services, their family members, guard and reserve personnel, and DoD civilians.

In an effort to reduce the potential fraud, waste, and abuse associated with obtaining benefits, the RAPIDS application was established to produce a more secure method of generating identification cards. Through this application, ID cards are created for the military, their family members eligible for benefits, guard and reserve personnel, and retirees. RAPIDS consists of a network of workstations and servers located in the Uniformed Services personnel offices and other selected locations worldwide.

The RAPIDS application is one of the principal means to update information in DEERS. Through the RAPIDS software, users can create, modify and use personnel information stored in the DEERS database to issue ID cards and provide other personnel support to those individuals eligible for benefits. After the DEPSECDEF mandated the creation of the CAC, steps were taken to redesign RAPIDS and DEERS to allow for the issuance of the CAC through the RAPIDS software for eligible personnel.

In order to upgrade RAPIDS, the addition of CAC software components and additional hardware is necessary. These additions, already underway, include a public key infrastructure (PKI) certificate management, Java™ Card applications, SSL client/server software, smart card encoders/readers, PVC plastic card printers, personal identification number (PIN) pads, and port replicators. Additionally, appropriate training is being provided following system upgrades to smooth the conversion process.

One of the integration issues faced was that the different military services (e.g., Army, Navy, Air Force, and Marine Corps) maintain their own networks, firewalls and communications infrastructure. This environment produces a unique challenge for establishing seamless integration while achieving and maintaining desired network performance and service levels for cardholders.

Business Issues

The CAC program was designed to address two main problems: (1) improve information assurance and (2) enable electronic commerce.

The need to improve information assurance, due to higher threats associated with increasing dependence on the Internet, prompted the development of a large-scale PKI in DoD. To comply with the Cohen-Clinger Act (which among other things requires the improvement of mission-critical information assurance in the Department's data and infrastructure), an improved information security process was developed based on implementing PKI across the Department for sensitive, but unclassified data.

The approach initially proposed to satisfy the need for digital signatures was to issue software tokens on floppy disks. Although this was stronger and better than passwords, it met only part of the requirement to improve mission critical “Defense-in-Depth.” Even though funded, the use of software tokens was an expensive proposition that would require the development and fielding of a complex face-to-face registration infrastructure to “verify” the identity of all military and civilian personnel within the Department as well as those eligible contractors who typically work inside DoD facilities. Migrating to a hardware-based token solution – where the cryptographic certificate material and private keys could be stored – was the more secure solution.

The second problem was that the current military ID card was increasingly prone to fraud. The ID card could easily be copied, duplicated or manufactured. Moving toward a stronger, more secure, solution that supported non-repudiation – such as an electronic “cyber” ID – was the desired outcome.

Decision Process

The DoD’s decision to embark on an extensive effort to adopt smart card technology and fully capitalize on the potential of that technology was driven by a solid business case. Financially justifying individual solutions to either problem outlined above on a stand-alone solution was not feasible. The infrastructure requirements necessary to deploy a PKI, which requires face-to-face verification of all of its users along with a coordinated database that could uniquely and reliably identify and verify each individual in the DoD, were extremely costly. Instead, by fielding an integrated solution that leveraged the existing ID card infrastructure, the Department was able to achieve economies of scale that provided for business process reengineering to combine three core functions (ID, PKI, and physical access) and their respective issuance infrastructures into a single process.

By employing a business-based approach to the implementation of this technology, the DoD sought to use the technology as a tool to enable business process reengineering and streamline operations in order to achieve performance improvement targets, such as infrastructure reduction, mission enhancement, improved security, increased customer satisfaction and improved quality of life.

Smart Card-Enabled

The DoD is using smart card-based technology and systems to transform and improve processes and mission performance by capitalizing on electronic commerce capabilities. The operational requirements defined by the DoD included electronic messaging, network identification and authentication (I&A) services, personal identification, electronic commerce functions, and physical access. The common thread tying all of these requirements together is the use of tokens as a secure vehicle for I&A. Tokens provide secure storage of a “secret” value (private key) in a public key-based system, identification and authentication of an individual, and a cost-effective, secure and portable credential. In support of a token strategy, the DoD explored available options.

Technologies considered included Personal Computer Memory Card International Association (PCMCIA) cards, USB tokens, software tokens, and smart cards. PCMCIA cards, while providing the best security and performance, had significantly higher infrastructure costs and were not the preferred format; they were not wallet-sized and did not allow for a photograph. USB tokens provided strong security, a ubiquitous interface to new personal computer (PC) platforms, and were already third generation devices. However, the form factor was once again a problem as these tokens could not accommodate photographs or other technologies from which the existing DoD infrastructure would be migrating. Software tokens presented a cost advantage, which was offset by the inadequate security features and limited portability. The fourth technology considered was smart cards, appealing because of their relatively low cost, robust security features, versatility and variety.

Seizing this hardware token strategy, the DoD sought to establish the baseline functional requirements for a multi-purpose token and identify which of the above four technologies would best serve its needs. The desired DoD PKI token had to support confidentiality, integrity, non-repudiation, and authentication as well as enable electronic messaging, network I&A services, e-commerce, personal identification, and physical access.

After assessing the token technologies and standards, the DoD decided to employ smart cards to obtain increased security. By combining such a large number of security features on one piece of plastic, the CAC has become one of the most versatile ID and access cards in the world.

The decision to use smart cards over other token technologies was based on the industry interoperability, commercial industry direction, economic considerations, multi-application capability, dynamic loading of applications, and software post-issuance. Smart cards provide the most comprehensive solution to a variety of applications and address the functional and technical requirements identified through the token strategy. Additionally, smart cards enable strong identification, digital signature, storage of demographic data, and Service-specific applications.

A final benefit the smart card offered was that, because of its format, the card functions as an ID card as well as a physical and logical access card. The multiple technologies, such as integrated circuit chip, bar codes and magnetic stripes, which are included on the smart card platform, also facilitated integration with the legacy systems prompting a strong economic business case.

Application Description

The CAC smart card holds multiple technologies. The chip holds the PKI encryption and authentication keys, demographic identification information, and the card management application. The PKI is considered to be “Government Furnished Equipment (GFE)” and is provided by the Defense Information Systems Agency (DISA).

The card has 32 kilobytes of Electronically Erasable Programmable Read Only Memory (EEPROM) with a co-processor capable of generating keys via digital signature with approved cryptographic algorithms. The operating system is Java-based (Java 2.1) and the security and the card protection software conform to Open Platform 2.0.

Smart card use and applications are based on an open system configuration, interoperable with commercial and government/service applications and is consistent with commercial industry standards. The application is designed to support a secure operating environment with rigorous security and information assurance for smart card systems and operations that ensure confidentiality and integrity of information, concurrently protecting sensitive data.

Implementation Overview

In order to deploy the CAC Department-wide beginning in October 2000, a number of decisions and actions had to be taken in the short-term. Prior to beginning implementation, the DoD had to complete a requirements definition, define CAC platform specifications, and finalize a strategy for procuring the smart cards and necessary smart card production hardware, firmware, and software.

Key milestones in the first six months of the implementation process (June 2000) included covering the development of government-wide interoperability specifications by the General Services Administration (GSA) and industry partners. The beta testing was scheduled in two phases with Phase I (CAC production) testing of the CAC to be completed by August 2000 and Phase II (CAC application) testing completed by January 2001. Finalizing the CAC configuration for the fielded version was targeted for September-December 2000. Rollout to more than 900 sites worldwide was targeted for the fiscal year 2001, with complete deployment in 2002. Due to technology issues, Phase I of the beta testing was initiated in October 2000 and Phase II started in March 2001.

Program Management and Support

The three primary organizations involved at the Department level to support the CAC are the Electronic Business Board of Directors (EB BOD), the Smart Card Senior Coordinating Group (SCSCG), and the Defense Manpower Data Center's (DMDC) Access Card Office (ACO). These three organizations were created as leadership and decision-making groups to manage and ensure effective implementation. Membership for both the SCSCG and EB BOD is composed of senior representatives and decision makers from the OSD, the Joint Staff, the war-fighting Commanders-in-Chief (CINCs), Military Services and the Defense Agencies (collectively known as the DoD Components).

A Smart Card Configuration Management Control Board (SCCMCB) originally was established to assure broad communication and the integration of cross-functional requirements. That body was disestablished and, at the time of this writing, the EB BOD serves as the decision authority for configuration management of the CAC smart card platform, and provides adjudication for any issues that cannot be resolved at the SCSCG-level. The EB BOD in turn reports its findings to the DoD Chief Information Officer (CIO) Executive Board, as stipulated in the DEPSECDEF memo of November 10, 1999, and ultimately is responsible for CAC implementation. Lastly, the ACO provides the operational, technical, program and policy support, and associated information management. The ACO is an element of the Defense Manpower Data Center (DMDC), an element of the Office of the Undersecretary of Defense for Personnel and Readiness and is under the operational control of the Department's CIO.

