United States Government Accountability Office

GAO

Testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

For release on delivery
expected at 9:30 a.m. EDT
Wednesday, October 6, 2004

ELECTRONIC GOVERNMENT

Smart Card Usage is Advancing Among Federal Agencies, Including the Department of Veterans Affairs

Statement of Linda D. Koontz
Director, Information Management Issues

GAO
Accountability * Integrity * Reliability

October 6, 2004

GAO Accountability•Integrity•Reliability

Highlights

Highlights of GAO-05-84T, a testimony to the Subcommittee on Oversight and Investigations, House Committee on Veterans' Affairs

ELECTRONIC GOVERNMENT

Smart Card Usage is Advancing Among Federal Agencies, Including the Department of Veterans Affairs

Why GAO Did This Study

The federal government is interested in the use of smart cards—credit card-like devices that use integrated circuit chips to store and process data—for improving the security of its many physical and information assets. Besides providing better authentication of the identities of people accessing buildings and computer systems, smart cards offer a number of other potential benefits and uses, such as creating electronic passenger lists for deploying military personnel and tracking immunization and other medical records.

Over the past 2 years, GAO has studied and reported on the uses of smart cards across the federal government. The Subcommittee requested that GAO testify on federal agencies' efforts in adopting smart card technology—based on the results of this prior work—and on the specific actions that the Department of Veterans Affairs is taking to implement smart card technology.

www.gao.gov/cgi-bin/getrpt?GAO-05-84T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda D. Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

As the unique properties and capabilities of smart cards have become more apparent, federal agencies, including the Office of Management and Budget, the National Institute of Standards and Technology, and the General Services Administration, have acted to advance the governmentwide adoption of smart card technology. In turn, numerous smart card projects that offer a variety of uses and benefits have been launched. As of June 2004, 15 federal agencies reported 34 ongoing smart card projects. Further, agencies' actions toward the adoption of smart cards continue to evolve as understanding of the technology grows. Agencies are moving away from the small-scale, limited-duration demonstration projects of past years (involving as few as 100 cardholders and aiming mostly to show the value of using smart cards for identification) to larger, more integrated, agencywide initiatives involving many thousands (or even millions) of users and that are focused on physical access to facilities and logical (information systems) access to computer systems and networks.

In pursuing smart card projects, federal agencies have had to contend with numerous management and technical challenges. However, these challenges may be less imposing in the future because of increased management concerns about securing federal facilities and because technical advances have improved the capabilities and cost effectiveness of smart card systems.

The Department of Veterans Affairs (VA) is one of 9 federal agencies currently pursuing large-scale, agencywide smart card initiatives. VA's project, currently in limited deployment, involves using, among other technologies, the One-VA Identification smart card to provide an agencywide capability to authenticate users with certainty and grant them access to information systems essential to accomplishing the agency's business functions. VA estimates that this project will cost about $162 million between 2004 and 2009, and enable it to issue 500,000 smart cards to its employees and contractors.

A Typical Smart Card (not to scale)

Source: GSA

Mr. Chairman and Members of the Subcommittee:

Thank you for this opportunity to participate in the Subcommittee's hearing regarding the adoption and use of smart card technology. Smart cards are plastic devices—about the size of a credit card—that generally use integrated circuit chips to store and process data, much like a computer. This processing capability distinguishes these cards from traditional magnetic stripe cards, which cannot process information interactively with automated information systems.

Our prior work has found that smart cards offer a variety of benefits to the federal government, such as better authentication of cardholders' identities, increased security over buildings, more effective safeguards of computer systems and data, and more accurate and efficient financial and nonfinancial transactions.[1] The General Services Administration (GSA) has promoted the adoption of smart card technology across government based on a goal of equipping all federal employees with a standardized smart card for a wide range of services. Nonetheless, the successful adoption of smart cards throughout the federal government has been a challenging task, and federal agencies' adoption of this technology continues to evolve.

