Secure Identity Management at the U.S. Department of Defense

White Paper
May 2003

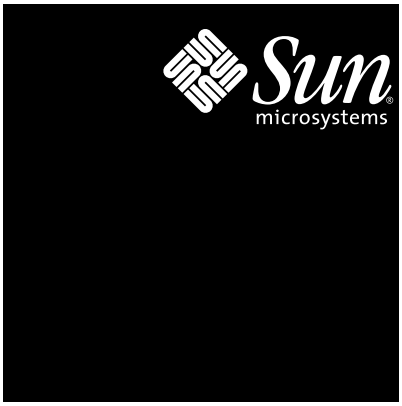


Table of Contents

Introduction 1

Based On Open Standards 2

Identity Management Goals 4

Using Current, Off-the-Shelf Technology 5

Identity Management Architecture 7

Architecture Overview 8

The DEERS Database 9

DEERS Architecture 9

RAPIDS Card Issuance Workstations 10

DMDC Issuance Portal 11

Issuance Portal Front End 12

Issuance Portal Back-End Systems 12

Certificate Authority 13

Common Access Card Issuance Process 15

Process Goals 15

Issuance Process Outline 16

Verification Officer Authentication 16

Potential Cardholder Verification 16

Card Initialization 16

Java Applet Loading and Instantiation 17

Card Usage 18

Securing Your Organization 19

References 21

Chapter 1

Introduction

There is no larger employer in the world than the United States Department of Defense (DoD). With more than 4.3 million uniformed service personnel and civilian contractors working at more than 40,000 locations in countries around the world, managing credentials that control everything from physical building entry to secure computing system access is a mammoth undertaking. With a workforce of this size, and with no less than national security at stake, the DoD faces a greater challenge than any corporation on the planet.

When the DoD decided to modernize their identity management system, they directed the Defense Manpower Data Center (DMDC) to design a Common Access Card (CAC) that could be used by all personnel in all of the armed services, including the Army, Navy, and Air Force. One challenge of the project was to consolidate the multiple identification and access cards that DoD employees must carry into a single card. Some functions — such as cryptographic keys for e-mail encryption — would be common to all cards, but the card would also need to be extensible so that individual services could tailor its capabilities to fit their own problem domain. For example, the Air Force might wish to incorporate pilot flight qualification information onto their access cards, and also prevent that information from being accessible at the commissary check-out stand.

The problem of creating a card that is secure, yet extensible, is compounded by many challenges faced by the DoD, including the need for high security, massive scale, worldwide deployment, ease of use, and integration with an existing personnel database with records on more than 15 million current and former employees along with 8 million of their dependents. Complicating the challenge further is that the card must operate with existing business processes that do not yet use digital data.

In the search for open, flexible, secure, and scalable identity management solutions, the DoD needed to look no further than Sun Microsystems and its affiliates. Knowing that security by obscurity is no security whatsoever, the DoD decided to use an open identity management solution that is based on the science of public-key cryptography and the security of Sun's Java™ technologies as embodied in its Java Card™ platform. By choosing an open platform, the DoD could adopt technologies that have been analyzed, tested, and challenged by virtually everyone, including academic institutions, cryptographers, and hackers, and thus found to be more secure than any system that depends on keeping knowledge of the system a secret. Indeed, the very fact the words in this paper can describe the DoD's solution is testimony to its openness.

Based on Open Standards

Sun has long based its business on creating open standards and then competing to provide the best implementation in the marketplace. The result is a vibrant, competitive industry that produces low prices, high quality, and product longevity. The DoD's choice of Java Card technologies as a basis for its CAC program not only gives it access to several competing card vendors; it also provides the long-term security that if one vendor goes out of business, there will still be multiple sources for the millions of cards the DoD will need to procure now and long into the future. Open standards also means the choice to mix and match vendors, and the DoD chose to use servers, software, and storage from Sun, and also software from its iForce℠ Certified Solution Partner ActivCard for card issuance and secure application access.

The quality and value of the DoD's access card implementation has been recognized by others within and outside of the U.S. Government. The Common Access Card program has been the recipient of more than ten awards, including:

- *Government Executive Award ('Gracie')* for demonstrating leadership in addressing privacy and security concerns
- *Federal CIO Council Excellence.Gov* for the first large-scale implementation of smart card technology for strong identification based on open specifications in the world
- *ComputerWorld Honors Program* for the use of information technology noteworthy for the originality of its conception, breadth of its vision, and significance of its benefit to society
- *Outstanding Smart Card Association (OSCA) Award* recognizing innovative and well-managed smart card implementations
- *PostNewsweek Tech Media Agency Award for 2002* based on innovation, ability to support program or policy requirements, improving service delivery, and acquisition and management of information technology

The purpose of this white paper is to tell the story of the DoD's Common Access Card program from the perspective of the systems, components, and tools that were used to deploy this innovative solution. The paper first discusses the goals and the challenges that the project's requirements imposed. Next, the solution's architecture is presented from the perspective of what systems are needed to support the card issuance process. Because the access card's security depends the most on the card issuance process, it is described in detail.

Most companies have significantly fewer employees and locations to manage than the U.S. Department of Defense, so the modularity and scalability of the DoD's framework is a great advantage — scaled-down versions of the DMDC's solution can be built and deployed with no compromise in security. As with the Department of Defense, any company can deploy secure solutions using Java technology, the Solaris™ Operating System, Sun™ Open Net Environment (Sun ONE) software, and products from Sun's iForce partners.