Cost/Benefit Analysis

The Department was driven by a need to improve business processes and provide added security to networks and systems. By employing state-of-the-art technology, the solution embedded in the CAC program would yield cost savings, improve readiness, enhance mission, support the war-fighter, and increase quality of life. Solving the fraud and information assurance problems individually as a stand-alone solution was not economically beneficial. However, by leveraging the existing ID card infrastructure, the DoD identified an approach that provided a satisfactory solution to both objectives and simultaneously offered associated benefits that supported the business case for both needs. With the adoption of PKI, the use of the Internet to transfer data securely and perform online transactions would become more reliable and common.

The Department's approach uses COTS technology following best industry practices. The card platform and architecture mirror the approach of the card industry – which has started its rollout in the United States. Sun Microsystems' corporate ID card – that is to be issued to all Sun Microsystems employees worldwide – is also based on the same platform and approach.

This approach is standards-based using IETF, ISO, ANSI and Global Platform specifications; this has allowed multiple organizations to competitively supply smart cards, readers/encoders, software and other equipment for this program. Furthermore, the DoD is leveraging the economies of scale of large organizations issuing smart cards globally. For example, Visa has 1 billion cardholder accounts worldwide enabling low-cost, common solutions to continue to improve the economics of this program.

In addition, the CAC platform supports multiple applications. This allows for additional services to be dynamically loaded after the cards are issued to provide additional capabilities and services. The U.S. Navy and U.S. Marine Corps will use the CAC as a physical ID card and as a logical ID card to gain access to the newly emerging Navy-Marine Corps Intranet (NMCI). As requirements change due to legislation, policy and other factors, the ability to evolve the CAC without re-issuance has tremendous economic benefits.

The smart card was envisioned as an updateable, individually carried, data storage device that functions as a vehicle to reduce fraud and as an integral component of the Department's enhanced security solution.

Lessons Learned and Recommendations

As of mid-2001, the CAC program was operational at 70 beta sites. The cards were issued with all functionality and within initial milestones. As of September 2003, DoD had issued 2.8 million smart cards on the way to 4 million, a goal that they expect to achieve by the early 2004.

Some key lessons learned from the implementation experience stem from the decentralized issuance. In circumstances where cards are issued through a number of sites, a good roadmap identifying different communication types involved and maintaining control over firewalls are critical factors to make integration more seamless. The DoD identified a need to improve the speed and reliability of the DEERS and RAPIDS issuance portal. Further troubleshooting highlighted the criticality of appropriately sizing the certification authority (CA) to support the expected volume of traffic. Maintaining connectivity between the RAPIDS workstations and issuance portals is vital to streamline the issuance process. When connectivity failed, stations were unable to issue CACs, and at times, congestion at the portal significantly slowed down the issuance process.

Another critical success factor in deploying any new system is user buy-in. To improve migration to the new CAC card, it is essential that users are educated about PKI and other card functionalities. The implementation experience highlighted the need to provide greater training and help desk assistance to users. Some end users reported they were not aware when they were performing PKI functions properly, particularly when signing and encrypting e-mail. Users need to be adequately instructed about how to use PKI identity certificates and smart cards. Training and help desk assistance are critical components of the implementation process that can ensure the success of a new system. A comprehensive public relations effort to ensure that the users of the smart cards are aware of their issuance ahead of time to facilitate the transition process will permit all system users to fully capitalize on the enhancements provided by the smart card technology.

The implications for this program are already spreading beyond the DoD. Private industry is adopting a similar model to provide an improved cyber identification credential for commercial and industrial e-commerce applications. Just as the DoD developed the Internet, a recent external review conducted by the Joint Service Advisory Group to the DoD CIO concluded: “The DoD Common Access Card – a combination Military ID card and the host for the PKI hardware token will eventually have the same national impact as the Arpanet did in leading to the Internet.”

This program has established the benchmark as the way to thrive in a more secure and safe manner in the digital economy, not only for the government, but for private industry as well.

Sources

Air Force PKI CAC Pilot, After-Action Report, May 2001.

Burch, Kate, interview and personal communication, August 2, 2001. Dreifus Associates Limited, Inc.

CAC Communications (Public Affairs) Plan, June 14, 2000.

CAC Execution Plan, June 14, 2000.

Common Access Card Specifications Release 1.0, Draft Version 0.9, May 10, 2000.

Configuration Management Plan for the Common Access Card, Version 1.1, June 18, 2001.

DoD PKI Authentication Device Carrier Report, Version 1.0, November 18, 1999.

DoD PKI Token Support, Token Strategy Discussion, August 11, 1999.

DoD Target Token Strategy, March 8, 2000.

Havrilla, Joe, *Security Tokens Overview*, June 10, 1999.

Monk, Justin, interview and personal communication, July 30, 2001. Dreifus Associates Limited, Inc.

Role of Smart Card Management System in the CAC Implementation, Draft Version 1.0, December 26, 2000.

Smart Card Senior Coordinating Group’s Chip Allocation Technical Workgroup: Common Access Card Release 1.0 Specification, Draft Version 0.6, March 17, 2000.

U.S. Department of Homeland Security Identification and Credentialing Card[12]

The Department of Homeland Security (DHS) is establishing a common trust model across the enterprise, formally composed of 22 separate entities. This solution addresses both physical and logical identification with a single, multi-purpose smart card-based credential. The system supports various stakeholders' access control systems by providing strong, centralized managed authentication, while retaining decentralized control of data and facilities. This initiative will facilitate physical access to DHS facilities, logical access to computer networks, and remote access communications as well as enabling electronic commerce.

This comprehensive identification and credentialing effort will be implemented using a hybrid cryptographic smart card using a public key infrastructure (PKI) for logical access and a contactless chip for physical access. Authentication of the individual to the card will employ biometrics, with a personal identification number (PIN) as a backup. DHS has rejected proprietary security infrastructures and will take advantage of the organic security features available from open standards-based applications and operating systems.

These cards will be totally interoperable within DHS as well as with the Department of Defense (DoD) smart card program and the smart card specifications developed by the National Institute of Standards and Technology (NIST) and General Services Administration (GSA). The cryptographic chip will be compliant with Java 2.1 and Global Platform 2. The contactless chip will adhere to ISO/IEC 14443 Type A specifications. DHS is planning to issue these smart ID cards to 190,000 employees by the end of 2006.[13]

Joe Broghamer, lead for Identification and Credentialing within DHS states: "DHS is leveraging policies and technologies from DoD, GSA, NIST and within DHS in order to drive standards and interoperability. The adherence to open standards will greatly reduce the interoperability problems that have plagued previous smart card/PKI efforts. DHS is in a position to positively influence industry and to become a leader in critical areas of identification and credentialing."

Joe Broghamer summarized this effort as: "Once implemented, this card will not only provide increased security for DHS systems, but equally as important, provide an eloquent, easy to use solution for enabling e-commerce and facility access."

[12] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force as part of the report, "Using Smart Cards for Secure Physical Access," July 2003.

[13] "Homeland Security To Issue 190,000 Smart Card IDs," Card Technology, December 9, 2003.

U.S. Department of State Access Control Smart Card Implementation Project[14]

The U.S. Department of State is implementing smart ID cards to function as an individual's identification card throughout the government enterprise. All U.S. Department of State employees, contractors, and affiliates who work within the Department will be issued smart ID cards by the Bureau of Diplomatic Security to be used for physical access. The Bureau of Information Resource Management (IRM), which oversees logical access, will use the smart ID card as a token for a public key infrastructure (PKI). The Department of State is one of the first federal agencies to use a smart card for physical access, logical access and PKI.

Employees and contractors will be required to insert their smart ID card into a physical access card reader, installed at external and internal entrances, allowing authorized users access to the facilities. The access control readers are secure, programmable readers provided by XTec™ Incorporated. One beneficial feature of the intelligent readers is the ability for a security manager to securely inject authentication keys into the reader. This is currently done at the reader, but will be done from a central management point in the near future. Plus, the smart ID cards and physical access readers adhere to the Government Smart Card Interoperability Specification (GSC-IS).

Another value of the programmable readers is the ability to communicate with the different legacy access control systems currently deployed at State Department. State Department has a three-year migration path to update or replace the current legacy access control system. The programmable reader allows the legacy MDI OS/2 system to operate with the smart cards in addition to the newly installed Software House C*Cure system. From a user perspective, it makes the conversion invisible. It gives State Department the ability to replace the old Wiegand card technology in a shorter time period.

Approximately 35,000 users will use the new card for facility access to State Department buildings. Because it is one of the first agencies to fully adopt the GSC-IS, the State Department is able to issue a variety of smart cards to meet specific needs. There are two cards used strictly for access control: the XTec Secure Mediametric™ memory card, and Oberthur CosmopolIC™ Java card. In addition, the Datakey 330G file card is being used not only for access control, but for logical applications such as secure email, network authentication, and logon.