At your request, my remarks today will summarize the federal government's efforts toward adopting smart card technology and the challenges that have been encountered. Also included in my discussion is an overview of the actions that the Department of Veterans Affairs (VA) is taking to implement smart cards. In addressing these objectives and developing this testimony, we relied primarily on previously reported information describing federal agencies' accomplishments and planned activities to promote smart cards and the challenges to smart card adoption identified across the federal government. We also assessed available documentation and interviewed VA officials regarding their specific actions to

[1] GAO, *Electronic Government: Progress in Promoting Adoption of Smart Card Technology,* GAO-03-144 (Washington, D.C.: Jan. 3, 2003); *Electronic Government: Challenges to the Adoption of Smart Card Technology,* GAO-03-1108T (Washington, D.C.: Sept. 9, 2003); and *Electronic Government: Federal Agencies Continue to Invest in Smart Card Technology,* GAO-04-948 (Washington, D.C.: Sept. 8, 2004).

implement smart cards; however, we did not verify the information that VA provided in support of its initiatives. We performed our work in accordance with generally accepted government auditing standards during September and October 2004.

Results In Brief

The unique properties and capabilities of smart cards—plastic devices that use integrated circuit chips to store and process data—offer the potential to significantly improve the security of federal buildings, systems, data, and transactions. With the potential uses and associated benefits in mind, federal agencies, including the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and GSA have taken actions to advance the adoption of smart card technology governmentwide. In turn, numerous projects have been launched that offer many capabilities and tangible and intangible benefits. As of June 2004, 15 federal agencies had reported 34 ongoing smart card projects. Further, as understanding of smart card technology has increased, agencies have begun pursuing larger, integrated agencywide smart card systems aimed at better securing both physical access to facilities and logical access to computer systems and networks. Nonetheless, agency managers have faced considerable management and technical challenges in their efforts. These challenges have become less formidable, however, as management concerns about securing federal facilities and information systems have increased and as technical advances have improved the capabilities and reduced the cost of smart card systems.

The Department of Veterans Affairs is among a number of federal agencies currently pursuing large-scale, agencywide smart card initiatives. VA's Authentication and Authorization Infrastructure Project, begun in December 2002 and currently in a limited deployment phase, is planned to employ a combination of smart card and other technologies to achieve the capability to authenticate users with certainty and grant them access to information systems necessary to perform business functions. VA estimates that this project will cost about $162 million between 2004 and 2009, and enable it to issue 500,000 smart cards to its employees and contractors.

Background

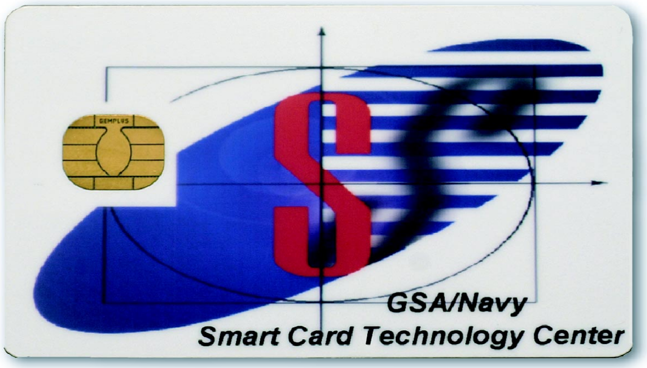
As you are aware, technology plays an important role in helping the federal government ensure the security of its many physical and information assets. Today, federal employees are issued a wide variety of identification (ID) cards that are used to access federal buildings and facilities, sometimes solely on the basis of visual inspection by security personnel. These cards often cannot be used for other important identification purposes—such as gaining access to an agency's computer systems—and many can be easily forged or stolen and altered to permit access by unauthorized individuals. In general, the ease with which traditional ID cards—including credit cards—can be forged has contributed to an increase in identity theft and related security and financial problems for both individuals and organizations.[2]

The unique advantage of smart cards—as opposed to cards with simpler technology, such as magnetic stripes or bar codes—is that smart cards can exchange data with other systems and process information rather than simply serving as static data repositories. Smart cards can readily be tailored to meet the varying needs of federal agencies or to accommodate previously installed systems. For example, other media, such as magnetic stripes, bar codes, and optical memory (laser-readable) stripes can be added to smart cards to support interactions with existing systems and services or to provide additional storage capacity. An agency that has been using magnetic stripe cards for access to certain facilities could migrate to smart cards that would work with both its existing magnetic stripe readers as well as new smart card readers. Of course, the functions provided by the card's magnetic stripe, which cannot process transactions, would be much more limited than those supported by