Chapter 2

Identity Management Goals

Within the U.S. Department of Defense, the Defense Manpower Data Center (DMDC) is responsible for identity management across all services, including 1.4 million men and women on active duty, 1.3 million volunteers serving in the National Guard and Reserves, 672,000 civilian employees and contractors, and 1.8 million retirees and families who receive benefits. The information that the DMDC maintains for each person not only determines access to secure facilities and computer systems; it also determines eligibility for valuable benefits including health care, use of military grocery and department stores, and access to recreational facilities.

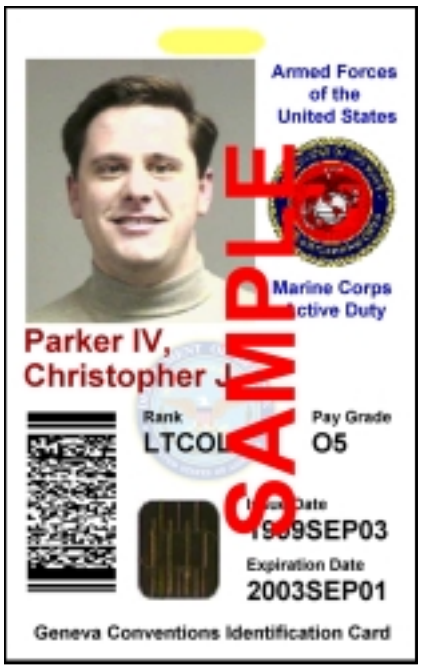
The mandate to modernize the DoD identification card presented the DMDC with both an opportunity and a challenge. With a secure identity card and integrated personnel records, the DMDC could provide technology to help the armed services streamline their own business processes. Improvements could be made so that, for example, lines of troops filing sequentially through processing stations at a troop readiness center could be made an image from the past. With a secure identity system, employees could update their own personal information, no longer requiring costly face-to-face time to merely make an address change. Access to sensitive systems could be authorized and secured through the use of public-key encryption for authentication, e-mail signing, and data encryption. Contracts could be signed and expenses approved with secure digital credentials. Where security requirements were even greater, a combination of cryptographic authentication with biometric data such as a fingerprint scan could be required. Finally, an ideal system would be flexible and extensible, allowing different services to customize the system for their own needs, with requirements yet unknown to the DMDC.

The challenge was to implement a system that could be incrementally deployed, without disrupting current business and authentication processes. The first and biggest challenge was to integrate a new secure identity system using the existing 23-million record Defense Enrollment Eligibility Reporting System (DEERS), a DoD-wide database that is central to personnel and benefits administration. The second existing system is known as RAPIDS, the Real-Time Automated Personnel Identification System, where ID cards have been issued for the last seventeen years. The new identity system would need to coexist with existing access systems for years to come, and would also have to continue to meet Geneva Convention requirements. As a result, the card's form factor and printed information had to be similar to existing cards — providing name, photograph, service, social security number, pay grade, rank, and information encoded in linear and 2-dimensional bar codes and a magnetic stripe. Any new features such as digital credentials had to be piggybacked onto the same form factor and work within a 10-minute time slot for issuance in order for the existing staff to support the new card. Finally, given that so many sensitive systems would depend on the authenticity of a new ID card, the issuance process had to be more secure, combining both face-to-face and biometric authentication.

Using Current, Off-the-Shelf Technology

In the past, the DoD might have addressed the problem with overly complex systems, closed implementations, or DoD-specific technologies. Mindful of these past mistakes, the DMDC surveyed the industry and quickly made some key decisions. The Java Card platform was chosen because it is an open smart card environment capable of securely storing cryptographic keys and identity information. Its 32-K bytes of EEPROM storage, combined with an on-board processor, cryptographic accelerator, and Sun certified Java virtual machine, could be used for the basic identity management functions of the DMDC with room to spare for future, service-specific applications. Plus, its standard credit-card size form factor is easy to carry, while providing the necessary space for printed information, bar codes, and a magnetic stripe used by legacy applications (Figure 2-1).

Figure 2-1: The DMDC's choice of Java Card technology enabled modernization while still providing the printed data required by Geneva Convention.



For secure loading of Java applets and on-card applet management, the Open Platform specification, the dominant technology in use by the credit card industry, was chosen as an industry best practice along with its implementation in products from ActivCard. Among the benefits provided by this software is the ability to create a firewall between multiple on-card applets, so neither bugs nor malicious behavior on the part of one applet could compromise the security of another. The Open Platform specification details a mechanism for loading Java applets where an encrypted tunnel terminates on the card itself, preventing any viewing or modification of the software or the data it stores as it is loaded through the tunnel onto the card. A final plus for the DMDC's decision is that this combination of Java Card technology and Open Platform software has passed the rigorous Federal Information Processing Standard (FIPS) 141 Level 2 certification process.

Java Card technology gave the DMDC a neutral, platform-independent mechanism for storing security credentials. When activated through insertion into a reader, the Java applets resident on the card can interact with the host system to provide a variety of services ranging from providing personal data to cryptographically signing e-mail messages. One of the key benefits of Java Card technology is that secret encryption keys never has to leave the card, where both the resident Java software and the physical microprocessor technology are designed to prevent successful hacking and physical tampering. Another benefit is the fact that encryption and identity applets can be designed to meet whatever cryptographic standards the DMDC requires — and can create new applets as requirements change.

