United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, September 9, 2003

ELECTRONIC GOVERNMENT

Challenges to the Adoption of Smart Card Technology

Statement of Joel C. Willemssen
Managing Director, Information Technology Issues

September 2003

ELECTRONIC GOVERNMENT

Challenges to the Adoption of Smart Card Technology

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-1108T, a testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

Why GAO Did This Study

The federal government is increasingly 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 better authentication of the identities of people accessing buildings and computer systems, smart cards offer a number of potential benefits and uses, such as creating electronic passenger lists for deploying military personnel, and tracking immunization and other medical records.

Earlier this year, GAO reported on the use of smart cards across the federal government (GAO-03-144). GAO was asked to testify on the results of this work, including the challenges to successful adoption of smart cards throughout the federal government, as well as the government's progress in promoting this smart card adoption.

www.gao.gov/cgi-bin/getrpt?GAO-03-1108T.

To view the full testimony, including the scope and methodology, click on the link above. For more information, contact Joel Willemssen at (202) 512-6222 or willemssenj@gao.gov.

What GAO Found

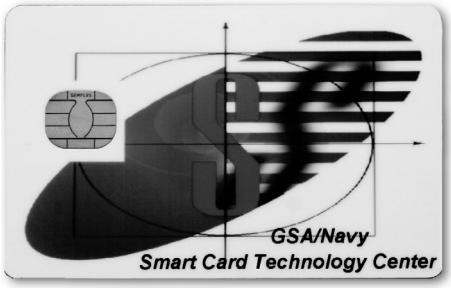
To successfully implement smart card systems, agency managers have faced a number of substantial challenges:

- sustaining executive-level commitment in the face of organizational resistance and cost concerns;
- obtaining adequate resources for projects that can require extensive modifications to technical infrastructures and software;
- integrating security practices across agencies, a task requiring collaboration among separate and dissimilar internal organizations;
- achieving smart card interoperability across the government; and
- maintaining the security of smart card systems and the privacy of personal information.

These difficulties may be less formidable as management concerns about facility and information system security increase and as technical advances improve smart card capabilities and reduce costs. However, such challenges, which have slowed the adoption of this technology in the past, continue to be factors in smart card projects.

Given the significant management and technical challenges associated with successful adoption of smart cards, a series of initiatives has been undertaken to facilitate the adoption of the technology. As the federal government's designated promoter of smart card technology, GSA assists agencies in assessing the potential of smart cards and in implementation. GSA has set up a governmentwide, standards-based contracting vehicle and has established interagency groups to work on procedures, standards, and guidelines. As the government's policymaker, OMB is beginning to develop a framework of policy guidance for governmentwide smart card adoption. In a July 2003 memorandum, OMB described a three-part initiative on authentication and identity management in the government, consisting of (1) developing common policy and technical guidance; (2) executing a governmentwide acquisition of authentication technology, including smart cards; and (3) selecting shared service providers for smart card technology. These efforts address the need for consistent, up-to-date standards and policy on smart cards, but both GSA and OMB still have much work to do before common credentialing systems can be successfully implemented across government agencies.

A Typical Smart Card (not to scale)



Source: GSA

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in the Subcommittee's hearing regarding the benefits of, and challenges to, the successful adoption of smart cards across the federal government. Smart cards are plastic devices—about the size of a credit card—that use integrated circuit chips to store and process data, much like a computer.[1] This processing capability distinguishes these cards from traditional magnetic stripe cards, which cannot interact with automated information systems. In January of this year, we reported 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.[2] However, challenges to the successful adoption of smart cards throughout the federal government need to be addressed before the benefits of their use can be fully realized.

As requested, in my remarks today, I will discuss the potential benefits that the use of smart cards can offer, the challenges to successful adoption of smart cards throughout the federal government, and the progress of the General Services Administration (GSA), the Office of Management and Budget (OMB), and other agencies in overcoming these challenges and promoting governmentwide adoption of smart cards.