[2] See GAO, *Identity Theft: Available Data Indicate Growth in Prevalence and Cost,* GAO-02-424T (Washington, D.C.: Feb. 14, 2002).

the card's integrated circuit chip. Optical memory stripes (which are similar to the technology used in commercial compact discs) can be used to equip a card with a large memory capacity for storing more extensive data—such as color photos, multiple fingerprint images, or other digitized images—and for making that card and its stored data very difficult to counterfeit.[3] A typical example of a smart card is shown in figure 1.

Figure 1: A Typical Smart Card



Source: GSA.

Smart cards can be used to significantly enhance the security of an organization's computer systems by tightening controls over user access. A user wishing to log on to a computer system or network with controlled access must "prove" his or her identity to the system—a process called authentication. Many systems authenticate users by requiring them to enter secret passwords, which provide only modest security because the passwords can be easily compromised. Substantially better user authentication can be achieved by supplementing passwords with smart cards.[4]

[3] Cards with an optical memory stripe are known as laser cards or optical memory cards. For more information, see GAO, *Technology Assessment: Using Biometrics for Border Security,* GAO-03-174, (Washington, D.C.: Nov. 15, 2002).

[4] To gain access under this scenario, a user is prompted to insert a smart card into a reader to provide identifying information to the computer as well as type in a password. This authentication process is significantly more difficult to circumvent because an intruder would need to not only guess a user's password, but also to possess the same user's smart card.

Even stronger authentication can be achieved when smart cards are used in conjunction with biometrics.[5] Smart cards are one type of media that can be configured to store biometric information—such as fingerprints or iris scans—in electronic records that can be retrieved and compared with an individual's live biometric scan to verify that person's identity in a way that is difficult to circumvent. A system requiring users to present a smart card, enter a password, and verify a biometric scan provides what security experts call "three-factor" authentication, with the three factors being (1) something you possess (the smart card), (2) something you know (the password), and (3) something you are (the biometric). Systems with three-factor authentication are considered to provide a relatively high level of security.

Additionally, smart cards can be used in conjunction with public key infrastructure (PKI) technology to better secure electronic messages and transactions. A PKI is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances that are important in protecting sensitive communications and transactions.[6] A properly implemented and maintained PKI can offer several important security services, including assurance that (1) the parties to an electronic transaction are really who they claim to be, (2) the information has not been altered or shared with any unauthorized entity, and (3) the parties will not be able to deny taking part in the transaction. Security experts generally agree that PKI technology is most effective when deployed in conjunction with smart cards.

Smart cards are grouped into two major classes: contact cards and "contactless" cards. Contact cards have gold-plated contacts that connect directly with the read/write heads of a smart card reader when the card is inserted into the device. Contactless cards contain

[5] For more information about biometrics, see GAO, *Information Security: Challenges in Using Biometrics*, GAO-03-1137T (Washington, D.C.: Sept. 9, 2003) and *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[6] For more information about PKI technology, see GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

an embedded antenna and work when the card is waved within the magnetic field of a card reader or terminal. Contactless cards are better suited for environments where quick interaction between the card and reader is required, such as high-volume physical access. For example, the Washington Metropolitan Area Transit Authority has deployed an automated fare collection system using contactless smart cards as a way of speeding patrons' access to the Washington, D.C. subway system. Smart cards can be configured to include both contact and contactless capabilities; however, two separate interfaces are needed because standards for the technologies are very different.