The basic set of Java applets stored on cards issued by the DMDC include:

- Three instances of a Public-Key Infrastructure (PKI) applet where the private keys are securely stored on the card. These PKI applets are used for secure identification, e-mail signing, and e-mail encryption.
- One Personal Identification Number (PIN) applet that validates a PIN typed by the cardholder during the authentication process.
- Four instances of a generic container applet used to store demographic data ranging from date of birth to employment status. Demographic information is partitioned into four different applets, some of which contain personal data (such as blood type) and some of which contain personnel data (such as agency name and rank). For example, a recreational facility would have no need for blood type data and would be denied access to its container applet.

This set of applets enables the modernized DoD identity card to support existing applications today, and it also allows applications — such as building access and e-mail encryption — to be incrementally upgraded to use the new digital identification services provided by the card. Better yet, with the flexible Java Card platform, the card itself can be updated as new applications are created.

Chapter 3

Identity Management Architecture

There are two major aspects to the identity management system built by the DMDC to support its cardholders. One is the network architecture, including the computing systems and the services that each one of them provide. The other is the functional aspect, how the architectural components interact to provide the desired services. Because the card issuance process is so fundamental to the entire DMDC system, and because the identity card's security depends so completely on the security of the issuance process, this paper focuses on the architecture and process for card issuance. This chapter discusses the architectural aspect, and the following chapter outlines the flow of information during the card issuance process.

The story of the DMDC's secure identity management architecture is one of a work in progress, one that illustrates the value of open systems. Because the DMDC chose to use open systems and open standards in modernizing the DoD identity card program, it has the flexibility to change underlying systems and software as business needs change. For example, because of the high cost associated with scaling systems that were hosted in the past on IBM mainframes, the DMDC migrated to highly-scalable Sun Enterprise™ 10000 servers that provide mainframe-level technology (such as Dynamic System Domains) at lower cost. Because the certificate server supports industry-standard X.509 certificates, today it can use software that dates from the Sun-Netscape Alliance, and in the future it can use scalable, high-performance Sun ONE Certificate Server software. The interfaces don't change; the quality of implementation does.

When the DMDC began designing their identity management architecture, it was clear that a Web-based approach would carry them well into the future, and as a result, they adopted a portal-based architecture to support the various functions related to identity card management. This chapter discusses the architecture for the issuance portal accessed by the RAPIDS card issuance system. Other portals not discussed here include a post-issuance portal that helps keep on-card Java applets up-to-date, and a user maintenance portal that enables cardholders to update their own personal information, for example changing their mailing address or their PIN.

Architecture Overview

At the highest level, the DMDC's identity management architecture for card issuance involves four key components, each of which will be described in detail in this chapter (Figure 3-1):

- The DEERS database is the DoD's personal information database, which provides personal information for on-card storage and also helps to authenticate the potential cardholder through biometric data.
- 1300 RAPIDS workstations are deployed at 900 sites in 13 countries.
- The *certificate authority* issues, renews, suspends, revokes, and manages digital certificates and encryption keys that correspond to on-card certificates.
- The *issuance portal*, one of several different kinds of portals deployed by the DMDC, coordinates the card issuance process from allocating and ordering more blank cards to auditing every activity ever performed on a card. Both the issuance portal and the certificate authority utilize a Hardware Security Module (HSM) that serves as a secure lock box for all keys involved in the cryptographic operations required by the issuance process.

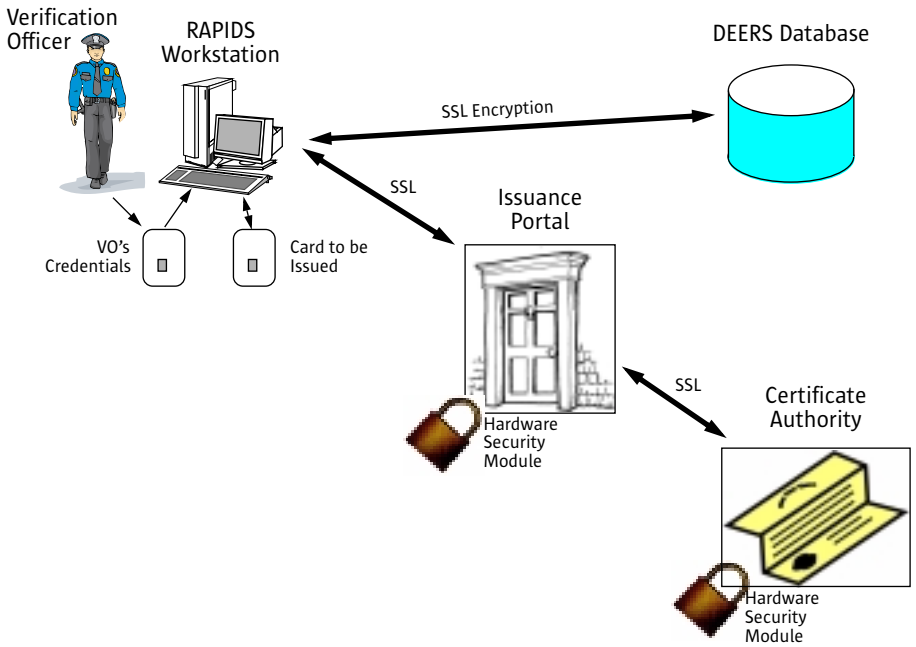


Figure 3-1: The DMDC's identity management architecture includes four key components.