Background

As you know, technology plays an important role in helping the federal government provide security for its many physical and information assets. Today, federal employees are issued a wide variety of identification (ID) cards, which 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

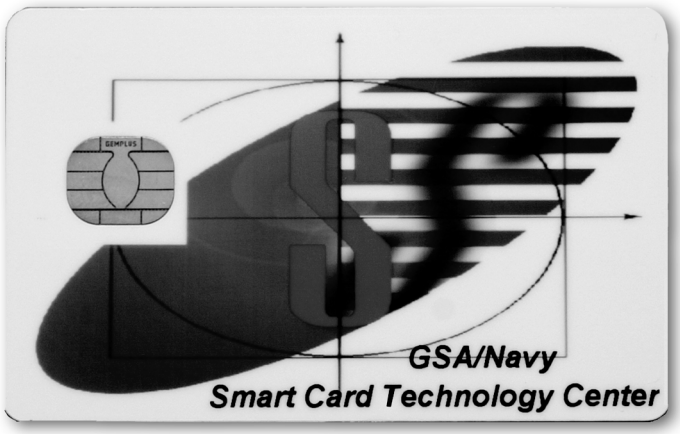
[1]The term "smart card" may also be used to refer to cards with a computer chip that only stores information without providing any processing capability. Such cards, known as stored-value cards, are widely used for services such as prepaid telephone service or satellite television reception. This statement focuses chiefly on cards with processing capability.

[2]U.S. General Accounting Office, *Electronic Government: Progress in Promoting Adoption of Smart Card Technology*, GAO-03-144 (Washington, D.C.: Jan. 3, 2003).

cards—can be forged has contributed to increases in identity theft and related security and financial problems for both individuals and organizations.[3]

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 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.[4] Figure 1 shows a typical example of a smart card.

Figure 1: A Typical Smart Card



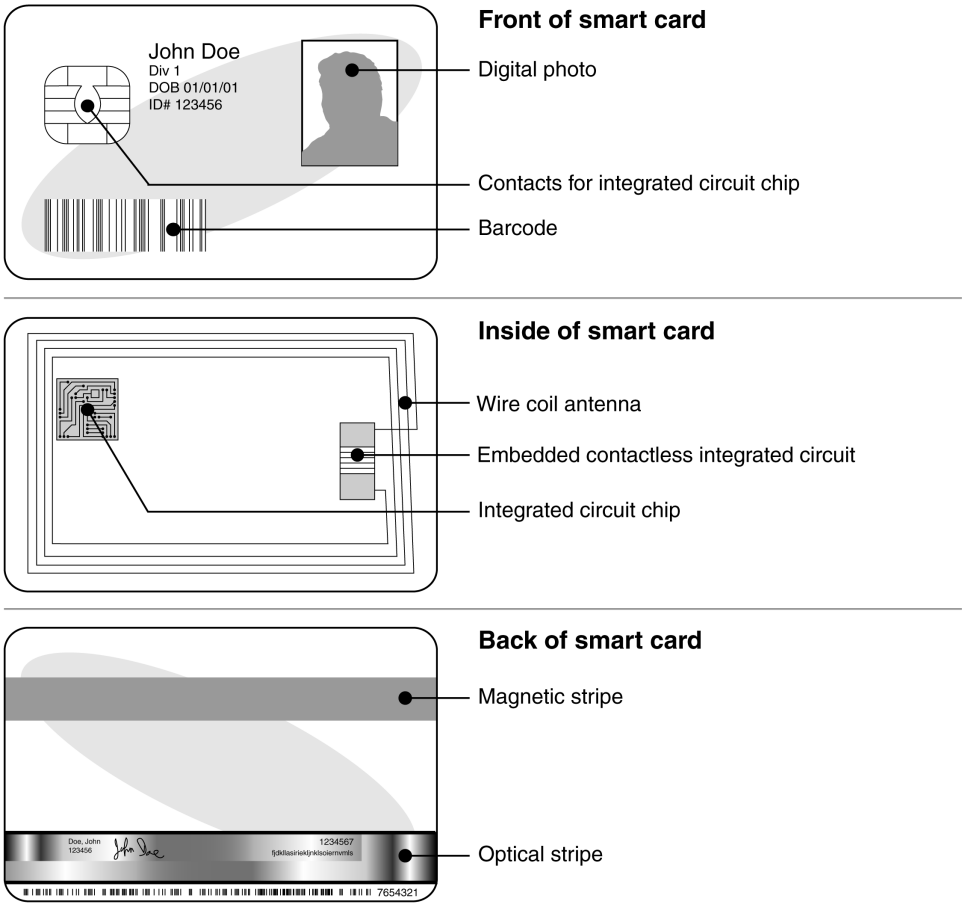
Source: GSA

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

[4]Cards with an optical memory stripe are known as laser cards or optical memory 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 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, but two separate interfaces are needed, because standards for the technologies are very different.

