GLOBALPLATFORM

THE STANDARD FOR SMART CARD INFRASTRUCTURE

CASE STUDY

Overview

In 1999, the US Department of Defense (DoD) began work on a program to issue a smart, common-access identification card to 4.5 million Active Duty, Selected Reserve, DoD civilian and eligible Contractor personnel.

The Common Access Card, or CAC, as it is referred to, is a smart card program designed to serve as a standard DoD ID card, enabling physical access to buildings and controlled spaces, and for logical access to the Department's computer networks and systems.

The driving factors for the development of this project involved issues of information assurance and the reduction of fraud associated with the current Armed Forces ID card. A smart card would improve the security of physical and logical access and enable e-commerce to become a possibility. The subsequent reduction in paperwork and decreased transaction and business process time would lead to an increase in efficiency and, overall, reduce costs.

One challenge was to design an interoperable and secure multi-application smart card that would function as a military ID card and ensure it complied with the Geneva Conventions. Cost was also a consideration while addressing this challenge and while the DoD considered creating a proprietary government specific approach, they eventually decided to adopt best commercial off-the-shelf (COTS) products adapted to the DoD environment. The ultimate goal was to be able to use a CAC anywhere that the cards are accepted, regardless of which Government Agency issued it.

The 1,500 workstations issuing the military ID cards would need to be upgraded to issue the more secure smart cards and up to 200 additional registration workstations included to provide issuance to the military as well as the DoD civilian and contractor personnel that had not been served by the existing card issuance workstations.

Approximately four (4) million participants are involved in the DoD's CAC program.

Active Duty Military personnel, Select Reserve personnel, DoD civilian employees and approved contractors are the initial recipients while the potential population is approximately thirteen (13) million.

The first Beta site was established at Quantico, Virginia, USA on October 2nd, 2000. By mid-2001, the CAC card was operational at 70 Beta sites. An accelerated rollout began. All workstations and sites were deployed by the end of May 2003. As of August 2006, more than 11 million CAC cards have been issued at a rate of approximately 10K cards per day. The cards have been issued on a decentralized basis at over 1,000 sites in 27 countries and 2,000 workstations.

Development of the Solution

The infrastructure for this program is extensive with 933 locations worldwide producing the DoD ID cards on demand. This global network manages the equipment, supplies and trained personnel to provide ID cards to all Uniformed Service members from the US Army, Air Force, Navy, Marine Corps, Coast Guard, Public Health Services (PHS) and National Oceanographic and Atmospheric Administration (NOAA), including Active Duty and guard/reserves personnel. In addition, family members eligible for benefits and retirees are provided with ID cards. To add to the challenge, each facility has its own set of procedures for providing separate organizational badges for building access.

The smart card technology had to be integrated into the Defense Eligibility Enrollment Reporting System (DEERS)* and the Real-Time Automated Personnel Identification System (RAPIDS)*, which are two independent, but closely aligned, systems providing eligibility information for DoD benefits. RAPIDS and DEERS needed to be redesigned to allow for the issuance of CAC through the RAPIDS software. This redesign, already underway, includes 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 – not to mention training.

So what were the issues addressed?

An integration issue to be addressed was that the different Military Services maintain their own networks, firewalls and communications infrastructure, which provided a unique challenge to establish seamless integration without jeopardizing network performance and cardholder service levels.

In addition, information assurance, fraud reduction and the facilitation of electronic commerce needed to become a part of the solution.

Establishment of identity is a basic business function and with an ever-increasing dependency on the Internet, this became a high priority for the DoD. Strong authentication, such as the large-scale PKI program established across the Department for sensitive, but unclassified data was introduced to improve information security and address one of the CAC's two main issues.

The use of software tokens to be issued on floppy disks was proposed to satisfy the need for digital signatures, however, it was determined that this would be an expensive solution requiring the development and fielding of a complex face-to-face registration system to verify every participant. DoD determined that migrating to a hardware-based token solution, where the cryptographic certificate material and private keys could be stored, was the more secure solution. This solution also solved the second problem that the existing military ID card was increasingly prone to fraud through the ability to copy, duplicate or manufacture fraudulent cards.

Why Smart Card Technology?

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.

PCMCIA (Personal Computer Memory Card International Association) cards, USB tokens, software tokens and smart cards were all technologies considered. PCMCIA cards provided the highest level of security and performance, but had significantly higher infrastructure costs and were not the preferred format. They were not wallet size, nor did they allow for a photograph. USB tokens
provided strong security, a ubiquitous interface to new PC platforms, and were already 3rd 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, however, they were deemed inadequate for their limited security features and portability. The fourth technology considered was smart cards, appealing because of their relatively low cost, robust security features, versatility and variety.

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 would 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 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 offered by the smart card was that because of format, the card functions as an ID card as well as a physical and logical access card. The multiple technologies, such as ICC, bar codes and magnetic stripes, which are included on the smart card platform, also facilitated integration with the legacy systems providing a strong economic business case.

The Implementation

Prior to starting any implementation of the project, the DoD defined their requirements in terms of the CAC platform specifications, the available smart cards and required production of hardware, firmware and software. The DoD's business-based approach enabled business process reengineering (BPR) and streamlining of their operations to achieve performance improvement targets, such as improved security, a reduction in infrastructure, mission enhancement and increased customer satisfaction.

As the DoD commenced the CAC project, they relied heavily on advice from the industry. In particular they worked closely with Visa and Sun Microsystems to secure business intelligence on the viability, security and robustness of the GlobalPlatform specification. ActivCard was also involved to help craft the card applets and the issuance process, both of which were developed around the GlobalPlatform Card Specification v2.0.