The majority of Department of State users (80-90%) will use their smart ID cards to secure their PKI applications, including desktop security and encryption using Entrust Entelligence™, secure email, and virtual private network access. Future plans include integrating biometric readers for logical access and possibly physical access into sensitive areas. The State Department plans to store other data on the smart card, including emergency medical information, human resources data, and travel orders.

According to Lolie Kull, former smart card implementation manager for the Department of State, "The smart card brings it all down to one simple, safe and secure denominator. One single token will simplify how we practice security as we get in the door or access our computers. At the same time, it

[14] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force as part of the report, "Using Smart Cards for Secure Physical Access," July 2003.

heightens security by 100%. The solution to our security challenges is this one smart card that does it all.”

U.S. Navy DENCAS[15]

The U.S. Navy Medical Information Management Command (NMIMC) and Bureau of Medical and Surgical (BUMED) saw a need to develop an e-business system to gather dental readiness and productivity information. The Department of the Navy's Smart Card Office (DONSCO) funded the project because it has the capability to use digital certificates stored on the Department of Defense (DoD) Common Access Card (CAC). DONSCO, NMIMC and BUMED all worked closely with the private contractor, MAXIMUS, in this one-year project.

The system is comprised of a web-based application with a centralized database. Public key infrastructure (PKI) is used to provide non-repudiation of a user's identity with the subsequent permissions structure being database-driven. PKI is also used for data transmission. This system, called DENCAS (Dental Common Access System) was designed in summer 2001, developed beginning in September 2000, and was deployed in June 2001 for beta testing. It is currently being deployed worldwide.

MAXIMUS project management and development staff met with all stakeholders to view the existing business process and to analyze the stakeholders' requirements for DENCAS. A functional requirements analysis (FRD) was created and submitted to the stakeholders for approval. From that FRD, a design document was drafted from which DENCAS development was then based.

Currently DoD is issuing a Common Access Card (CAC) as a smart identification (ID) card. The process is underway to replace all military ID cards with CACs, including reserves, dependents and retirees. The total number of CACs is expected to exceed four million smart cards, with as many as 13 million eventually issued.

Operating Environment

Prior to DENCAS implementation, Navy dental patient treatment and productivity data were collected in approximately 400 standalone databases. The productivity data were sent to a centralized location monthly with the patient treatment data available only to the command from which it was generated. Data being transmitted were not protected by encryption, thus anyone able to intercept it could view it.

Navy personnel are now able to access DENCAS through their normal Internet connection and by using their digital certificates to achieve secure logon. These digital certificates are used to identify the user who is then associated with user permissions stored in the database. User permissions allow users to enter and view near-real-time data to which they should have authorized access.

For the first time, corporate users at BUMED and NMIMC have access to Navy-wide patient treatment and productivity data. This capability allows for immediate and accurate determination of U.S. Navy dental readiness, something that once took over a month's worth of data collection and processing to compute.

[15] This case study, published in April 2002, was developed by the Smart Card Alliance's Digital Security Initiative with the assistance of Barbara Selter, MAXIMUS.

Decision Process

DONSCO and NMIMC were concerned about the privacy and confidentiality of patient data being accessed over the Internet. The DoD had previously decided to issue digital certificates to DoD personnel on the CAC IDs because it believed that PKI offers the most effective security available. Therefore, it was consistent with prior DoD decisions to design DENCAS with PKI and CAC. DENCAS provided the opportunity to demonstrate the cost-effective use of PKI and smart card technology to enhance the delivery of dental services in the military.

Business Issues

Prior to DENCAS, all patient and productivity data were collected and stored at approximately 400 individual terminals. The distribution of data both upward to corporate users and downward to customer command users required paper printouts of data. This collection and processing of data was cumbersome, tedious and time-consuming, resulting in an end product that was out-of-date and no longer accurate by the time it reached its recipients.

DENCAS' web-based architecture allows individuals Navy-wide to view data that is pertinent to them. At the corporate level, the Director of Navy Dentistry can view patient and productivity data either Navy-wide or drill down to various Navy Dental Commands. Dental liaisons at bases and in the fleet are able to view their unit's dental readiness and obtain a list of individuals who need to be sent for dental treatment or for exams.

In all cases, DENCAS relieves dental clinics of the chore of creating reports. Dental Technicians previously assigned to clerical duties can reduce their paperwork by using DENCAS, freeing them to provide enhanced patient services. Shifting dental technicians from clerical assignments to patient support has not only improved the quality of care, but also enhanced the productivity of this staff.

Further, DENCAS has streamlined the deployment process. By enabling secure access to dental readiness data, DENCAS has decreased the time needed to deploy troops while increasing the security and confidentiality of patient information.

Smart Card-Enabled

Smart cards are currently used at all Navy and Marine Corps recruit commands with the Smart Dental Information (SDI) application. SDI documents dental examinations and stores the information on the recruit's smart card as well as in a central database. Dental examination data are then uploaded into the DENCAS system. Upon completion of CAC issuance Navy-wide, individuals logging onto the system can use certificates stored on the CAC to verify their identity.

Application Description

DENCAS is a web-based application that resides on a server running Windows 2000 Advanced Server. It uses Active Server Pages (ASP) running on Internet Information Services (IIS). The database is SQL Server 2000.

Data from the approximately 400 standalone terminals are initially uploaded to DENCAS to populate the database and to preserve valuable data that existed prior to DENCAS implementation. Because some dental facilities do not have reliable Internet connectivity, DENCAS is designed to allow users to input data into their existing legacy system and then upload that data when connectivity is available. This provides added reliability to clinics that rely on their local data to operate. For this reason, DENCAS data are considered near-real-time rather than real-time.

Smart cards are currently being designed to become the new Armed Forces ID card. In the future personal dental information will be carried on military ID cards (CAC) in addition to the recruit cards already in use. The digital certificate issued on the CAC can be used to log onto DENCAS.

Implementation Overview

In 2000 the concept of DENCAS was developed between the medical professionals at NMIMC and the medical division at MAXIMUS ITD. During that year the requirements and design were fully fleshed out in detail by NMIMC, BUMED, DONSCO and MAXIMUS.

After this design phase, the development phase began in September of 2000. In June of 2001, the initial beta testing began and in August, 2001 the server was delivered to NMIMC.

This was a very rapid design, development and deployment timeline that has been in keeping with the Navy's Task Force Web, which calls for an 80 percent solution in five months rather than a 100 percent solution several years down the road.

Program Management and Support

The project was led by a representative from each of the four entities: NMIMC, BUMED, DONSCO and MAXIMUS.

The program is supported by various entities. Operator training was conducted at NMIMC in July 2001. A help desk maintenance contract was negotiated. Certificates are issued by DoD, in compliance with the DoD certificate policy. Smart cards are currently issued at the recruit depots and the Armed Forces Smart ID cards (CAC) are being deployed.

Cost/Benefit Analysis

The goal of the DENCAS system was to provide a secure and rapid web-based system to review dental readiness and productivity throughout the Navy.

The system was delivered on time and on budget. It has surpassed expectations for security and operability.

DENCAS eliminates many hours of report generation for dental providers, allowing dental technicians to perform their core responsibilities. This will lead to greater productivity and efficiency at dental clinics. Top management at the DOD has Navy-wide clinic productivity information to use for allocation of resources; this information was never before available at a reasonable cost.

Unit deployability and dental readiness information is now in a secure, central database and continuously available for near-real-time analysis by operational decision makers. This dental readiness review was not possible at a reasonable cost previously.

Although no studies have been performed to date determining the specific cost savings of DENCAS over the existing paper and standalone dental systems, the anecdotal evidence points to significant time savings and better utilization of staff. Additionally, system users emphasize the importance of using smart cards with digital certificates to maintain the privacy and confidentiality of patient identification.

This solution is in conformance with the security and privacy requirements of the Health Information Portability and Accountability Act (HIPAA) legislation. The Navy has awarded DENCAS its e-Government Award, citing the enhanced efficiency and security it provides.

Lessons Learned and Recommendations

The active participation by the medical/dental professionals with the MAXIMUS team enabled continuous refinement of the system. User involvement was critical to the successful implementation of this system.

Rapid deployment methodologies using emerging technologies such as web applications and smart cards result in far more flexible and usable systems. DENCAS is a prime example of the Navy's new model for IT system development—that is, providing an 80 percent solution in 5 months versus a 100 percent solution in 5 years. Due to the volatile nature and rapid pace of technology advancement, a rapid development approach enables a more cost-effective approach to keeping up with emerging technologies.

Use of the smart card and web access to multiple databases allowed secure access to critical data not otherwise available without significant investment of man-hours.

Health Care

French Sesam Vital Health Card[16]

Starting in 1997, France began a complete reform of health care organizations and professionals. The purpose was to develop a program meeting the data exchange expectations and needs of everyone involved in French health care, from insured patients to health care professionals and insurance funds.

France was one of the first countries in the world to introduce large scale deployment of smart cards as part of a health insurance system. The system, known as Sesam Vitale, was the first completely automatic system in which smart cards were used in the health sector. Today, there are approximately 57 million cards in use. That number is expected to rise to 65 million in the near future.