Figure 2: Features That May Be Incorporated into Smart Cards



Source: GAO (not to scale)

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 multiapplication smart cards across government. At the time, OMB envisioned broad adoption of smart card technology throughout the government, as evidenced by the President's budget for fiscal year 1998, which set a goal of enabling every federal employee ultimately to be able to use one smart card for a wide range of purposes, including travel, small purchases, and building access. In January 1998, the President's Management Council and the Electronic Processing Initiatives

Committee[5] (EPIC) established an implementation plan for smart cards that called for a governmentwide, multiapplication card that would support a range of functions—including controlling access to government buildings—and operate as part of a standardized system. More recently, the Enhanced Border Security and Visa Entry Reform Act of 2002 called for enhancing national security and counterterrorism efforts by using technologies such as smart cards that could provide biometric comparison and authentication to better identify individuals entering the country.[6]

In developing this testimony, our objectives were to explain the potential benefits of smart cards, to discuss the challenges to successful adoption of smart cards, and to discuss the steps that federal agencies have taken to address those challenges. To address these objectives, we obtained relevant documentation and interviewed officials from GSA and the Department of the Interior. We also analyzed agencies' accomplishments and planned activities to promote smart cards in light of the challenges to smart card adoption across the federal government that we identified in our January report. We performed our work between August 2003 and September 2003, in accordance with generally accepted auditing standards.

Smart Cards Can Provide a Variety of Benefits to Federal Agencies

The unique properties and capabilities of smart cards offer the potential to significantly improve the security of federal buildings, systems, data, and transactions. For example, the process of verifying the identity of people accessing federal buildings and computer systems, especially when used in combination with other technologies, such as biometrics, is significantly enhanced with the use of smart cards. 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. Other potential

[5]EPIC, an interagency body, was established during the 1990s to help improve the delivery of electronic commerce activities across government and to assist the President's Management Council on such issues. In 2000, EPIC was replaced by the Electronic Government Coordinating Committee.

[6]Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. No. 107-173, 116 Stat. 543).

benefits and uses include creating electronic passenger lists for deploying military personnel and tracking immunization and other medical records.

The 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. By securely exchanging information, a smart card can help authenticate the identity of the individual possessing the card in a far more rigorous way than is possible with simpler, traditional ID cards.

Even stronger authentication can be achieved if smart cards are used in conjunction with biometrics. Smart cards 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 as a means of verifying 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, the three factors being "something you possess" (the smart card), "something you know" (the password), and "something you are" (the biometric). Systems employing three-factor authentication are considered to provide a relatively high level of security.[7]

Several Agencies Are Pursuing Smart Card Projects

As of November 2002, 18 agencies had reported initiating a total of 62 smart card projects in the federal government. In what could be the largest federally sponsored smart card rollout to date, the Department of Homeland Security's Transportation Security Administration (TSA) plans to issue smart ID cards to up to 15 million transportation workers who require unescorted access to secure parts of transportation venues, such as airports, seaports, and railroad terminals. TSA's goal is to create a standardized, universally recognized and accepted credential for the transportation industry. According to agency officials, the card is being designed to address a minimum set of requirements, but it will remain flexible enough to support additional requirements as needed. According to TSA's plans, local authorities will use the card to verify the identity and

[7]For more information about biometrics, see U.S. General Accounting Office, *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).

security level of the cardholder and will grant access to facilities in accordance with local security policies.

In addition to Homeland Security, a number of other agencies have undertaken pilot projects to test the capabilities of smart cards. The Department of the Interior's Bureau of Land Management, for example, launched a pilot to provide smart cards to about 1,100 employees to be used for personal identification at the bureau's facilities and to serve as an example to communicate the benefits of smart cards to employees throughout the bureau. According to bureau officials, the project has been a success, and the bureau plans to continue the rollout of smart cards to its remaining employees. Other major smart card projects are also under way at the Departments of the Treasury and State.