The infrastructure requirements necessary to deploy a PKI, requiring face-to-face verification of all its users along with a coordinated database that could uniquely and reliably identify and verify each individual, were extremely costly. However, by leveraging the existing ID card infrastructure, which was an integrated solution, the Department was able to achieve economies of scale allowing for business process reengineering combining three core functions; identification, PKI and physical access, and their respective issuance infrastructures into a single process.

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 card has 32 kilobytes of EEPROM (Electronically Erasable Programmable Read Only Memory) with a cryptographic co-processor capable of generating keys via digital signature with approved cryptoalgorithms. The operating system is Java 2.1 and the security and the card protection software conform to GlobalPlatform Card Specification v2.0.

"The inclusion of the GlobalPlatform specification in the Common Access Card program was the catalyst that jump started the development program and eased the fears within the Department about the security and interoperability of the DMDC solution," commented Rob Brandewie, Deputy Director, Defense Manpower Data Center.

Smart card usage and applications are based on an open systems configuration, interoperable with commercial and Government/Service applications and are consistent with commercial industry standards. The CAC 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.

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 to be completed by January 2001. Due to technology issues, Phase I of the Beta testing was initiated in October 2000 and Phase II started in March 2001. Finalizing the CAC configuration for the fielded version was targeted for the September-December 2000. Rollout to more than 900 sites worldwide was targeted for the fiscal year 2001, with complete deployment in 2003.

To date, the DoD has issued 11.2 million CAC cards at a rate of approximately 10K cards per day. The extensive issuance infrastucture has now reached 1,000 sites in 27 countries.

The Results

Driven by the need to improve business processes and provide heightened security to networks and systems, the DoD employed state-of-the-art technology. The embedded solution has yielded cost savings, improved readiness and increased quality of life. Solving the fraud and information

assurance problems on their own 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 whilst supporting the business case for both needs. With the adoption of PKI, the use of the Internet to transfer data securely and perform online transactions has become more reliable and more frequent.

The Department's approach uses COTS technology following the best industry practices. The card platform and architecture mirror the approach of the card industry with early adopters including Fleet Bank's "Fusion", Visa's credit card, First USA Bank's "Smart Visa", as well as American Express' "Blue" card program. Sun Microsystems "Sun Badge" corporate ID card, issued to all Sun employees worldwide, is also based on the same platform approach.

This approach is standards-based utilizing IETF (Internet Engineering Task Force), ISO International Organization for Standardization), ANSI (American National Standards Institute) and GlobalPlatform Specifications, which has allowed for multiple vendors to competitively supply smart cards, readers/encoders, software and other equipment for this program. Furthermore, the DoD is leveraging the economies of scale of these large organizations. As an example, Visa has one billion cardholder accounts worldwide enabling low-cost, common solutions to continue to improve the economies 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 cards as an ID card and to gain access to the newly emerging Navy-Marine Corps Intranet (NMCI). As requirements change via legislation or policy, the ability to evolve the CAC without re-issuance has vast economic benefits.

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

The next steps for the DoD are to utilize the CAC cards for signing and encrypting email and to expand the number of portals capable of doing web-based ebiz using PKI authentication tools. The aim is to include a biometric in FY 2004 for three factor authentication – what you have (i.e. the card), what you know (i.e. a password or PIN), and who you are (i.e. the biometric). The Department is also looking at ways to cross-credential among federal agencies and between the DoD and industry partners.

Lessons Learned – MovingForward

Some key lessons learned from the implementation experience stem from 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/RAPIDS issuance portal. Maintaining connectivity between the RAPIDS workstations and issuance portals is vital to streamline the issuance process. When connectivity failed, stations were unable to issue CAC's, and at times, congestion at the portal significantly slowed down the issuance process.

User acceptance and "buy-in" is another critical success factor. To ensure the migration to the new CAC card was smooth, it was essential that users were educated about PKI, card functionalities and the goals of the program. Implementation displayed 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. 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 would permit all system users to fully capitalize on the enhancements provided by the ICC technology.

The implications for this program are already ispreading beyond the DoD. Private industry is adopting a similar model to provide an improved cyber identification credential for commercial and industrial e-commerce applications.

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

"DoD is a leader in the development of a sophisticated identity management infrastructure.The Common Access Card is at the very center of that infrastructure and is critical to the continued efficient and secure operation of the DoD's many computer systems and the key to emerging physical access systems." Rob Brandewie, Deputy Director DMDC.

Notes:

* DEERS 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/reserve personnel, and DoD civilians.

* RAPIDS is one of the principal means to update information in DEERS, established to produce a more secure method of generating ID cards. RAPIDS consists of a network of workstations and servers located in the Uniformed Services personnel offices and other selected locations worldwide. 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 mandate to create CAC, steps were taken to redesign RAPIDS and DEERS to allow for the issuance of the CAC through RAPIDS software for eligible personnel.

Sources

Department of Defense Common Access Card White Paper, October 2001

Department of Defense Common Access Card (CAC) Fact Sheet, January 2003

Smart Card Alliance Digital Security Initiative Case Study, 2002

DMDC Presentation on Identity Management, by Rob Brandewie, Deputy Director, Defense Manpower Data Center, January 2003

Excerpt of Interview with Mary Dixon, Director of the Department of Defense Common Access Office, at CardTech/SecurTech, May 2003

Rob Brandewie, July 2003 (Personal communication)