The DEERS Database

The Defense Enrollment Eligibility Reporting System (DEERS) is the DMDC's central repository for personal information on DoD employees. It contains accurate, timely information on all eligible uniformed service members (active, reserve, retired), their families, and also some DoD civilian employees and contractors. The DEERS system acts as the DoD's personnel database, and provides information on both identity and benefit program eligibility. The DEERS database is a 24x7 operation because it serves a user community in multiple time zones. There are 25,000 authorized users throughout the DoD making more than 250,000 substantive updates every day.

DEERS Architecture

There are two main components to the DEERS infrastructure: the Oracle database and transaction-processing software that provides client access. Once hosted on IBM mainframes, DMDC has been moving DEERS components to Sun servers. As Bill Boggess, Chief of the Access and Authentication Technology Division at the DMDC points out, moving to Sun provided them the same production services (such as partitioned domains) as the mainframes they had been using, but with lower capital and operating costs. Using Linux on a mainframe would still require the cost of mainframe hardware and software experts, along with costs to administer the additional IBM virtual machine operating system necessary to support Linux.

The database was moved from IBM to Sun Enterprise 10000 servers about five years ago, while migration and modernization of the transaction-processing components continues. The DMDC must continue to provide a CICS interface into DEERS because of the requirements of its legacy clients. But today, the DMDC is rewriting its business rules using "Write Once, Run Anywhere™" Java technology, with the Sun Mainframe Transaction Processing tool supporting legacy interfaces to the DMDC's clients.

The architecture of the DEERS system reflects the fact that, with its key role in the Department of Defense, the database simply can't go offline. To achieve the high levels of availability required, DEERS uses clustering technology combined with redundant storage area networking (SAN) and Ethernet fabric that eliminate single points of failure. In order to enable the system to remain available even in the event of a regional disaster, the DEERs configuration and its data are replicated to a remote site.

The network architecture of one of the two sites is illustrated in Figure 3-2. A single Sun Enterprise 10000 server with approximately 36 CPUs and 15 GB of main memory is partitioned into two domains, one running the transaction-processing software and one running the Oracle database. Each domain is clustered with a 20-CPU, 8-GB Sun Enterprise 6500 server using VERITAS Cluster Server software.

Each server and domain has Fibre Channel connectivity to a pair of 16-port Fibre Channel switches, each of which has redundant connections to a Sun StorEdge™ 9960 storage system with 14 TB of disk space, currently upgrading to 21 TB of storage. One of the benefits of the Sun StorEdge 9900 series storage systems is the built-in features for replication to the remote data center and point-in-time snapshots for making consistent backups.

Each server and domain also connect to a pair of redundant Gigabit Ethernet switches that provide connectivity with clients as well as the tape backup system hosted on a Sun Fire™ V880 server and a Sun StorEdge L11000 tape library.

In addition to the production system described here, the DMDC has additional Sun Enterprise 10000 servers for staging and testing. Although the Sun Enterprise 10000 servers can host up to 64 processors, and the current system has significant headroom for scaling, the DMDC is in the process of upgrading to Sun Fire 15K servers, each with the capacity to scale up to 106 64-bit UltraSPARC® III processors.

RAPIDS Card Issuance Workstations

While the DEERS database acts as the central repository for personnel information, the Real-Time Automated Personnel Identification System (RAPIDS) workstations are the client systems used for issuing cards and updating personal information in the database. There are approximately 1300 RAPIDS systems deployed at 900 sites in 13 countries. One of the goals of the DMDC modernization project was to utilize the existing card issuance infrastructure, and there are plans to expand the number of card issuance workstations over time. Because these systems are in the field and not under direct control of the DMDC, they must never be allowed to store or view sensitive information. This feat is accomplished through the use of ActivCard Gold software and its implementation of the Global Platform specification, which enables the system to load applets onto the cards directly from the issuance portal, without the RAPIDS workstation being able to view or store the data in transit.

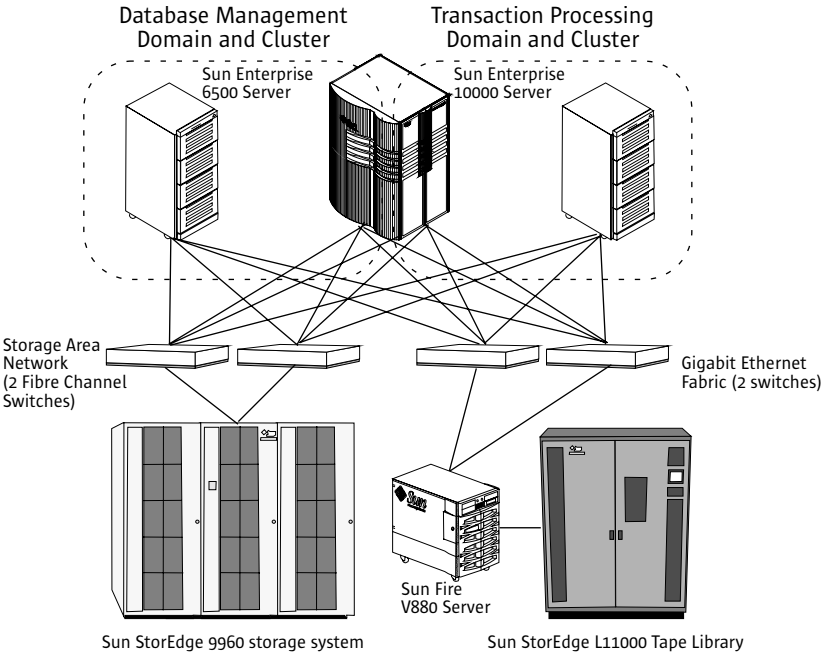


Figure 3-2: Each of two DEERS sites use dynamic system domains in Sun Enterprise 10000 servers, clustering, and redundant storage and Ethernet networks for high availability. Remote replication is accomplished through TruCopy software installed on the Sun StorEdge 9960 storage system.