Federal Agencies' Pursuit of Smart Card Technology Is Evolving and Involves Challenges

Since the 1990s, the federal government has considered the use of smart card technology as one option for electronically improving security over buildings and computer systems. In 1996, OMB tasked GSA with taking the lead in facilitating a coordinated interagency management approach for the adoption of multi-application smart cards across government. In this regard, GSA has taken important steps to promote federal smart card use. For example, since 1998, it has worked with several other federal agencies to promote broad adoption of smart cards for authentication throughout the federal government. Specifically, GSA worked with the Department of the Navy to establish a technology demonstration center to showcase smart card technology and applications and it established a smart card project managers' group and Government Smart Card Interagency Advisory Board.[7]

For many federal agencies, GSA's chief contribution toward promoting smart card adoption was its effort in 2000 to develop a standard contracting vehicle for use by federal agencies in procuring

[7] In 2000, GSA established the Government Smart Card Interagency Advisory Board to address government smart card issues, standards, and practices, as well as to help resolve interoperability problems among agencies.

commercial smart card products from vendors. Under the terms of the Smart Access Common ID Card contract, GSA, NIST, and the contract's awardees worked together to develop smart card interoperability guidelines—including an architectural model, interface definitions, and standard data elements—that were intended to guarantee that all the products made available through the contract would be capable of working together.

Further, OMB has begun taking action to develop a framework of policy guidance for governmentwide smart card adoption. Specifically, on July 3, 2003, OMB's Administrator for E-Government and Information Technology issued a memorandum detailing specific actions the administration was taking to streamline authentication and identity management in the federal government.[8] This included establishing the Federal Identity and Credentialing Committee to collect agency input on policy and requirements and coordinate the development of a comprehensive policy for credentialing federal employees.

Since 1998, multiple smart card projects have been launched in the federal government addressing an array of capabilities and providing many tangible and intangible benefits, including enhancing security over buildings and other facilities, safeguarding computer systems and data, and conducting financial and nonfinancial transactions more accurately and efficiently. As of June 2004, 15 federal agencies reported 34 ongoing smart card projects.

Initially, many of the smart card initiatives that were undertaken were small-scale demonstration projects that involved as few as 100 cardholders and intended to show the value of using smart cards for identification or to store cash value or other personal information. However, federal efforts toward the adoption of smart cards have continued to evolve as agencies have gained an increased understanding of the technology and its potential uses and benefits. Our most recent study of federal agencies' investments in smart card

[8] Office of Management and Budget, *Memorandum for Chief Information Officers of Departments and Agencies on Streamlining Authentication and Identity Management within the Federal Government* (Washington, D.C.: July 3, 2003).

technology, which we reported on last month,[9] noted that agencies are increasingly moving away from many of their earlier efforts—which frequently involved small-scale, limited-duration pilot projects—toward much larger, integrated, agencywide initiatives aimed at providing smart cards as identity credentials that agency employees can use to gain both physical access to facilities, such as buildings, and logical access to computer systems and networks.[10] In some cases, additional functions, such as asset management and stored value, are also being included.

To date, the largest smart card program to be implemented in the federal government is the Common Access Card program of the Department of Defense (DOD), which is intended to be used for identification by about 3.5 million military and civilian personnel. Results from this project have indicated that smart cards can offer many useful benefits, such as significantly reducing the processing time required for deploying military personnel, tracking immunization records of dependent children, and verifying the identity of individuals accessing buildings and computer systems.

Another large agencywide initiative is the Department of Homeland Security's (DHS) Identification and Credentialing project, an effort in which the agency plans to issue 250,000 cards to employees and contractors using PKI technology for logical access and proximity chips for physical access. Authentication is to rely on biometrics with a personal identification number as a backup. Further, GSA's Nationwide Identification is a recently initiated agencywide smart card project in which the agency plans to issue a single standard credential card for identification, building access, property management, and other applications to 61,000 federal employees, contractors, and tenant agencies.

While smart card technology offers benefits, launching smart card projects—whether large or small—has proved challenging to federal

[9] GAO-04-948.