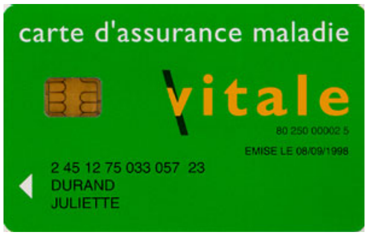
Health care in France is funded partly by the French government and partly by private insurance companies. This situation leads to a complex process for reimbursement for the individuals involved, both patients and professionals. The old paper system was prone to error, fraud, and long delays before final payment was received.

Sesam Vitale

Sesam Vitale is a highly secure dual-card system. The cards (one for patients and one for health care professionals) are the heart of a French health care system that links every individual with health care resources, including public hospitals, private clinics, general practitioners, specialist doctors, nurses, and midwives, all through a secure network. The Sesam Vitale system simplifies the procedure by which health care costs are cleared and also dramatically reduces the risks that refunds to insured patients will be delayed by replacing an annual 1 billion pages of health care information with electronic transactions. The result is that the average reimbursement time has been reduced from up to 6 weeks to 2 or 3 days. In addition, payments are made directly to health professionals by the insurance companies. The system also tracks health care spending and, in the future, will be used to transfer electronic prescriptions to the health care funds responsible for reimbursement.

Sesam Vitale Patient's Card

The Sesam Vitale patient's card is a micro-controller (MCU) card containing approximately 4 pages of text. The patient's surname, first name, and Numéro d'inscription au Répertoire (NIR)[17] are printed on the front of the card. On the back is the card serial number.



[16] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force with the assistance of Ian Duthie, Atmel Corporation, as part of the report, "HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," September 2003.

[17] The NIR is the French equivalent to the U.S. social security number; however, no credit bureau is allowed to gather financial information using the NIR. This eliminates the use of the number for identity theft.

The data stored in the chip are separated into two zones and include the NIR, health insurance system code, branch, entitlement start date, proof of entitlement, presence of permanent entitlement, surname, first name, date of birth, status of beneficiary, information specific to the health insurance system, and entitlement end date. The card replaces the standard “soft copy” individual health insurance card.

The first, family version of the card (Vitale1) contains administrative data that is available to health professionals (such as physicians, pharmacists, dentists, physiotherapists, and nurses). The data is read immediately and stored as a secure electronic health care cost claim sheet (e-sheet) during the patient visit. (The data cannot be read without the presence of a health care professional’s card, or CPS, described below.) Depending on the software application and the smart card reader, this e-sheet can be stored either in programmable secure reader memory or on the health professional computer’s hard disk. The sheets are bound daily into secure electronic batches and transmitted through the secure national health intranet, the RSS (Réseau Santé Social), to the health insurance front-end servers. There the sheets are automatically processed by a back-office system for further cost clearing.

Sesam Vitale Health Care Professional’s Card

The Sesam Vitale health care professional’s card, called the Carte de Professionnel de Santé (CPS), is also a highly secure smart card that is easily recognized by its color. The MCU embedded in the card includes a crypto-processor that manages public keys and generates digital signatures.

The card identifies the health care professional and provides authentication, digital signatures, and data encryption. Pharmacists and medical staff also receive a card. More than 425,000 cards have already been issued to health care professionals, with more than 90,000 to physicians.

German Health Care Card[18]

Health insurance is required in Germany, and the majority of the population is served by public health insurance. Currently, Germans carry a health care card that can be characterized as an insurance card. Its primary function is administrative.

Current Health Card Program

The current German health card program was rolled out in 1993 and is fully implemented. A total of 80 million people now carry the card. The card contains a 256 byte protected memory chip (not a microprocessor) and stores the following data:

- Identity of the insurance
- Insured person's name, address, and date of birth
- Status of the insurance
- Expiration date for the insurance

This data supports the following administrative benefits:

- Patient identification
- Elimination of duplicate records
- Reduced paperwork and cost associated with mailing health insurance forms
- Streamlined admission process
- Reduced transaction costs

A 1997 study by the German Ministry of Health showed that the cost of the cards was fully amortized in the 3 years after introduction.

When data on the card become obsolete, insurers reissue the card (even though overwriting the obsolete data is possible). Between 15 and 20 million cards are issued annually.

Next Generation Health Card Program

Germany is now planning for the next generation of health care cards. The new program is expected to include cards for patients and cards for health care professionals. These more advanced cards will be based on 16 or 32 kilobyte (KB) microprocessors. The cards are expected to provide multiple additional benefits, such as enabling insurers to collect co-payments that are currently uncollected and eliminating paperwork associated with the current prescription drug program.

Trials of the new program are expected in 2004-2005, with January 2006 the target date for rollout. The expected total cost to upgrade the system infrastructure and issue new cards is approximately $500 million. Although this figure sounds high, a study commissioned by the Federal Association of Pharmacists and one of the country's health insurance funds and undertaken by Hamburg-based health consulting firm Debold & Lux predicts that the new health card system could pay for itself within 12 months.

[18] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force with the assistance of Linda Brown, Infineon Technologies, as part of the report, "HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," September 2003.

Many health care professionals in Germany would also like to see an electronic prescription drug application. The Minister of Health is investigating potential pilots for such an application.

Mississippi Baptist Health Systems[19]

Starting with two doctors in 1911, Mississippi Baptist Health Systems (MBHS) now comprises two hospitals (Mississippi Baptist Medical Center and Baptist Restorative Care Hospital), 500 doctors on staff, 110,000 emergency room outpatients a year, and a host of health-related services in the community. In an attempt to stay ahead of the legislated requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), MBHS has begun work on a smart card-based program to replace their current magnetic stripe identification card system. The added bonus of being able to use multiple applications on a single card was also a factor in deciding to use smart cards.

To the 70,000 current card-carrying members of their system, MBHS hopes to reach new levels of patient convenience, safety and privacy with the smart card program. Their goal is to replace all legacy cards within two years of the institution of the new program. In addition to the functionality provided by the new smart card program, MBHS also hopes to gain visibility from its initiative, marking it as a leader in health care technology.

The cards will contain a subset of the patient's medical record and demographic information. When visiting a doctor's office, emergency room or clinic, upon presentation of the patient's card, a form specific to the site visited will print out. The card will maintain a record of clinical history such as blood pressure, pulse, and medications. In the future, the cards will be used to fax medical records from incoming ambulances to the destination emergency rooms.

MBHS is using in-house developers to integrate the new technology into their existing data infrastructure. Using Java Card programming, they have developed their own Internet update and maintenance programs. They have also created their own user interfaces and have designed clinic kiosks for on-site patient use. The initial pilot is scheduled for October 2003 with full production to follow before the end of the year.

[19] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force with the assistance of Jim Canfield, Alegra Technologies, as part of the report, "HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," September 2003.

Taiwan Health Care Smart Card Project[20]

The Taiwan health care smart card project is one of the largest health care smart card solutions in the world and the first of its kind in Taiwan, Republic of China. The total bid price for the project was US$108 million, and contractors were requested to finish within 25 months of the start date, April 12, 2001. The smart card project infrastructure is integrated into the original paper-based health care system.

Project Background[21,22,23]

The total population of Taiwan is now 22.5 million, and 96% of Taiwan citizens joined the National Health Insurance (NHI) program that was established 8 years ago. A total of 16,558 hospitals and clinics (90% of the total) registered in the NHI program, creating a service network for insured applicants nationwide. Taiwan had a strong IT foundation: the original paper-based health care system included 92% of contracted medical institutions with a computerization rate of at least 70% and public satisfaction levels of 71%.

The NHI program recognized revenue from insurance premiums of US$8.3 billion in 2001. Total health expenditure is 5.5% of Taiwan's GDP.

Before the smart card was introduced, paper cards were used by the Bureau of National Health Insurance (BNHI) to audit patient information, then reimburse service providers monthly. The card is renewed after the patient uses medical services up to six times. Even though reporting and information handling is well run and maintained, the system has certain problems, such as identity fraud, excess false insurance premium claims from health care institutions, complex program vouchers, waste of resources due to high frequency of card replacement, and high losses due to discontinuity of insured applicants. To solve these problems, in April 2001 the Bureau of National Health Insurance (BNHI) issued 22 million smart health care cards using Java Card technology to Taiwanese citizens.

Project Implementation

The main contractor, the Smart Card Division of the Information System & Service Sector of TECO Electric & Machinery Co., Ltd. (TECO),[20] integrated the original back-end database for the paper card system with the interface for the new smart card system. In the first year, they created specifications that met the requirements for hospitals and clinics, computer back-end needs, security rules, and networks. They also completed the system development required by the specifications. In the second year, TECO manufactured the cards, developed the required applets to be loaded on the cards, audited the

[20] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force with the assistance of Yuh-Ning Chen, Ph.D., MartSoft Corporation, as part of the report, "HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," September 2003.