As the following chapter explores, software running on the RAPIDS workstations authenticates a potential cardholder by comparing biometric data between the workstation and the DEERS database. It then coordinates between the DMDC issuance portal and the DEERS database to download Java applets into the card's EEPROM memory and instantiate them with personal information from DEERS.

Each RAPIDS workstation is a PC running DMDC-specific software along with ActivCard Gold and ActivCard Identity Management (AIMS) software, a modular, standards-based system that securely initializes and personalizes Java Cards with card applet management software, applet packages, and a variety of credentials. The RAPIDS workstations are PCs currently configured with a digital camera, fingerprint capture device, smart card reader, and smart card printer.

DMDC Issuance Portal

The DMDC issuance portal is accessed by the RAPIDS workstations during the card issuance process, and also handles inventory and audit functions. The portal is used to:

- Create a secure tunnel between it and the card to be populated
- Instantiate and personalize the Java applets to be stored on the card
- Interact with the certificate authority to request the cardholder's digital certificates
- Manage card inventory, automatically ordering additional cards as stock is depleted
- Maintaining a database that tracks every applet ever loaded onto a card, including size and version information
- Audit every action ever taken on a card, including initialization, changes, and destruction

With the issuance portal having to manage, initialize, and track millions of cards, the required infrastructure is beyond what most large corporations would need. As implemented by the DMDC, its size serves to illustrate how the design can scale up to serve millions of employees; because of its modularity, the portal can be scaled up or down depending on individual company needs. The issuance portal is built as a multitier Web services environment using JavaServer Pages™ technology, iPlanet™ Web Server, iPlanet Directory Server, and ActivCard Issuance Portal software, part of its AIMS software suite. ActivCard is currently updating the portal's implementation to incorporate the current versions of both Sun ONE Web Server and Sun ONE Directory Server software.

The issuance portal front end is currently hosted on a set of 13 PCs. The DMDC is in the process of consolidating the portal onto three scalable Sun servers so that they can reduce the number of platforms to support, lower administration costs, and increase reliability by using Sun's Solaris Operating System. The issuance portal architecture described in this section reflects the architecture currently being implemented using Sun servers. The back-end functions have been hosted on Sun servers from the beginning.

The planned issuance portal architecture is illustrated in Figure 3-3. It will include the issuance portal front end, back-end card data repository, inventory logistics, and key management systems. The inventory console will be used for the process of checking in new cards that arrive from approved vendors.

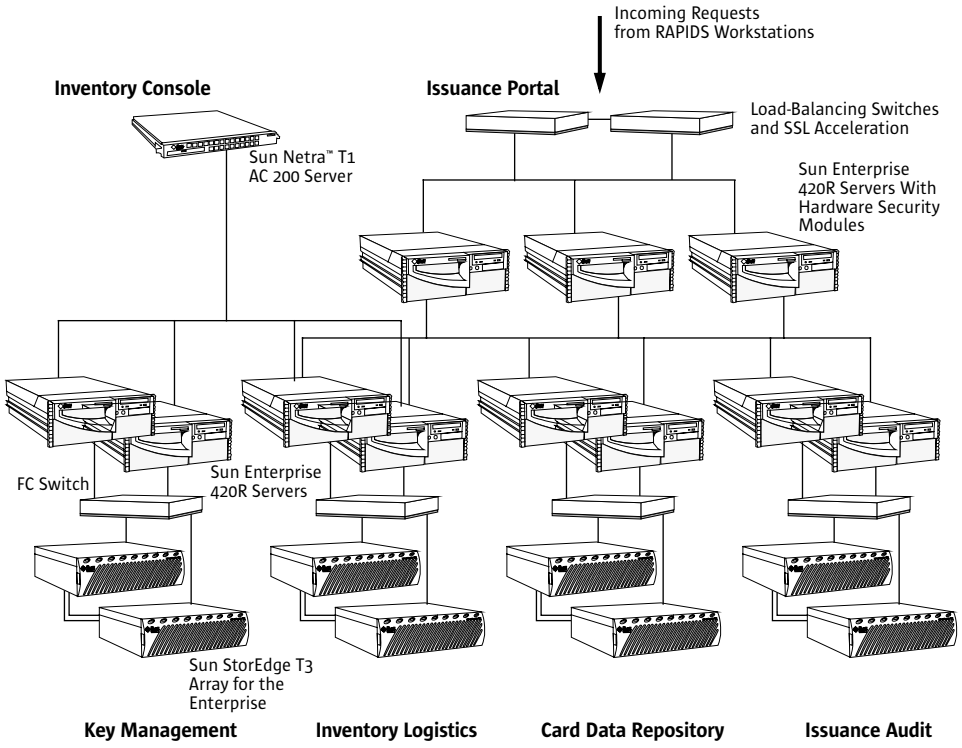


Figure 3-3: The planned issuance portal will be built as a multitier Web services environment, from load-balancing switches and front-end Web servers to back-end systems containing protected data.