[10] As of June 2004, agencies reported that more than half of the smart card projects previously identified as ongoing (28 of 52) had been discontinued because they were absorbed into other smart card projects or were deemed no longer feasible.

agencies and efforts to sustain successful adoption of the technology across government. Our prior work noted a number of management and technical challenges that agency managers have faced. These challenges include:

- **Sustaining executive-level commitment.** Maintaining executive-level commitment is essential to implementing smart card technology effectively. Without this support and clear direction, large-scale smart card initiatives may encounter organizational resistance and cost concerns that lead to delays and cancellations. DOD officials stated that having a formal mandate from the Deputy Secretary of Defense to implement a uniform, common access identification card across the department was essential to getting a project as large as the Common Access Card initiative launched and funded.[11]
- **Recognizing resource requirements**. Smart card implementation costs can be high, particularly if significant infrastructure modifications are required, or other technologies, such as biometrics and PKI, are being implemented in tandem with the cards. Key implementation activities that can be costly include managing contractors and card suppliers, developing systems and interfaces with existing personnel or credentialing systems, installing equipment and systems to distribute the cards, and training personnel to issue and use smart cards. As a result, agency officials have found that obtaining adequate resources is critical to implementing a major government smart card system.
- **Integrating physical and logical security practices across organizations.** The ability of smart card systems to address both physical and logical (information systems) security means that unprecedented levels of cooperation may be required among internal organizations that often had not previously collaborated, particularly physical security organizations and information technology organizations. In addition to the gap between physical and logical security organizations, the sheer number of separate and incompatible existing systems also adds to the challenge of establishing an integrated agencywide smart card system.

[11] Deputy Secretary of Defense, *Memorandum on Smart Card Adoption and Implementation* (Washington, D.C.: Nov. 10, 1999).

- **Achieving interoperability among smart card systems.** Interoperability is a key consideration in smart card deployment.[12] The value of a smart card is greatly enhanced if it can be used with multiple systems at different agencies, and GSA has reported that virtually all agencies agree that interoperability at some level is critical to widespread adoption of smart cards across the government. However, achieving interoperability has been difficult because smart card products and systems developed in the past have generally been incompatible in all but very rudimentary ways. With varying products available from many vendors, there has been no obvious choice for an interoperability standard. GSA considered the achievement of interoperability across card systems to be one of its main priorities in developing its Smart Access Common ID Card contract that I discussed earlier.
- **Maintaining security of smart card systems and privacy of personal information.** Although concerns about security are a key driver for the adoption of smart card technology in the federal government, the security of smart card systems themselves is not foolproof and must be addressed when agencies plan the implementation of a smart card system. Although smart card systems are generally much more difficult to attack than traditional ID cards and password-protected systems, they are not invulnerable. In order to obtain the improved security services that smart cards offer, care must be taken to ensure that the cards and their supporting systems do not pose unacceptable security risks. In addition, protecting the privacy of personal information is a growing concern and must be addressed with regard to the personal information contained on the smart cards. Once in place, smart card-based systems designed simply to control access to facilities and systems could also be used to track the day-to-day activities of individuals, thus potentially compromising the individual's privacy. Further, smart card-based systems could be used to aggregate sensitive information about individuals for purposes other than those prompting the initial collection of the information, which could compromise privacy. The Privacy Act of 1974[13] requires the

[12] Interoperability is the ability of two or more systems or components to exchange information and to use the information exchanged.

[13] 5 U.S.C. section 552a.

federal government to restrict the disclosure of personally identifiable records maintained by federal agencies while permitting individuals access to their own records and the right to seek amendment of agency records that are inaccurate, irrelevant, untimely, or incomplete. Further, the E-Government Act of 2002[14] requires agencies to conduct privacy impact assessments before developing or procuring information technology that collects, maintains, or disseminates personally identifiable information. Accordingly, agency officials need to assess and plan for appropriate privacy measures when implementing smart card-based systems and ensure that privacy impact assessments are conducted when required.

In considering these challenges, it is important to note that, while they served to slow the adoption of smart card technology in past years, they may be less difficult in the future because of increased management concerns about securing federal facilities and information systems and because technical advances have improved the capabilities and reduced the cost of smart card systems. Nonetheless, sustained diligence in responding to such challenges is essential in light of the growing emphasis on the use of smart card technology.