[21] Taiwan Bureau of National Health Insurance web site, www.nhi.gov.tw (in Chinese), news articles; www.nhi.gov.tw/01intro/intro_5.htm (in Chinese); www.win2000.com.tw/teeth/iccard.php?menu=5 (in Chinese).

[22] *National Health Insurance: An Overview and Perspectives*, Bureau of National Health Insurance, Taiwan, 2002.

[23] Interview with Mr. K. P. Chang from TECO Electric and Machinery Co., Ltd., by Matt Wylie, TECO.

information for all 22 million people, took photographs, issued cards to everyone, and installed card readers in 16,000 participating hospitals. They also tested and verified all processes. Currently about 70% of the hospitals are online. It is believed that the online rate will be almost complete by the end of 2003.

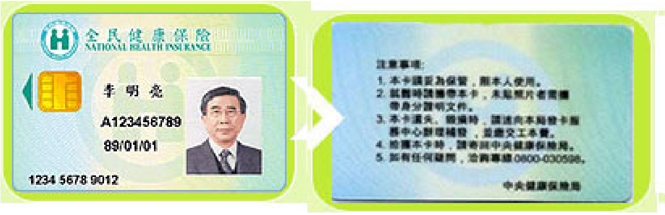
This project required multiple stages. The tasks for the main contractor included the following:

- Design and facilitate the execution of security policies.
- Allocate resources to design, manufacture, and distribute approximately 22.3 million smart cards and 300,000 reader security access module (SAM) cards.
- Install 20,000 free reader sets (one for each health institution in the pilot trial).
- Establish and manage a 150-seat call center for card use support.
- Develop a comprehensive computing network between BNHI headquarters and its branches and develop a medical virtual private network.
- Integrate a platform for information transmission between BNHI, hospitals with different health information systems, and medical institutions with different IT infrastructures.
- Manage 800 training courses for end users and hospitals nationwide.

Project Results[24]

TECO and the other participating entities integrated the entire IT infrastructure of Taiwan's health industry and then integrated this new infrastructure with a secure smart card solution.

The NHI health care smart card (illustrated below) can be used for 5 to 7 years, making annual replacement unnecessary. The front side of the card includes the card's serial number and the cardholder's photo, name, ID number, and date of birth. People are not required to present an additional ID when they use the card for NHI health care services.



The smart card is a microcontroller-based card and has 32 kilobytes (KB) of memory, of which 22 KB will be used for four kinds of information:

- Personal information, including the card serial number, date of issue and cardholder's name, gender, date of birth, ID number, and picture.
- NHI-related information, including cardholder status, remarks for catastrophic diseases, number of visits and admissions, use of NHI health prevention programs, cardholder's premium records, accumulated medical expenditure records and amount of cost-sharing.

[24] Source: MartSoft Corporation. Special thanks to Mr. K. P. Chang and Ms. Tiffany Lee for providing interviews and access to reports about the Taiwan health care smart card.

- Medical service information, including drug allergy history and long-term prescriptions of ambulatory care and certain medical treatments. This information is planned to be gradually added depending on how health care providers adapt to the system.
- Public health administration information (such as the cardholder's personal immunization chart and instructions for organ donation).

The Taiwanese government has reserved the other 10 KB of memory for future use.

Moving to the smart card system has resulted in the following changes:

- Hospitals and clinics upload electronic records daily to BNHI.
- After every six patient visits, card information is uploaded online for data analysis, audit, and authentication.
- The reimbursement process is faster.

Privacy and Security[25]

BNHI has strong privacy and security requirements for the Taiwan health care smart card, including a defined privacy policy, multiple smart card security mechanisms to prevent counterfeiting and protect cardholder information, mechanisms to protect the security of information during transmission, practices to prevent computer viruses and a crisis management and response plan. The overall system architecture was designed to implement these policies, protecting the cardholder's private information while allowing access by authorized health care professionals. Key smart card security and privacy mechanisms are:

- High-grade card printing, comparable to payment cards.
- Encryption of information stored on the card.
- BNHI-issued SAM card for each smart card reader, with a strict authorization and mutual authentication process to access on-card data.
- Cardholder personal identification numbers (PINs) to protect on-card personal information.
- Plans for a health professional card that would be used to authorize health care provider access to medical information on the card.

Lessons Learned[26]

To be successful, similar smart card projects must ensure physical, platform and application interoperability. The following items are important for successful project implementation:

- A comprehensive system security plan to guard the cardholder privacy.
- Certification of security control at each step.
- A comprehensive plan for managing the first issuance of the card, which must involve as few errors as possible to reduce cost.
- A comprehensive plan for the entire information system structure.
- An assessment of the efficiency of system operations.

[25] Taiwan Bureau of National Health Insurance National Heath Insurance IC Card web site, http://www.enhi.com.tw/ (in Chinese).

[26] "Eight key areas in successful smart card deployment," by TECO Smart Card Business Center, March 2003 (in Chinese).

- A marketing project plan.
- Integration testing and acceptance procedures.
- Card application development to ensure that the necessary card applications are available when needed.

The infrastructure development required to support the Taiwan health care smart card project is well underway. Starting July 1, 2003, both health care smart cards and paper cards are in use simultaneously in Taiwan. As of September 6, 2003, smart cards have been issued to 95% of the population of Taiwan and 70% of the hospitals and clinics are online and in operation for smart card usage. It is estimated that by January 2004, health care smart cards will be fully implemented and paper cards will be phased out.[27] In the current (initial) stage, only name, date of birth, and national ID number are stored in the card.[28]

[27] Taiwan Bureau of National Health Insurance National Health Insurance IC Card web site, http://www.enhi.com.tw/news_detail.asp?file_id=4201.

[28] Taiwan Bureau of National Health Insurance National Health Insurance IC Card web site, http://www.enhi.com.tw/news_detail.asp?file_id=4396.

University of Pittsburgh Medical Center[29]

Faced with dramatic growth, the University of Pittsburgh Medical Center (UPMC) found it difficult for their technology infrastructure to keep up with their business requirements. Given their size – 20 hospitals and a group of over 5,000 doctors in over 400 offices – processes such as verifying the eligibility of individuals while maintaining the confidentiality of sensitive patient information became increasingly difficult. UPMC found that it was obvious they were moving toward unmanageable administrative processes, high and increasing operational costs and ineffective intra-health system communications.

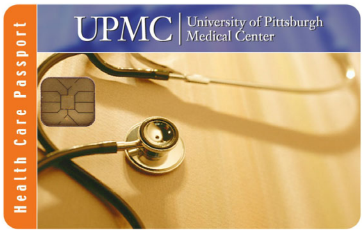
An initiative was undertaken to implement a solution that would integrate UPMC's disparate systems and practices. The mandate for this system would be to:

- Solve the challenges of complying with data privacy and confidentiality legislation (i.e., the Health Insurance Portability and Accountability Act of 1996(HIPAA)) requiring higher security.
- Enable patients to have access to their information and play a part in updating their data.
- Provide a portable solution capable of immediate access and consistent data flow.

UPMC determined that smart cards were the obvious choice as the centerpiece in this new system.

Following a successful two-year pilot project – in which approximately 300 cards were distributed to UPMC Health Plan subscribers, and one physician's office was equipped with readers – the UPMC smart card, called the Healthcare Passport, has now been distributed to 2,000 UPMC patients, 1,000 UPMC physicians and five members of the Chip Ganassi NASCAR racing team. This is the next phase of a five-year, $500 million electronic medical records initiative.

For the patient, the immediate benefits include speeding the check-in process during office visits. The cards enable better care through faster retrieval of important medical information, according to Scott Gilstrap, director for technology solutions at UPMC. "The smart card eliminates a lot of paperwork for the patient and makes the visit to the doctor more convenient and less stressful," Mr. Gilstrap said. "It can be a true lifesaver, especially for the elderly who may not remember all of the medications they are taking. This information is stored, updated accurately and easily available on the card."



Patients will no longer need to fill out their personal information each time they visit their doctors since the cards will contain pertinent critical information such as medications, allergies and chronic conditions. By inserting the patient card in a computer in the exam room, the physician can have instant access to accurate and up-to-date information on the patient.

Patients can also check their stored information by using a computer kiosk in the physician's office or they may purchase a card reader to use with a home

[29] This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force with the assistance of Jim Canfield, Alegra Technologies, as part of the report, "HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," September 2003.

computer. For the patient, a personal identification number (PIN) is required to gain access to their data.

In addition to patient use of smart cards, 1,000 medical staff physicians and affiliated physicians from UPMC will also have cards. Physicians will be able to access information on their patients from home or office using their smart cards. These cards are being called MDID – Medical Digital Identification.

"The key is to give physicians access at home, comply with HIPAA privacy and security rules, and make it easy for UPMC physicians to view vital health information and take better care of their patients at our facilities," said Ralph Schwartz, M.D., director of UPMC MedCall. UPMC MedCall is an extensive physician tracking system that includes immediate contact information of more than 14,000 UPMC physicians that is available 24 hours per day, seven days per week, maintains more than 400 on-call schedules, and is considered among the largest electronic physician tracking systems in the United States.