Issuance Portal Front End

Incoming requests from RAPIDS workstations is load balanced across a set of issuance portal servers. The load-balancing mechanism includes two Lucent load-balancing switches with separate Ingrian secure socket layer (SSL) proxy modules that take the SSL encryption/decryption workload off of the issuance portal servers. The load balancers are deployed as a redundant pair to eliminate any single point of failure at this level.

The issuance portal software will be hosted on a set of three Sun Enterprise 420R servers with up to four processors. Each server will be equipped with a hardware security module that securely manages the keys needed to load software onto the cards. ActivCard's Issuance Portal software is written using JavaServer Pages technology, where the dynamically-generated Web pages will be served to clients via the Sun ONE Web Server. The issuance portal coordinates the interactions between the portal, the back-end servers, the client RAPIDS workstation, and the Java Card technology itself.

Issuance Portal Back-End Systems

The issuance portal uses a set of back-end systems for issuance audit, the card data repository, inventory logistics, and key management. Each of these four systems will be implemented using the same Sun server and storage technology as well as components from ActivCard's AIMS suite, and is designed to minimize points of failure:

- One Sun Enterprise 420R server provides services to the issuance portal, with a second server acting as a cold spare, able to boot and assume the IP address of the main server in the event of a failure.

- Each server has dual Fibre Channel interfaces to a single Fibre Channel switch. Each Fibre Channel switch, in turn, has dual connections to a Sun StorEdge T3 Array for the Enterprise.
- The Sun StorEdge T3 Array for the Enterprise is a configuration that uses two T3 Arrays with interconnected backplanes that allow the RAID controller in each array to access each array's storage. This configuration has no single point of failure. If one controller fails, the second controller can provide the same services as the first. Each Sun StorEdge T3 Array hosts nine 36-GB disk drives and is typically used with eight drives in a RAID 5 configuration and a hot spare that can immediately be populated with the data from any failed drive.

Inventory Logistics

The inventory logistics system tracks all cards up to the point of issuance, including their serial numbers, location, and manufacturer, helping to prevent any stolen or unauthorized copies of cards to be used. It manages inventory levels at all RAPIDS sites, making sure that adequate supplies are on hand, and ordering additional cards from approved vendors as needed. When a card is inserted into a RAPIDS workstation, the inventory logistics system verifies that it is a valid DoD card ready for issuance. Card inventory information is maintained in an Oracle database, all coordinated with ActivCard's AIMS Inventory and Logistics Portal software. The console for the inventory logistics system, enabling administrators to check cards into inventory, is hosted on a Sun Netra™ T1 AC200 server.

Key Management

The key management system enables the DMDC to take control of the master encryption keys for the cards. It manages its hardware security modules, storing the initial manufacturer keys for the card and the DMDC-issued keys as they are replaced. The key management system is based on AIMS KMS provided by ActivCard.

Card Data Repository

Once a card is issued, the card data repository tracks physical characteristics of the card (for example, the manufacturer and the amount of on-board memory), all software loaded onto the card and its version, and all changes to the card. The card data repository is consulted before any applets are loaded onto the card to verify that adequate memory space exists.

Issuance Audit

The issuance audit system tracks every operation ever performed on a card, including software downloads, personal data changes, and PIN changes. This log provides a complete audit trail for monitoring cards in the field, and is maintained by ActivCard's AIMS Audit Server software.

Certificate Authority

The certificate authority is managed by the Defense Information Security Agency (DISA) and it is a key player in the use of digital certificates and encryption to automate business processes using the new common access card. The use of standard X.509 certificates enables both secure access to Web sites internal to the DoD, but also supports e-mail signing and encryption that is enabled by the common access card. Some of the functions that the certificate authority provides include:

- Presenting cardholder certificates to users and systems that request them, so that the public keys contained within can be used for secure communication with the cardholder.

- Signing certificates to validate their authenticity, which enables secure e-mail signing, encryption, and identification using public keys for which the private keys reside on the common access card.
- Hosting a data recovery manager that will divulge an escrowed, asymmetric, e-mail encryption key when authorized by a sufficient number of officers with the right level of authority. Keeping e-mail encryption keys in escrow enables the historic — and perhaps strategic — value in encrypted e-mail messages to be retrieved in the event that the cardholder or the card is lost.

The certificate authority is just as essential to operations within the Department of Defense, and hence its infrastructure is replicated at two separate sites. Each location uses four Sun Enterprise 3500 servers: a directory server that publishes certificates, an e-mail signing certificate authority, an identification certificate authority, and a data recovery manager. These servers are equipped as necessary with hardware security modules for secure key storage. The software running on these four servers includes early versions of products that later became Sun ONE Certificate Server.

Chapter 4

Common Access Card Issuance Process

One of the most complex processes that support the new common access card is card issuance. This process utilizes every component of the DMDC's identity management architecture, and serves to illustrate how each component contributes to the overall goal of enabling secure authentication and encryption for everything from building access to automated business processes. This chapter illustrates the sequence of activities that occur in order to issue a card, which also serves to illustrate the extent to which the DMDC has gone to protect the security of the common access card.

Process Goals

The goal of the card issuance process is to:

- Make the card usable only by the Department of Defense
- Load and instantiate Java applets onto the card
- Issue digital certificates and put certain private keys into escrow
- Ensure that the card is issued to the correct person
- Track the card so that only DoD-approved applications can access the card's applets and update their contents

Issuance Process Outline

The issuance process is designed so that two people must be physically present in order to issue a card: the verification officer and the cardholder.