Recognizing the critical role that GSA, OMB, and NIST play in furthering the successful adoption of smart card technology, we made recommendations in January 2003 to these agencies that were aimed at advancing the adoption of smart card technology governmentwide. Specifically, we recommended that

- the Director, OMB, issue governmentwide policy guidance regarding adoption of smart cards for secure access to physical and logical assets;
- the Director, NIST, continue to improve and update the government smart card interoperability specification by addressing governmentwide standards for additional technologies—such as

[14] E-Government Act of 2002, P.L. 107-347, sec. 208 (Dec. 17, 2002).

contactless cards, biometrics, and optical stripe media—as well as integration with PKI; and

- the Administrator, GSA, improve the effectiveness of GSA's promotion of smart card technologies within the federal government by (1) developing an internal implementation strategy with specific goals and milestones to ensure that GSA's internal organizations support and implement smart card systems consistently; (2) updating its governmentwide implementation strategy and administrative guidance on implementing smart card systems to address current security priorities; (3) establishing guidelines for federal building security that address the role of smart card technology; and (4) developing a process for conducting ongoing evaluations of the implementation of smart card-based systems by federal agencies to ensure that lessons learned and best practices are shared across government.

As of last month, all three agencies had taken actions to address the recommendations made to them. Specifically, in response to our recommendations, OMB issued its July 3, 2003, memorandum to major departments and agencies directing them to coordinate and consolidate investments related to authentication and identity management, including the implementation of smart card technology.[15] NIST responded by improving and updating the government smart card interoperability specification to address additional technologies, including contactless cards and biometrics.[16] GSA responded to our recommendations by updating its "Smart Card Policy and Administrative Guidance" to better address security priorities, including minimum-security standards for federal facilities, computer systems, and data across the government.

However, three of our four recommendations to GSA remained outstanding. GSA officials stated that they were working to address

[15] OMB, *Memorandum for the Chief Information Officers of Departments and Agencies*, July 3, 2003.

[16] NIST, *Government Smart Card Interoperability Specification,* version 2.1, Interagency Report 6887 (July 2003).

the recommendations to develop an internal GSA smart card implementation strategy, develop a process for conducting evaluations of smart card implementations, and share lessons learned and best practices across government. The responsibility for one recommendation—establishing guidelines for federal building security that address the role of smart card technology—was transferred to DHS.

Recent federal direction contained in Homeland Security Presidential Directive 12[17] could further facilitate smart card adoption across the federal government. This directive, signed in late August, seeks to establish a common identification standard for federal employees and contractors to protect against a litany of threats, including terrorism and identity theft. The directive instructs the Departments of Commerce, State, Defense, Justice, and Homeland Security to work with OMB and the Office of Science and Technology Policy to institute the new standards and policies. With federal agencies' increasing pursuit of smart cards, directives from central management such as this one could be an important vehicle for ensuring that more comprehensive guidance is available to support and sustain the broader implementation of agencywide smart card initiatives.

VA Is Pursuing Agencywide Use of Smart Cards

Mr. Chairman, beyond the governmentwide assessment presented, you requested that we specifically address actions of the Department of Veterans Affairs in adopting smart card technology. Our report last month discussing agencies' investments in smart card technology identified VA as being among 9 federal agencies that currently have large-scale, agencywide smart card projects underway.[18]

[17] Homeland Security Presidential Directive 12/Hspd-12, August 27, 2004.

[18] GAO-04-948.

VA's effort—the Authentication and Authorization Infrastructure Project (AAIP)—was begun in December 2002 as an attempt to provide agencywide capability to authenticate users with certainty and grant them access to information systems necessary to perform business functions. The initiative, currently in a limited deployment phase, involves three core components: (1) a One-VA ID smart card; (2) an enterprise PKI solution;[19] and (3) an identity and access management infrastructure that addresses internal and external access requirements for VA users. VA currently estimates that, between fiscal years 2004 and 2009, this initiative will cost about $162 million.

The project is currently focusing on development of the One-VA ID card, which is to employ a combination of smart card and PKI technologies to store a user's credentials digitally.[20] According to project documentation, the One-VA ID card is intended to replace the several hundred methods for issuing identification cards that are currently in place across the department,[21] and improve physical and information security by strengthening the ability to authenticate users and grant access to information systems that employees and contractors rely on to perform VA's business functions.[22] As an official source of government identification credentialing, the card is expected to be compliant with Homeland Security Presidential Directive 12.

[19] VA plans to contract out a key component of the PKI known as a certification authority. For more information on contracting out certification authorities, see GAO-04-1023R.