The UPMC smart card uses sophisticated security measures that make it nearly impossible for strangers or unauthorized personnel to retrieve a patient's medical information. "In order to access information, each patient and physician must have a card and a PIN. This is called two-factor authentication. One piece of authentication is useless without the other," Dr. Schwartz said.

The cards also may decrease the likelihood of inaccurate billing. About 90 percent of services denied by insurance companies are due to clerical errors made at the time of registration for a clinical service.

Because of the numerous UPMC facilities and the need for an integrated system, the software and integration applications of the smart card were developed by UPMC's Information Technology Division.

The card contains 64 kilobytes (KB) of memory (EEPROM) that is devoted to data storage. The data are stored using compression technology with a 10-to-1 compression ratio, allowing 640KB of information to be stored on the card. (640KB is the same capacity as some of the earlier computers.)

Soon, paramedics and emergency rooms equipped with card readers will be able to rapidly access potentially life-saving information about a patient, such as allergies to medications and chronic medical conditions. The initial rollout will include smart card readers at the Presbyterian University Hospital Emergency Department, Sports Medicine in the Kaufmann Building, Sports Medicine in Southside and Dr. Solano's practice in Oakland, Pennsylvania.

"It won't be long before most, if not all, emergency departments and physician offices, even those not affiliated with UPMC, will have smart card readers, which currently cost less than $20. Readers are already being integrated into most of the newer personal computers. There is every reason to believe that the technology will soon be in medicine," Mr. Gilstrap explained. "This technology not only solves our immediate security concerns for granting access to electronic health records, but also provides a feature-rich alternative to include a host of other applications which provide improved medical care, improved access and convenience of care, and at the same time enhance our business relationships."

The smart card project is just one component of an ambitious information technology initiative at UPMC. The centerpiece of the initiative is the development of an electronic health record to be totally integrated across the entire system, which includes 17 hospitals in both urban and rural settings, hundreds of physician practice offices, and nursing, personal care and long-term care facilities.

The goal of UPMC's information technology initiative is to improve the quality of patient care, to reduce errors and duplication of services, and to be a more cost-effective system. Importantly, UPMC believes information technology allows patients greater access to care and a more informed, interactive health care experience.

Retail Payment

American Express ExpressPay[30]

American Express ExpressPay is a contactless payment device that is targeted at fast, low-value transactions. The card is half the size of a regular credit card and fits on a key chain. American Express is piloting ExpressPay with consumers in Phoenix, Arizona, at its New York facilities and in Singapore.

ExpressPay is an easy-to-use alternative to cash for making purchases at merchants where speed and convenience are important — such as quick serve restaurants, supermarkets, drug stores, gas stations, and corporate cafeterias. Users simply hold the ExpressPay key fob next to a companion reader at checkout to make purchases. Payment is authorized in seconds and no signature is required. ExpressPay links directly to an existing credit, charge or debit card to fund the purchase.

Consumers enroll in ExpressPay and select a payment account that should be used for ExpressPay transactions. Consumers have two options for funding ExpressPay. ExpressPay Direct Link, which carries a daily spending limit of $150, links to an American Express charge or credit card for payment. Individual charges are recorded directly on the card member's monthly billing statement for easy tracking. ExpressPay Pre-Loaded can be prepaid up to $600 monthly, using any debit, charge, or major credit card (e.g., American Express, Visa, MasterCard, or Discover). The card can be reloaded automatically from the same payment source when the value goes below $20. As with all American Express Card products, customers are not liable for any fraudulent ExpressPay charges.

The ExpressPay system uses a high-frequency RF payment device (based on the ISO/IEC 14443 standard) that identifies the consumer and processes the transaction as a traditional credit or debit card transaction. The ExpressPay reader can be easily implemented at merchant locations, working with a merchant's existing point-of-sale system.

ExpressPay has implemented security and fraud prevention features to protect consumers, including:

- Encrypted data on the ExpressPay device.
- No visible information about the funding account.
- Unique identification for each device stored in the smart card chip and anti-counterfeit graphics.
- Daily spending limits and monthly funding limits.
- Protection from liability in the event of fraudulent charges.

According to American Express, ExpressPay pilot results show that participating merchants have seen customer spending increase by 20 to 30 percent compared to their cash spending, while customers have seen their checkout time reduced by 30 to 40 percent.

[30] "American Express expands availability of new "contactless" payment product designed to make everyday purchases quick and easy," American Express press release, July 16, 2003.

MasterCard PayPass[31]

MasterCard's PayPass, announced in December 2002, eliminates the need for users to swipe their payment cards through a reader. Consumers tap their cards on a specially equipped merchant terminal that then transmits the payment details wirelessly. The new solution is targeted for traditional cash-only environments where speed is essential, such as quick service restaurants, gas stations, convenience stores, and movie theaters.

Chase, Citibank, and MBNA are working with MasterCard in a MasterCard PayPass trial in Orlando, Florida. Consumers can use the PayPass card at a variety of participating Orlando merchants, including Boater's World, Chevron, City of Orlando Parking, Eckerd, Friendly's, Loews Universal Cineplex, McDonald's, Ritz Camera, and Wolf Camera. The MasterCard PayPass card also includes a magnetic stripe, allowing consumers to use it at any location that accepts MasterCard.

The MasterCard PayPass card uses a high-frequency RF payment device based on the ISO/IEC 14443 standard (Types A and B) to securely transmit Track 1 and Track 2 payment information from the card to the merchant terminal using RF. This eliminates the need for a cardholder to present the card to the merchant to swipe through a reader, allowing the cardholder to remain in control of the card.

MasterCard PayPass is straightforward for retailers to implement. It uses standard credit card data for the payment transaction to leverage the existing magnetic stripe-based infrastructure. The simplified approach of using Track 1 and Track 2 data allows merchants to cost-effectively retrofit their current magnetic stripe POS terminal to start accepting PayPass cards.[32] A special contactless module can be added to any magnetic stripe POS terminal. This module includes a contactless reader that collects the card information and passes it to the terminal, as if the information were from a regular magnetic stripe credit or debit card. From that point on, the transaction is treated as a traditional credit or debit card transaction.

In May 2003, MasterCard also announced a market trial in Dallas, Texas, with MasterCard PayPass incorporated into Nokia mobile phones. This trial allows consumers to tap or wave their phone to make payments.[33]

MasterCard consumer research revealed the following reactions to PayPass:[34]

- 63% of the consumers surveyed said that they would "definitely" or "probably" use MasterCard PayPass if their bank offered it to them.
- Consumers who said that they would definitely use the card indicated that it will replace cash in more than half (53%) of their transactions.

[31] This implementation profile was developed by the Smart Card Alliance Terminal and eTransaction Infrastructure Task Force as part of the report, "Contactless Payment and the Retail Point of Sale: Applications, Technologies and Transaction Models," March 2003.

[32] "U.S. Smart Card Breakthrough," The Nilson Report, January 2003.

[33] "MasterCard PayPass Continues to Build Momentum as 'The Simpler Way to Pay'," MasterCard press release, May 13, 2003.

[34] "New MasterCard PayPass Utilizes Contactless Payment Technology," MasterCard press release, December 12, 2002.

- PayPass is perceived to be "innovative" and "fun to use," as well as an enhancement that "would make shopping less of a hassle."

By the end of 2004, MasterCard expects that there will be 4 to 6 million PayPass cards in the U.S.[35]

[35] "MasterCard Orders Pay-With-A-Wave Chips," CTWeekly, December 10, 2003.

Visa Contactless Payment in South Korea[36]

Since 1998, approximately 6 to 7 million Visa-branded contactless cards have been issued by several large Visa members in South Korea. These cards contain a chip, which is used for contactless payment in the Seoul transit system, and a magnetic stripe, which is used for regular credit card payments. The popularity of transit applications on credit cards means that contactless chips have become a standard feature for the majority of new credit cards issued to residents of Seoul. Several other major cities in South Korea (Busan, Jeonju, Inchon, and Ulsan) have also deployed Visa credit cards coupled with a contactless transit application. However, unlike the cards used in Seoul, these cards are issued as "dual-interface" cards in which a contact-based electronic purse (on a chip) is offered along with a contactless transit application (also on a chip).

In 2002 Visa introduced the dual-interface GlobalPlatform (GP) card, based on Philips technology. Unlike previous dual-interface cards, the new GP cards allow applications to be downloaded, modified, and deleted after the card has been issued. The cards also support VSDC and Visa multi-functionality. Three major districts in South Korea, (City of Daejon, City of Gwangju, and Chungnam Province) have adopted these dual-interface GP cards. Issuance begins in 2003, with a target of up to 2 million cards. In addition to the ISO/IEC 14443 and MIFARE-based transit application, the card will also carry VSDC (EMV credit and debit), digital ID, Visa Cash e-purse, and loyalty applications. Other cities that have been issuing proprietary transit cards are planning to migrate to Visa's dual-interface Global Platform cards.