Verification Officer Authentication

1. The Verification Officer (VO) inserts their identity card into the RAPIDS workstation and authenticates to the system through possession of the card, typing in a PIN, and providing a fingerprint scan.
2. The DEERS database is consulted to see if the person can assume the role of VO, and provides fingerprint data for the RAPIDS system to match with the fingerprint scan. This, and all future connections to the DEERS database, are made using an SSL connection using the on-card certificate identifying the VO.
3. The issuance portal is consulted to see if the VO has authority to request certificates, one of the operations that will take place during the card issuance process. The connection is made using SSL with the on-card certificate belonging to the VO. In turn, the issuance portal contacts the certificate authority using a separate SSL connection to verify that the VO is indeed authorized to issue cards.

Note that, to this point the VO has been identified based on possession of the card, fingerprint, and PIN matching, and then two different independent systems have been consulted to authenticate the VO and enable the role to be assumed. The VO is now able to issue a card.

Potential Cardholder Verification

1. The VO meets the potential cardholder, compares the person with the photo on an existing ID card, and then compares the photo with the one retrieved by the RAPIDS workstation from the DEERS database.
2. A fingerprint scan is taken and compared to the data stored in the DEERS database.

Card Initialization

1. The VO takes a new Java Card technology-based ID card from inventory and inserts it into the RAPIDS workstation.
2. The Geneva Convention-specified information is first printed onto the card. A Code 39 (linear) and a PDF 417 (2-dimensional) bar code is printed, and a magnetic stripe is initialized so that the card can be used for the many DoD applications not yet using the digital data stored on the common access card.
3. The RAPIDS workstation contacts the issuance portal, which accesses information on the card from the inventory logistics system. The inventory logistics system tracks cards until they are issued and controls them up to the point at which they are activated. This tracking helps prevent any Trojan horses from being loaded on the card before it is issued, and any stolen, duplicated, or unauthorized cards from being used.
4. The issuance portal indicates to the RAPIDS workstation that the card is indeed a valid DoD card and logs the action to the issuance audit system. (Individual audit system entries will not be noted from this point on).
5. The issuance portal moves card tracking information from the inventory logistics system to the card data repository, which will track the card throughout its lifetime, including applets loaded, version numbers, updates made, and memory available.

6. The hardware security module connected to the issuance portal allows the ActivCard software to set up a secure, encrypted tunnel from the issuance portal directly to the software on the card itself. The session is encrypted on the HSM itself with the manufacturer's key so that the portal can load new key material through the tunnel without the possibility of it being intercepted or modified by the RAPIDS workstation. Besides the HSM, the only other holder of the manufacturer's key is the card itself. This system is part of the Open Platform specified by Visa International, and is one of the critical features that helps ensure card security.
7. A Global Platform key swap operation is conducted, which results in the manufacturer's key being replaced by a DoD-issued key. The manufacturer can no longer access the card for any reason, and the only applications able to interact with the card are those in possession of one of the DoD keys. This key is kept in HSM devices so they cannot be arbitrarily copied or used for unintended purposes.

An additional level of security provided by the Open Platform specification is the firewalling of applets on the card itself. This prevents any malicious action on the part of one applet from being able to access or compromise the security of any other on-card applet.

Java Applet Loading and Instantiation

1. Three Java applets are loaded into the new card: a public-key infrastructure applet, a PIN management applet, and a generic container applet. These applets are loaded using the DoD encryption key stored in the issuance portal's HSM.
2. Four instances of the generic container applet are instantiated, and different subsets of the cardholder's personal information are stored in different object instances using information from the DEERS database. The different information subsets are protected with different access rules.
3. The PIN management applet is instantiated with a user PIN that can be typed by the cardholder to verify that the cardholder is present when the card is used.
4. Two instances of the PKI applet are created for e-mail signing and identification. For each instance, the applet creates a public/private key pair using its cryptographic accelerator. Once the pair is generated, the public key is sent through the encrypted channel to the issuance portal, which contacts the certificate authority to generate and sign an X.509 certificate using the public key and the personal information for the cardholder obtained from the DEERS database. Once the certificate is issued, it is passed to the issuance portal. The issuance portal returns it to the on-card PKI applet, which now holds a copy of the entire identity certificate.
5. An instance of the PKI applet is created for e-mail encryption. The e-mail encryption key pair is generated in the HSM on the issuance portal and sent back over the encrypted channel to the card for injection using the Global Platform's protocol for secure injection of key material. It is also encrypted and sent to the certificate authority for escrowing. This allows e-mail to be decrypted in the event that the card or the cardholder is lost for any reason. Two authorized officers must be present in order to access the escrowed key.

   E-mail content is encrypted using symmetric keys that are generated for each e-mail message and passed to the recipient in the e-mail body itself using the S/MIME standard and encrypted using the recipient's public key.
6. The process ends with the card being presented to its holder.

Card Usage

The newly issued card can be used by the cardholder for all legacy DoD applications, as well as for a growing number of new ones. For example, using the ActivCard Gold product, e-mail can be encrypted and signed using a private key known only to the Java applet stored on the card itself. Business processes can be automated by using digital signatures for everything from expense report approvals to contract signing. Depending on the level of security required, applications may request a PIN to be entered by the cardholder and verified with the PIN applet, or they may request a fingerprint scan that is verified with the copy stored in the DEERS database.