Smart Cards Offer Enhanced Safeguards for Access to Computer Systems and Data

In addition to better securing physical access to facilities, smart cards can be used to enhance the security of an organization's computer systems by tightening what is known as "logical" access to systems and networks. 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 merely requiring them to enter secret passwords, which provide only modest security because they can be easily compromised. Substantially better user authentication can be achieved by supplementing passwords with smart cards. To gain access under this scenario, a user is prompted to insert a smart card into a reader attached to the computer as well as type in a password. This authentication process is significantly harder to circumvent, because an intruder would need not only to guess a user's password but also to possess the same user's smart card.

Smart cards can also be used in conjunction with public key infrastructure (PKI) technology to better secure electronic messages and transactions. A properly implemented and maintained PKI can offer several important security services, including assurance that (1) the parties to an electronic transaction are really whom 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. An essential component is the use of special pairs of encryption codes, called "public keys" and "private keys," that are unique to each user. The private keys must be kept secret and secure; however, storing and using private keys on a computer leaves them susceptible to attack, because a hacker who gains control of that computer may then be able to use the private key stored in it to fraudulently sign messages and conduct electronic

transactions. In contrast, if the private key is stored on a user's smart card, it may be significantly less vulnerable to attack and compromise. Security experts generally agree that PKI technology is most effective when deployed in conjunction with smart cards.[8]

The largest smart card program currently in the implementation phase is the Department of Defense's Common Access Card, which is being used initially for logical access to automated systems and networks. Rollout began in October 2000 with a goal of distributing cards to approximately 4 million individuals across the department by October 2003. In addition to enabling access to specific Defense systems, the card is also used to better ensure that electronic messages are accessible only by designated recipients. The card includes a set of PKI credentials, including an encryption key, signing key, and digital certificate, which contains the user's public key. Defense plans to add biometrics to the Common Access Card in the future—which may include fingerprints, palm prints, iris scans, or facial features—and to enable users to digitally sign travel vouchers using the digital certificates on their cards. Defense also plans to add a contactless chip to the card in the future to speed physical access for military personnel to Defense facilities.

Challenges to the Successful Adoption of Smart Cards

The benefits of smart card adoption can be achieved only if key management and technical challenges are understood and met. While these challenges have slowed 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.

Sustaining Executive-Level Commitment

Maintaining executive-level commitment is essential to implementing a smart card system effectively. For example, according to Defense officials, the formal mandate of the Deputy Secretary of Defense to implement a uniform, common access identification card across Defense was essential to getting a project as large as the Common Access Card initiative

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

launched and funded.[9] The Deputy Secretary also assigned roles and responsibilities to the military services and agencies and established a deadline for defining smart card requirements. Defense officials noted that without such executive-level support and clear direction, the smart card initiative likely would have encountered organizational resistance and concerns about cost that could have led to significant delays or cancellation.

Treasury and TSA officials also indicated that sustained high-level support had been crucial in launching smart card initiatives within their organizations and that without this support, funding for such initiatives probably would not have been available. In contrast, other federal smart card pilot projects have been cancelled due to lack of executive-level support. Officials at the Department of Veterans Affairs (VA) indicated that their pilot VA Express smart card project, which issued cards to veterans for use in registering at VA hospitals, would probably not be expanded to full-scale implementation, largely because executive-level priorities had changed, and support for a wide-scale smart card project had not been sustained.

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.

For example, at least $4.2 million[10] was required to design, develop, and implement the Western Governors Association's Health Passport Project to service up to 30,000 customers of health care services in several western states. A report on that project acknowledged that it was complicated and costly to manage card issuance activities. The report

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

[10]According to the project's final report, additional costs were incurred that have not been quantified.

further indicated that help-desk services were difficult to manage because of the number of organizations and outside retailers, as well as different systems and hardware involved in the project.[11] Project officials said they expect costs to decrease as more clients are provided with smart cards and the technology becomes more familiar to users; they also believe that smart card benefits will exceed costs over the long term.