[20] A PKI is a system of computers, software, and data that relies on certain cryptographic techniques for some aspects of security. A properly implemented and maintained PKI can offer several important security services, including assurance that (1) the parties to an electronic transaction are really who they claim to be, (2) the information has not been altered or shared with any unauthorized entity, and (3) neither party will be able to wrongfully deny taking part in the transaction. For more information, see GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

[21] VA's facilities include 57 regional offices, 158 hospitals, 133 nursing homes, 7 centralized mail out pharmacies, and 9 regional loan centers.

[22] The One-VA ID card will not be issued to veterans or other VA beneficiaries.

VA is using a phased approach to develop and implement the One-VA ID card. This approach involves prototype testing followed by limited production testing at the department's facilities in the United States, and by 2006, the issuance of 500,000 cards with PKI credentials to its personnel. VA reported that it has already begun an initial limited deployment of the cards to about 15,000 to 25,000 users. The AAIP project manager anticipated that the results from this limited deployment would provide lessons learned for ensuring successful implementation, support, and training once full deployment of the One-VA ID card begins in early 2005. Further, the department has indicated that it plans to use information gathered from the limited deployment to create agency-wide policies and procedures for the full deployment of smart cards across all VA business units. As of late September, VA reported that fiscal year 2004 spending on the One-VA ID card totaled approximately $27 million for activities such as the acquisition of smart cards, card readers, and hardware support.

We have not yet had an opportunity to fully assess the outcomes of the department's One-VA ID card initiative or its actions to develop the enterprise PKI solution and identity and access management infrastructure that are also key components of this initiative. However, VA officials believe that the department is sufficiently positioned to successfully implement the smart card technology on an agencywide level. The AAIP project manager noted the chief information officer's involvement, as chair of the department's Enterprise Information Board, in monitoring progress of the project.

Further, as a participant in a number of governmentwide initiatives supporting the adoption of smart card technology, VA should be effectively positioned to carry out such an undertaking. Among its collaborations, VA is one of five agencies[23] using GSA's Smart Card Access Common ID contracting vehicle and plans to purchase smart cards for AAIP through the GSA contract. It is also a member of the Federal Identity Credentialing Committee, which provides guidance to federal agencies on the use of smart card technology that

[23] The other agencies are the National Aeronautics and Space Administration and the departments of Defense, Homeland Security, and Interior.

supports interoperable identity and authentication to enable an individual's identity to be verified within an agency and across the federal enterprise for both physical and logical networks. Collectively, the department's experiences and collaborations should lend strength to its own and overall federal efforts toward making smart cards a key means of securing critical information and assets.

In summary, the federal government is continuing to make progress in promoting and implementing smart card technology, which offers clear benefits for enhancing security over access to buildings and other facilities, as well as computer systems and networks. The adoption of such technology is continuing to evolve, with a number of large-scale, agencywide projects having been undertaken by federal agencies over the past several years. As agencies have sought greater use of smart cards, they have had to contend with a number of significant management and technical challenges, including sustaining executive-level commitment, recognizing resource requirements, integrating physical and logical security practices, achieving interoperability, and maintaining system security and privacy of personal information. These challenges become less difficult to address, however, as managers place greater emphasis on enhancing the security of federal facilities and information systems and technical advances improve the capabilities and reduce the costs of smart card systems. The challenges are also tempered as increased federal guidance brings direction to agencies' handlings of their smart card initiatives.

VA is among a number of agencies currently undertaking large-scale, agencywide projects to implement smart cards. While its project is still under development, VA has gained experience as a participant on governmentwide initiatives to further smart card adoption that should facilitate the increasing movement toward the use of smart cards as an essential means of securing critical information and assets.

Mr. Chairman, this concludes my statement. I would be pleased to respond to any questions that you or other members of the subcommittee may have.

Contacts and Acknowledgements

If you should have any questions about this testimony, please contact me at (202) 512-6240 or via e-mail at koontzl@gao.gov. Other major contributors to this testimony included Michael A. Alexander, John de Ferrari, Nancy Glover, Steven Law, Valerie C. Melvin, J. Michael Resser, and Eric L. Trout.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov(202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548