Chapter 5

Securing Your Organization

The story of secure identity management at the United States Department of Defense is one that illustrates how Sun ONE software and products from Sun's affiliates can be used to build an identity system of massive scale, able to support more than 4 million users worldwide. It illustrates how products implementing open standards — including Java technology and the Java Card platform — enable integration between state-of-the art security systems and legacy platforms, including DEERS and RAPIDS. It is a story about how open standards support choice — choice to migrate from closed, legacy systems to open standards-based systems embodied in Sun ONE software and the Solaris Operating System; and even choice to use products from Sun's competitors. The DMDC story shows how open standards can be used to implement security solutions robust enough to protect U.S. national security. But first and foremost, the DMDC's secure identity management system illustrates how security systems strong enough to protect the U.S. Department of Defense are available for use by organizations large and small, supporting the most minimal to the most stringent security requirements.

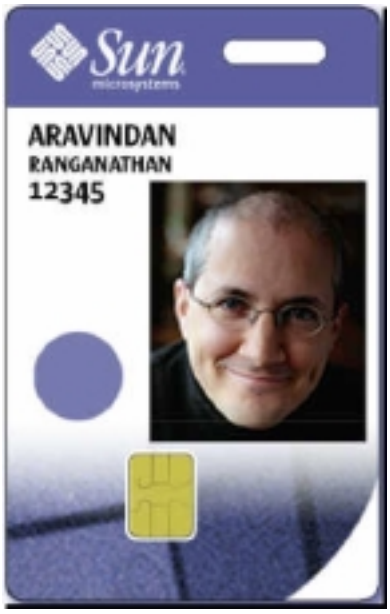
Using off-the-shelf servers and software from Sun and its affiliates, companies can implement identity management systems just as secure as the U.S. Department of Defense and use them for their own specific purposes, including secure authentication of workstations, servers, Web sites, and physical building access. Using Sun ONE software and modular components including ActivCard Gold client software, FIPS-approved Java applets, and ActivCard's AIMS suite, organizations can integrate with legacy database systems and third-party physical security products to build an integrated identity management system of their own.

Sun Microsystems itself provides an example of just how easily this can be done. Sun is in the process of updating its own identity management system to use Java Card technology and modular software products from ActivCard to integrate its own personnel systems, card issuance workstations, and building access software to leverage the benefits of a single, secure access card for all corporate functions (Figure 5-1). Examples of how Sun's own use of Java Card technologies will benefit its organization include:

- Workstations, servers, and Web sites can be securely accessed using standard X.509 certificates stored on the Java Card platform for secure authentication to systems running the Solaris Operating System, Sun Ray™ appliances, Linux, Apple Macintosh, and Microsoft Windows platforms. Solaris technologies like Pluggable Authentication Modules (PAMs) can be used to flexibly configure the authentication mechanisms required for access to the system, including login/password, smart card insertion, and biometric verification, in any combination. Once authenticated, technologies like Kerberos can be used as a network single sign-on mechanism.
- Remote access can be provided using Web single sign-on mechanisms implemented using Java technologies, and VPNs can be set up using on-card encryption keys.
- Employee demographics stored on the access card can be used to automate business processes, including travel and expense report handling.
- Using modules integrating with Sun's existing physical access control software, employees can access authorized areas using either a magnetic stripe printed on the card or with the proximity-activated circuitry of the Java Card platform.
- Finally, even food at the company cafeteria can be purchased by deducting value from a secure e-cash applet loaded onto the access card.

The most remarkable aspect of the story of secure identity management at the U.S. Department of Defense is that the strongest security and identity systems found anywhere are available to ordinary users and companies with just a phone call. The Sun℠ Services organization has years of experience implementing security systems for companies worldwide. With affiliates like ActivCard and the experience of its Java Center℠ architects, Sun can create both off-the-shelf and custom solutions for customers of all sizes. With the DMDC's massive scale, 24x7 availability, and stringent security requirements standing as testimony to the power of open solutions, companies know to choose Sun when implementing secure identity solutions of their own.

Figure 5-1: Sun is consolidating its many access cards onto one — the Java Card platform.



Chapter 6

References

Sun Microsystems posts complete information on Sun's hardware and software products and service offerings in the form of datasheets, specifications, and white papers on its Web page at *http://www.sun.com*. Please refer to the following URLs for more specific information on:

- Sun software, *sun.com/software*
- Solaris Operating System, *sun.com/solaris*
- Sun Server technology, *sun.com/servers*
- Sun Storage products, *sun.com/storage*
- ActivCard's identity management products, *activcard.com*

Learn More

Get the inside story on the trends and technologies shaping the future of computing by signing up for the Sun Inner Circle program. You'll receive a monthly newsletter packed with information on the latest innovations, plus access to a wealth of resources. Register today to join the Sun Inner Circle Program at sun.com/joinic.

To receive additional information on Sun software, products, programs, and solutions, visit sun.com/software.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 800 786-7638 or +1 512 434-1577 **Web** sun.com

We make the net work.

Sun Worldwide Sales Offices: Africa (North, West and Central) +33-13-067-4680, Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India–Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand–Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China–Beijing +86-10-6803-5588; Chengdu +86-28-619-9333; Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Singapore +65-6438-1888, Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-596-9900, Sweden +46-8-631-10-00, Switzerland–German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44-1-276-20444, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800 05/03 FE-1989-1