The full cost of a smart card system can also be greater than originally anticipated because of the costs of related technologies, such as PKI. For example, Defense initially budgeted about $78 million for the Common Access Card program in 2000 and 2001 and expected to provide the device to about 4 million military, civilian, and contract employees by October 2003. It now expects to expend over $250 million by 2003—more than double the original estimate—and likely will not have all cards distributed until 2004. Many of the increases in Common Access Card program costs were attributed by Defense officials to underestimating the costs of upgrading and managing legacy systems and processes for card issuance. According to Defense program officials, the department will likely expend over $1 billion for its smart cards and PKI capabilities by 2005. In addition to the costs mentioned above, the military services and defense agencies were required to fund the purchase of over 2.5 million card readers and the middleware to make them work with existing computer applications, at a cost likely to exceed $93 million. The military services and defense agencies are also expected to provide funding to enable applications to interoperate with the PKI certificates loaded on the cards. Defense provided about $712 million to issue certificates to cardholders as part of the PKI program but provided no additional funding to enable applications.[12]

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, especially physical security organizations and information technology organizations. Nearly all federal officials we

[11]Jenny Bernstein, Robin Koralek, Cheryl Owens, Nancy Pindus, and Barbara Selter, *Final Report—The Health Passport Project: Assessment and Recommendations* (December 2001).

[12]Office of the Inspector General, Department of Defense, *Implementation of DOD Public Key Infrastructure Policy and Procedures*, Report No. D-2002-030 (Dec. 28, 2001).

interviewed noted that existing security practices and procedures varied significantly across organizational entities within their agencies and that changing each of these well-established processes and attempting to integrate them across the agency was a formidable challenge.

Defense officials stated that it has been difficult to take advantage of the multiapplication capabilities of its Common Access Card for these very reasons. As it is being rolled out, the card is primarily being used for logical access—for helping to authenticate cardholders accessing systems and networks and for digitally signing electronic transactions using PKI. Officials have only recently begun to consider ways to use the Common Access Card across the department to better control physical access over military facilities. Few Defense facilities are currently using the card for this purpose. Defense officials said it had been difficult to persuade personnel responsible for the physical security of military facilities to establish new processes for smart cards and biometrics and to make significant changes to existing badge systems.

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 to establishing an integrated agencywide smart card system. One Treasury official, for example, noted that departmentwide initiatives, such as its planned smart card project, require the support of 14 different bureaus and services. Each of these entities has different systems and processes in place to control access to buildings, automated systems, and electronic transactions. Agreement could not always be reached on a single business process to address security requirements among these diverse entities.

Achieving Interoperability among Smart Card Systems

Interoperability[13] is a key consideration in smart card deployment. 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

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

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, which is intended to serve as a governmentwide vehicle for obtaining commercial smart card products and services. Accordingly, GSA designed the contract to require awardees to work with GSA and the National Institute of Standards and Technology (NIST)[14] to develop a government interoperability specification. The resulting specification defines a uniform set of command and response messages for smart cards to use in communicating with card readers. Vendors can meet the specification by writing software for their cards that translates their unique command and response formats to the government standard. Such a specification previously had not been available.

According to NIST officials, the first version of the interoperability specification, completed in August 2000, did not include sufficient detail to establish interoperability among vendors' disparate smart card products. The officials stated that this occurred because representatives from NIST, the contractors, and other federal agencies had only a very limited time to develop the first version. The current version, version 2.1,[15] released in July 2003, is a significant improvement, providing better definitions of many details, such as how smart cards should exchange information with software applications and card readers, as well as a specification for contactless cards and accommodations for the future use of biometrics. However, potential interoperability issues may arise for those agencies that purchased and deployed smart card products based on the original specification.

[14]NIST is the lead agency in the Standards Technical Working Group, which was established by the Government Smart Card Interagency Advisory Board to develop and update the Government Smart Card Interoperability Specification. In addition, NIST is responsible for developing a comprehensive conformance test program for the specification.

[15]*Government Smart Card Interoperability Specification, Version 2.1*, NIST Interagency Report 6887 (Jul. 16, 2003).

Maintaining the 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 is not foolproof and must be addressed when agencies plan the implementation of a smart card system. Smart cards can offer significantly enhanced control over access to buildings and systems, particularly when used in combination with other advanced technologies, such as PKI and biometrics. Although smart card systems are generally much harder 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.

