DIGITAL SECURITY INITIATIVE

CASE STUDY

Smart Card Alliance

Department of Defense to issue up to 13 million Common Access Cards for smart card-enabled PKI

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/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 four 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, VA. As of mid-2001, the CAC card was operational at 70 Beta sites. An end-to-end security analysis presently is underway and upon a successful evaluation, a roll-out will proceed to achieve initial operating capability.

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 US Army, US Air Force, US Navy, US

Marine Corps, US 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.

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/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/reserve, 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, non-repudable solution – 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 unfeasible. 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 will use 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 (not wallet size, did not allow for a photograph). USB tokens provided strong security, a ubiquitous interface to new personal computer (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, 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 ICC, 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 crypto-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 Admin-

istration (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's) 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 comprised 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 the EB BOD now 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.

COSTS 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 the best industry practices. The card platform and architecture mirror the approach of the card industry – which has started its rollout in the United States – with early adopters including Fleet Bank's "Fusion," Visa credit card, First USA Bank's "Visa Smart", as well as American Express' successful "Blue" card program. Sun Microsystems' "Sun Badge" corporate ID card – that is to be issued to all Sun Microsystems employees worldwide – is also based on the same platform/approach.

This approach is standards based utilizing IETF, ISO, ANSI and the Global Platform specifications, which has allowed for 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 these large organization. As an 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 cards as an ID card and 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/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. A full rollout is anticipated for Fiscal Year (FY) 2002 after a full security evaluation.

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/RAPIDS issuance portal. Further troubleshooting highlighted the criticality of appropriately sizing the 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 the 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 ICC 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. (2001, August 2). {Interview-personal communication} Dreifus Associates Limited, Inc.

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

CAC Execution Plan, June 14, 2000.

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

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

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

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

DoD Target Token Strategy, 8 March 2000.

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

Monk, Justin. (2001, July 30). {Interview-personal communication} Dreifus Associates Limited, Inc.

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

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