Visa continues to work very closely with S-1/Samsung Electronics in several areas to provide VSDC payment and multi-function capabilities through the dual-interface smart card chip. Current programs include contactless access control to corporate buildings for Samsung employees and their families and contactless access for residents of apartment buildings in several major South Korean cities.

SK Telecom, the largest mobile telecommuni-cations service provider in South Korea, launched the second phase of their Moneta card program in December 2002. The Moneta card now supports Visa payment at the point of sale using an IR beam or signal sent from mobile telephone handsets to upgraded merchant terminals. Plans are in place to expand this program and include contactless Visa payment in 2003. By the end of 2003, it is anticipated that approximately 400,000 terminals will be upgraded to support IR and contactless smart card technology and approximately 2 to 3 million handsets will be deployed.

Two other South Korean telecommunications providers, KTF and LGT, have indicated that they will also provide Visa payment at the retail POS using infrared and contactless smart card technology in 2003.

[36] This implementation profile was developed by the Smart Card Alliance Terminal and eTransaction Infrastructure Task Force with the assistance of Julie Krueger, JCB International Credit Card Co., as part of the report, "Contactless Payment and the Retail Point of Sale: Applications, Technologies and Transaction Models," March 2003.

Transit Payment

Hong Kong Octopus Card[37]

The Hong Kong Octopus card, launched in 1997 as an electronic purse for public transportation, is the most successful and mature implementation of contactless smart cards used for mass transit payment. The card's acceptance and popularity have since extended its use to nearby retailers.

Octopus cards were developed as an automatic fare collection (AFC) scheme for Hong Kong's transit system. Over 9 million Octopus cards and 150,000 smart watches have been issued, and over 7 million transactions are recorded on a daily basis, for a daily transaction value of over HK$50 million (about US$6.5 million). This contactless smart card ticketing system currently includes over 100 service providers, including all of the major transport operators (bus, taxi, subway, train, tram, and ferry services). Because Hong Kong's main transport operators are all partners in the Octopus card, kiosks are widely available, making it easy for customers to check the balance on a card and recharge it with cash or electronic payments. The use of the card has shortened queues at ticket barriers, because the card doesn't have to be taken out of a bag or wallet — customers can just wave it past a scanner at a distance of several centimeters.

The first non-transit applications for the Octopus card allowed the card to be used for payment at photo booths located in the Mass Transit Railway (MTR) stations and pay phones operated by New World Telephone. After only 5 years, 25 percent of Octopus card transactions are unrelated to transit. The card lets consumers make payments quickly and conveniently and is accepted by more than 160 merchants.

- Park 'N Shop (Hong Kong's leading supermarket), Watson's, 7-Eleven, Starbucks, McDonald's and Circle K convenience stores accept the Octopus card.
- More than 3,000 soft drink vending machines in offices, schools, and shopping malls now have Octopus scanners. Sales have increased, as consumers make more impulse buys when they don't need to use cash.
- Pay phones, photo booths, and many car parks accept the card, removing the need for consumers to carry change. The card can also be used for admission to public swimming pools and other recreational centers.
- Nokia has launched a mobile phone cover that includes an embedded Octopus chip and antenna, enabling commuters to use their phone to make Octopus payments.

While Octopus cards are anonymous by default, over 500,000 personalized cards have been issued and are used for the Octopus Automatic Add-Value Service. Twelve Hong Kong banks and one credit card company support the automatic add-value service. Because each personalized card has a unique identification number, up to 40,000 cards are also being used as security passes at housing estates, for staff identification cards, and as loyalty cards.

[37] This implementation profile was developed by the Smart Card Alliance Terminal and eTransaction Infrastructure Task Force with the assistance of Julie Krueger, JCB International Credit Card Company, as part of the report, "Contactless Payment and the Retail Point of Sale: Applications, Technologies and Transaction Models," March 2003.

The contactless Octopus card is based on Sony's FeliCa™ technology, a proprietary 13.56 MHz technology similar to but not compliant with the ISO/IEC 14443 standard technology. This technology has widespread acceptance in the Asia Pacific region, with over 25 million cards issued worldwide, according to JCB International Credit Card Company. Terminals read the cards instantly, processing transactions in less than one-third of a second. On the MTR, a scanner at the ticket barrier loads data on the card that is then used by scanners at the exit gates to deduct the correct fare and show the remaining credit.

In 2002, the Asia Pacific Smart Card Association reported that 95% of the "economically active population" in Hong Kong was using the Octopus card. Travelers have found that the card provides increased convenience, allowing them to pass through fare collection points 15 to 20% faster, according to Octopus card statistics. The scheme has succeeded because it offers real convenience to cardholders.

References

"Contactless Smart Card Schemes in the Asia Pacific Region," Asia Pacific Smart Card Association report, August 2002.

Donald Davis, "The Contactless Wave," *Card Technology*, January 2003.

Octopus card web site, www.octopuscards.com.

London Oyster Card[38]

In November 2002, TranSys, Transport for London, and London Underground began rolling out smart cards as part of a £1.2 billion world-class ticketing system designed to make travel in the capital faster, easier, and more convenient for London's commuters.

As of November 2002, 6,000 buses and 255 Tube stations were equipped to accept the new contactless cards, and a comprehensive data acquisition and control system is installed to support ongoing operations, revenue management, and reporting. After months of field testing, the card, called Oyster, was given to almost 80,000 Tube and bus staff in August 2002. In May 2003, a limited public introduction was made to 200 users. Success with each of these stages led to a June 2003 launch with cards available for sale through the Oyster card web site. Web support also includes online purchases of monthly, annual, and weekly passes which are electronically delivered to in-the-field Oyster cards via a directed auto-load and the fare processing device. In September 2003, ticket office sales were introduced. As of September 10, 2003, 26,000 cards had been issued. Fare policies will be introduced in January, providing incentives for Oyster card use on bus routes. It is anticipated that upon stabilized penetration more than 5 million cards will be issued in the greater London area. There are over 16,000 Oyster card-enabled terminals spread throughout the greater London area.

The credit card-sized Oyster cards need simply to be touched on the card readers on buses or at gates. For some travelers, the Oyster card will carry a period ticket, while others will use the card for a new PrePay ("pay-as-you-go") facility. The cards can currently be reloaded via the on-line facilities and at ticket offices. Functionality coming online includes load capability at ticket vending machines and via merchant terminals in a network of over 2,300 merchants called PASS agents.

The Oyster card is more secure than the previous magnetic stripe ticket and will speed travel by reducing the number of people paying cash to a bus driver and the number of trips travelers must make to the ticket office. The cards will also make it easier to switch between different modes of transportation. Ultimately they will operate across the network, including on trams and Docklands Light Railway as well as on buses and the Tube. Future plans include building a London-wide payment system that could be used for parking and other services.

[38] This implementation profile was developed by the Smart Card Alliance Terminal and eTransaction Infrastructure Task Force with the assistance of David deKozan, Cubic Transportation Systems, Inc., as part of the report, "Transit and Retail Payment: Opportunities for Collaboration and Convergence," October 2003.

San Francisco Bay Area TransLink[39]

In 1999, the Metropolitan Transportation Commission (MTC) of the San Francisco Bay Area awarded a contract for a regional fare collection system that provides a single smart card to be used on every transit system in the area. This project, in which one card can be used on all modes of transportation with numerous transit providers, is the only project of its kind in the United States.

The Bay Area covers nine counties and 100 cities and has a population of over 6 million people living in an area of 7,000 square miles. On an average weekday, about 1.5 million rides are taken on public transportation. The area includes eight major transit operators and an additional 18 smaller operators.

Approximately 7,000 contactless smart cards, called TransLink cards, have been distributed for Phase 1 of the project. Phase 1 encompasses the six largest transit operators in the San Francisco Bay Area and involves certain buses, light, medium, and heavy rail, and ferries. The travel routes selected for the Phase 1 implementation include transfer points between the six Phase 1 operators, to enable passengers to experience the benefits of an integrated fare collection system using the contactless smart card. This first phase has been operating since mid-2002. In June 2002, the entire San Francisco Muni Metro system was commissioned to accept the TransLink card. Phase 2 of the project commenced with an expansion of the program for two of the transit agencies. Work is also underway to integrate the smart card into existing Bay Area Rapid Transit (BART) system fare gates. Ultimately, up to 26 transit operators could participate in the program.

The Phase 1 system comprises over 1,500 pieces of equipment, including card processors, add-value machines, portable hand-held readers, ticket office terminals, and point-of-sale (POS) devices for use at retail outlets. Phase 2 of the project will involve almost 9,000 pieces of equipment. The add-value machines and selected card processors provide audio in two languages to assist the hearing impaired. Keys on the add-value machines and some card processors also include Braille, to assist the visually impaired.