Smart card systems generally are designed with a variety of features designed to thwart attack.[16] For example, cards are assigned unique serial numbers to counter unauthorized duplication and contain integrated circuit chips that are resistant to tampering so that their information cannot be easily extracted and used. However, security experts point out that because a smart-card–based system involves many different discrete elements that cannot be physically controlled at all times by an organization's security personnel, there is at least a theoretically greater opportunity for malfeasance than would exist for a more self-contained system.[17]

In fact, a smart-card–based system involves many parties (the cardholders, data owner, computing devices, card issuer, card manufacturer, and software manufacturer) that potentially could pose threats to the system. For example, researchers have found ways to circumvent security measures and extract information from smart cards, and an individual cardholder could be motivated to attack his or her card in order to access and modify the stored data on the card—perhaps to change personal information or increase the cash value that may be stored on the card. Further, smart cards are connected to computing devices (such as agency networks, desktop and laptop computers, and automatic teller machines)

[16]In this context, an attack is an attempt by one or more parties involved in a smart-card–based transaction to cheat by taking advantage of potential weaknesses in the security of the card.

[17]Bruce Schneier and Adam Shostack, "Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards" in *USENIX Workshop on Smart Card Technology* (USENIX Press, 1999), pp. 175–185.

through card readers that control the flow of data to and from the smart card. Attacks mounted on either the card readers or any of the attached computing systems could compromise the safeguards that are the goals of implementing a smart card system.

Smart cards used to support multiple applications may introduce additional risks to the system. For example, if adequate care is not taken in designing and testing each software application, loading new applications onto existing cards could compromise the security of the other applications already stored on the cards. In general, guaranteeing the security of a multiapplication card can be more difficult because of the difficulty of determining which application is running inside a multiapplication smart card at any given time. If an application runs at an unauthorized time, it could gain unauthorized access to data intended only for other applications.

In addition to security, protecting the privacy of personal information is a growing concern and must be addressed with regard to the personal information contained on 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, potentially compromising their 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[18] requires the 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[19] requires that agencies 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.

GSA, NIST, and other agency officials indicated that security and privacy issues are challenging, because governmentwide policies have not yet

[18]5 U.S.C. § 552a.

[19]E-Government Act of 2002, Public Law 107-347 (Dec. 17, 2002).

been established, and widespread use of the technology has not yet occurred. As smart card projects evolve and are used more frequently, especially by citizens, agencies are increasingly likely to need policy guidance to ensure consistent and appropriate implementation that ensures an adequate degree of security as well as privacy.

Actions Have Been Taken to Promote Consistent Smart Card Adoption across Government

Given the significant management and technical challenges associated with successful adoption of smart cards, an ongoing series of initiatives have been undertaken in the federal government to facilitate the adoption of the technology. As I mentioned earlier, GSA was originally tasked in 1996 with coordinating an effort to adopt multiapplication smart cards across the federal government, and it has taken important steps to promote federal smart card use. For example, since 1998, GSA 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.[20] The agency also established an interagency team to plan for uniform federal access procedures, digital signatures, and other transactions, and to develop federal smart card interoperability and security guidelines.

For many federal agencies, GSA's chief contribution to promoting federal adoption of smart cards was its effort in 2000 to develop a standard contracting vehicle for use by federal agencies in procuring commercial smart card products from vendors.[21] 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. Several federal smart card projects—including projects at NASA and the Departments of Homeland Security, State, and the Treasury—have used or

[20]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.

[21]GSA released the solicitation (GS-TFF-99-203) for the Smart Identification Card on January 7, 2000. In May 2000, the contract was awarded to five vendors.

are planning to use the GSA contract vehicle. This effort is intended to directly address the challenge of achieving interoperability among smart card systems that I mentioned earlier.

In our report issued earlier this year, we pointed out additional areas that are important for GSA to address in order to more effectively promote adoption of smart cards, including, among other things, implementing smart cards consistently throughout GSA and developing an agencywide position on the adoption of smart cards. We made recommendations to GSA to address these issues, and agency officials told us they have begun to address them. Specifically, GSA has adopted a new agencywide credential policy and consolidated its internal smart card projects within the Public Buildings Service. It is planning to roll out a uniform smart ID card for all GSA employees by December 2003.