The card being used complies with ISO/IEC standards for smart cards, including ISO/IEC 7816 and ISO/IEC 14443 Type B, and contains 4 kilobytes of internal memory for data and application storage. The card is a dual-interface card, containing both contact and contactless interfaces for communicating with the card's microprocessor. For the transit system, the contactless interface is essential, providing ease of use and fast boarding times. The contact interface allows the card to be used for other applications, such as at ATMs or POS terminals, where a contact slot already exists or is more acceptable. For example, the third-party merchants that provide card reload facilities use off-the-shelf POS terminals with a built-in contact smart card slot.

A central clearinghouse and service bureau operates and manages the smart card system. This facility processes all transactions and settles payments on a daily basis between all participants in the program. Every 24 hours, transit operators receive payment for the day's activities and have access to

[39] This implementation profile was developed by the Smart Card Alliance Terminal and eTransaction Infrastructure Task Force with the assistance of David McIlwraith, ERG Group, as part of the report, "Transit and Retail Payment: Opportunities for Collaboration and Convergence," October 2003.

detailed financial and operational reports, down to the individual transaction. The service bureau provides all cardholder, transit agency, and merchant support services. Cardholders can order and reload their smart cards using a variety of means, including telephone, mail, the Internet, and "autoload." Reload locations are located throughout the region at transit customer service locations, add-value machines, and third-party merchants.

In June 2002, a focus group of TransLink Phase 1 pilot program participants was asked whether they would vote for TransLink to be launched region-wide if they were in charge of Bay Area transit. The participants in the focus group unanimously responded yes. Overall, the focus group was very positive about the TransLink program.

It was always envisioned that the smart farecard would be expanded to carry applications beyond the initial transit application. The first instance of this expansion is parking, with the smart card reader being integrated into new electronic parking meters to be installed in San Francisco in 2003 and 2004. The TransLink card can then be used to pay at parking meters throughout the city. The pilot program for the smart card-enabled parking meters started in early 2003.

Other applications being investigated are tolling (MTC also administers the tolls for the six major bridges in the region), taxis and retail payment.

Ventury County Transit Smart Card[40]

Ventura County, California, covers an area of 1,873 square miles with 43 miles of coastline. Public transportation serves the communities of Ventura, Oxnard, Simi Valley, Thousand Oaks, Moorpark, Camarillo, Santa Paula, and Fillmore. The population of Ventura County is 742,000, making the county the 12th most populous county in California. Within Ventura County, the Ventura County Transportation Commission manages six transit operators, with service that crosses into Santa Barbara and Los Angeles counties. The six operators are Ventura Intercity Service Transit Authority (VISTA), South Coast Area Transit (SCAT), Simi Valley Transit (SVT), Thousand Oaks Transit (TOT), Camarillo Area Transit (CAT), and Moorpark City Transit (MPT).

In 2000, the Ventura County Transportation Commission awarded a contract to the Motorola/ERG alliance to supply an AFC system using smart cards. The proposed system combined the smart card fare medium with automated passenger counting and Global Positioning System (GPS) location. In late 2001, the Motorola portion of the contract was transferred to ERG, with ERG assuming sole responsibility for the contract.

A total of 330 pieces of equipment have been installed and put into revenue service since January 2002. This equipment includes on-bus smart card readers, driver's consoles, and automated passenger counters. A network of 19 POS terminals allows cards to be purchased and reloaded. In addition, passes and epurse values can be loaded remotely. This capability allows reloading to occur automatically when the smart card is tagged on a bus.

A total of 10,000 cards have been supplied, and additional cards are in procurement for the current year. The cards in use are dual-interface smart cards with 4 kilobytes of memory and comply with the ISO/IEC 7816 and ISO/IEC 14443 Type B standards.

In addition to collecting fares, the system includes automated passenger counting equipment that provides GPS location data and passenger entrance and exit counts.

The campus of California State University Channel Islands (CSUCI) has its own version of the smart card. The card is used for transit on the VCTC system and serves as a student identity badge for use on campus. The student smart cards carry two epurses—one for transit and one for use on campus. The campus epurse will be suitable for small transactions typical at a university, such as those at vending machines, photocopiers, cafeterias, and for computer services. Other potential uses of the card include on-campus parking and building access.

The student smart card allows university students to travel on the buses free of charge. The system records all bus rides taken by students using their cards. This record is used to reimburse the transit agencies, using funds provided by the university.

[40] This implementation profile was developed by the Smart Card Alliance Terminal and eTransaction Infrastructure Task Force with the assistance of David McIlwraith, ERG Group, as part of the report, "Transit and Retail Payment: Opportunities for Collaboration and Convergence," October 2003.

Washington Metropolitan Area Transit Authority – SmarTrip[41]

The Washington Metropolitan Area Transit Authority (WMATA) operates the second largest rail transit system and the fifth largest bus network in the United States. The Authority was created in 1967 by an interstate compact to plan, develop, build, finance and operate a balanced regional transportation system in the National Capital area. Construction of the Metrorail system began in 1969. Four area bus systems were acquired in 1973. The first phase of Metrorail began operation in 1976. The final leg of the original 103-mile rail network was completed in early 2001. Metrorail operates 83 stations.

Metrorail and Metrobus serve a population of 3.5 million within a 1,500 square mile area. The transit zone consists of the District of Columbia, the suburban Maryland counties of Montgomery and Prince George's, the Northern Virginia counties of Arlington, Fairfax and Loudoun, and the cities of Alexandria, Fairfax and Falls Church. Overall, 41 percent of those working in the center core, Washington and parts of Arlington County, use mass transit.

WMATA launched a contactless smart card called SmarTrip® in May 1999, with the broad objective of making transit travel easy, simple, and attractive for the customer. Just over four years later, more than 360,000 travelers have switched from paper to plastic, using smart cards to pay MetroRail system fares and Metro-operated parking lot fees. From the customer perspective, SmarTrip's success can be credited to the convenience of the card in terms of transaction speed, durability, reload capability, and ease of replacement if the card is lost, stolen, or damaged.

In the long term, WMATA is focusing on moving away from being a card-issuing organization to a card-accepting organization. In the short term, WMATA is the lead agency in promoting contactless smart cards as the payment tool for transit in the National Capital region. The largest functioning contactless transportation application in the U.S. is SmarTrip, which operates in metropolitan Washington, D.C. Since May 1999, sales at a limited number of facilities and an Internet site have remained steady at 6,000 to 8,000 cards per month. The only significant system enhancements have been the addition of card readers to all entry and exit gates in the MetroRail system (in March 2000) and of SmarTrip-equipped express exit gates at many of WMATA's parking facilities. The ability to use the card at any gate had a clear impact on card awareness and acceptance and on utility to the customer.

Contracts are in place throughout Washington, D.C., Northern Virginia, and the state of Maryland to populate 15 additional operators with SmarTrip-accepting infrastructure (provided by Cubic Transportation Systems, Inc. and ERG Group).

Since the introduction of the SmarTrip card, several pilot projects have been conducted to test the viability of multi-application cards that include transit fare payment. As part of an agreement with First Union National Bank in 2000, 1,000 cobranded cards were issued. The cards could be used both as a contactless transit payment card in the WMATA system and as a magnetic stripe debit card for banking transactions or for card reload for transit use.

[41] This implementation profile was developed by the Smart Card Alliance Terminal and eTransaction Infrastructure Task Force with the assistance of Greg Garback, WMATA, as part of the report, "Transit and Retail Payment: Opportunities for Collaboration and Convergence," October 2003.

The cards were reissued to participants in 2002 and the pilot successfully concluded in August 2003.

Survey data gathered from cardholders indicated that the consolidation of functions on such a multi-application card was an attractive feature and would lead to increased use of the card. Satisfaction levels with the card were high for both the bank and the transit operator. There was some indication that the card could be a moderate draw for new customers. However, use levels for the card did not change for either the bank or the transit operator.[42] While other financial institutions have shown interest in similar types of initiatives, no additional combination transit-banking cards have been developed.

WMATA has also entered into pilot projects with the U.S. General Services Administration and U.S. Department of Education for a cobranded combination transit-building access card. These projects were initiated in 2000 and 2002, respectively. They include approximately 2,000 cardholders between the two agencies and continue to operate today.

WMATA customer surveys have found very high levels of acceptance and satisfaction with SmarTrip. The convenience, speed and utility of the SmarTrip card, coupled with WMATA's attention to customer service, has led to a 99% customer satisfaction index.

[42] Steve McKinney, Enterprise Knowledge Research Group, February 2001.

Publication Acknowledgements

This report was developed by the Smart Card Alliance to provide examples of successful implementations of smart cards. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The case studies and implementation profiles included in this report were compiled from a number of Smart Card publications. The Smart Card Alliance wishes to thank members of the Secure Personal ID Task Force, the Terminal and eTransaction Infrastructure Task Force and the Digital Security Initiative for their participation in Smart Card Alliance projects.

Trademark Notice