OMB Has Recently Set New Policy for Governmentwide Smart Card Adoption

In our January report, we also recommended that OMB develop governmentwide policy guidance for adoption of smart cards, seeking input from all federal agencies, with particular emphasis on agencies with smart card expertise. We noted that without such guidance, agencies may be unnecessarily reluctant to take advantage of the potential of smart cards to enhance the security of agency facilities and automated systems.

OMB has begun to take 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.[22] The memo sketched out a three-part initiative:

- First, OMB plans to develop common policy for authentication and identity management, including technical guidance to be developed by GSA and NIST, that will result in a comprehensive policy for credentialing federal employees. A newly established Federal Identity and Credentialing Committee is intended to collect agency input on policy and requirements and coordinate this effort.

[22]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).

- Second, OMB intends to execute a governmentwide acquisition of authentication technology, including smart cards, to achieve cost savings in the near term. The memo states that agencies are encouraged to refrain from making separate acquisitions without coordinating with the Federal Identity and Credentialing Committee.

- Finally OMB plans to consolidate agency investments in credentials and PKI services by selecting shared service providers by the end of 2003 and planning for agencies to migrate to those providers during fiscal years 2004 and 2005.

Challenges Remain in Implementing the New Policy

Much work remains to be done to turn OMB's vision of streamlined federal credentialing into reality. According to GSA's smart cards program director, it will be difficult to reconcile the widely varying security requirements of federal agencies to arrive at a stable system design that all agencies can adhere to. Even with a new version of NIST's governmentwide smart card interoperability specification in place, agencies are still not in agreement about definitions for certain basic elements, because advances in technology create endless opportunities to change the specification. For example, the Department of Defense is currently seeking a change in the standard size of a smart card's embedded identifying code, to strengthen the card's internal security. However, implementing such a change may be very expensive for agencies already committed to the existing specification. While it is important to keep technical specifications up to date—and addressing security is a challenge that I've already noted—frequent changes in specifications could nevertheless slow progress in achieving a governmentwide solution. Given the trade-offs that must be considered, achieving governmentwide interoperability of smart cards could take longer than OMB's memorandum anticipates.

In our January report, we recommended that NIST continue to improve and update the government smart card interoperability specification by addressing additional technologies—such as contactless cards, biometrics, and optical stripe media—as well as integration with PKI. As I discussed earlier, NIST recently issued version 2.1 of the specification, which includes as an appendix a specification for contactless cards, as well as accommodations for the future use of biometrics. NIST officials said they intend to continue working to improve the specification and plan to actively participate in the newly established Federal Identity and Credentialing Committee.

Another potential difficulty in achieving OMB's vision of streamlined federal credentialing could be the need to reach consensus on policies for using smart-card–based systems. In our January report, we recommended that OMB issue governmentwide policy guidance regarding adoption of smart cards for secure access to physical and logical assets, and to do so in conjunction with federal agencies that have experience with smart card technology. According to the chair of the Federal Identity and Credentialing Committee, basic policy guidance on developing smart-card–based systems is being readied, based on work done at the Department of Homeland Security. However, additional guidance will also be needed to define minimum standards for the process of verifying individuals' identities when credentials are issued to them. According to the committee chair, it is likely that agencies currently have in place a wide variety of ways of performing identity verification, and it will be challenging to achieve consistency in how this is done across government. Without such consistency, agencies might not be able to rely on credentials issued by other agencies, because they would not know what level of assurance was met in issuing those credentials.

In summary, the federal government has made progress in promoting the adoption of smart cards, which have clear benefits in enhancing security over access to buildings and other facilities as well as computer systems and networks. However, agencies continue to face a number of challenges in implementing smart-card–based systems, 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. In July 2003, OMB took an important step in addressing these challenges by issuing new policy for streamlining authentication and identity management in the federal government. However, much work still needs to be done before credentialing systems that are interoperable and achieve consistent levels of assurance are commonplace across government agencies.

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

Contact and Acknowledgements

If you should have any questions about this testimony, please contact me at (202) 512-6222 or via E-mail at willemssenj@gao.gov. Other major contributors to this testimony included Barbara Collier, John de Ferrari, Steven Law, Elizabeth Roach, and Yvonne Vigil.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

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. General Accounting 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

Public Affairs

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