United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on Technology and Procurement Policy, House of Representatives

January 2003

ELECTRONIC GOVERNMENT

Progress in Promoting Adoption of Smart Card Technology

GAO

Accountability ⋆ Integrity ⋆ Reliability

GAO
Accountability•Integrity•Reliability
Highlights

Highlights of GAO-03-144, a report to the Chairman, Subcommittee on Technology and Procurement Policy, House of Representatives

January 2003

ELECTRONIC GOVERNMENT

Progress in Promoting Adoption of Smart Card Technology

Why GAO Did This Study

Smart cards—credit-card-like devices that use integrated circuit chips to store and process data—offer a range of potential uses for the federal government, particularly in increasing security for its many physical and information assets. GAO was asked to review the use of smart cards across the federal government (including identifying potential challenges), as well as the effectiveness of the General Services Administration (GSA) in promoting government adoption of smart card technologies.

What GAO Recommends

GAO recommends, among other things, that GSA establish guidelines for federal building security that address smart card technology; that OMB establish policy on adoption of smart cards for physical and logical security; and that NIST continue to improve and update the government smart card interoperability specification.

In commenting on a draft of this report, agency officials generally agreed with its content and recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-03-144.

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

What GAO Found

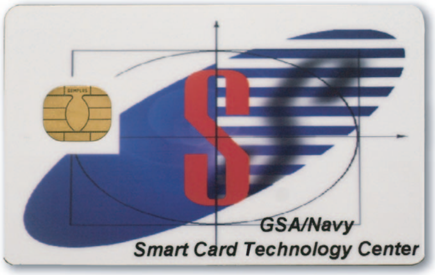
Progress has been made in implementing smart card technology across government. As of November 2002, 18 federal agencies had reported initiating a total of 62 smart card projects. These projects have provided a range of benefits and services, ranging from verifying the identity of people accessing buildings and computer systems to tracking immunization records.

To successfully implement such 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;
- maintaining the security of smart card systems and privacy of personal information.

In helping agencies to overcome these challenges, not only GSA but also the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have roles to play. As the federal government's designated promoter of smart card technology, GSA assists agencies in assessing the potential of smart cards and in implementation. Although GSA has helped agencies significantly by implementing a governmentwide, standards-based contracting vehicle, it has not kept guidance up to date and has not addressed important subjects, such as building security standards, in its guidance. Further, OMB, which is responsible for setting policies for ensuring the security of federal information and systems, has not issued governmentwide policy on adoption of smart cards. In its role of setting technical standards, NIST is responsible for the government smart card interoperability specification, which does not yet address significant emerging technologies. Updated guidance, policy, and standards would help agencies to take advantage of the potential of smart cards to enhance security and other agency operations.

A typical smart card (not to scale)



Source: GSA.

United States General Accounting Office

Contents

Letter

Appendix

Glossary

Tables

Figures

Abbreviations

CAC	Common Access Card
DOD	Department of Defense
EBT	electronic benefits transfer
EPIC	Electronic Processes Initiatives Committee
FAA	Federal Aviation Administration
GSA	General Services Administration
GSC-IAB	Government Smart Card Interagency Advisory Board
HPP	Health Passport Project
ID	identification
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PKI	public key infrastructure
TSA	Transportation Security Administration
VA	Department of Veterans Affairs
WGA	Western Governors' Association

G A O

Accountability ⋆ Integrity ⋆ Reliability

United States General Accounting Office
Washington, D.C. 20548

January 3, 2003

The Honorable Tom Davis
Chairman, Subcommittee on Technology
and Procurement Policy
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

As you know, technology plays an important role in helping the federal government provide security for its many physical and information assets. In particular, "smart cards"[1] offer the potential to significantly improve 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. Further, smart cards can be used to support other business-related functions, such as tracking immunization records or storing cash value for electronic purchases. The General Services Administration (GSA) has promoted the adoption of smart card technology across government based on a goal, set in 1998, of equipping all federal employees with a standardized smart card for a wide range of services.

This report responds to your request that we review the federal government's progress in promoting the use of smart cards as a way to streamline and better secure interactions between individuals and government agencies. Specifically, we agreed to assess (1) the extent to which federal agencies have adopted smart card technologies and realized the associated benefits, (2) the challenges of adopting smart cards within federal agencies, and (3) the effectiveness of GSA in promoting the adoption of smart card technologies within the federal government.

Results in Brief

As of November 2002, 18 agencies had reported initiating a total of 62 smart card projects in the federal government. These projects have provided a range of benefits and services to agencies and individual cardholders. Until

[1] 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. This processing capability distinguishes these cards from traditional magnetic stripe cards, which cannot process or exchange data with automated information systems.

recently, many of these projects were small-scale demonstration projects, involving 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, over the last 2 years, much larger projects have been initiated to provide agencywide identification credentials and support advanced technologies to verify the identity of people accessing computer systems. To date, the largest smart card program to be implemented in the federal government is the Common Access Card (CAC) program of the Department of Defense (DOD), which is intended to be used for identification by about 4 million military and civilian personnel. Results from projects that are already in place indicate that smart cards offer many useful benefits, such as significantly reducing the processing time required for deploying military personnel, tracking immunization records of children, and verifying the identity of individuals accessing buildings and computer systems.

While the technology offers benefits, launching smart card projects—whether large or small—has proved challenging to federal agencies. According to agency officials, the multiple benefits of smart card adoption can be achieved only if key management and technical challenges are understood and addressed. Major implementation challenges include the following:

- *Sustaining executive-level commitment.* Without executive-level support and clear direction, large-scale smart card initiatives may encounter organizational resistance and cost concerns that lead to delays or cancellation. DOD officials stated that having a formal mandate to proceed with their CAC program has been crucial to its success.

- *Recognizing resource requirements*. Implementing a smart card system can be an expensive undertaking. Extensive upgrades may be needed to an agency's technical infrastructure, such as installing smart card readers on every computer system or developing new back-end systems to process and keep track of the identities associated with each card. If a public key infrastructure (PKI) is implemented in conjunction with smart cards, additional costs may be incurred to modify existing software applications so that they work with smart cards and PKI.[2] Nevertheless, to obtain significant benefits such as increasing security over buildings, safeguarding computer systems and data, and conducting financial and nonfinancial transactions more accurately and efficiently, these costs may be justified.

- *Integrating physical and logical security practices across organizations*. The ability of smart card systems to address both physical and "logical" security[3] means that unprecedented levels of cooperation may be required among internal organizations that often had not previously collaborated, such as physical security organizations and information technology (IT) organizations. Further, a departmentwide smart card initiative is likely to require substantial changes in existing processes for credentialing individuals, verifying those credentials when presented at building entrances, and accessing and using computer systems.

- *Achieving interoperability among smart card systems*.[4] As agencies consider adopting smart cards and plan specific implementations, it will be important to ensure that these implementations are consistent across the government. Developing standards to ensure that smart cards, card readers, and related technologies such as biometrics can interoperate across government will be critical to realizing the benefits that could be achieved by investments in such technologies.

- *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 themselves is not foolproof and must be addressed when agencies plan the implementation of smart card systems. In addition, protecting the

[2] A public key infrastructure is a system of computers, software, and data that relies on certain cryptographic techniques for some aspects of security. For more information, 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).

[3] Access to computer systems is known as "logical access," in contrast to "physical access," which applies to buildings and other physical facilities.

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

privacy of personal information is of growing concern and must be addressed with regard to the data contained on smart cards.

These challenges have slowed the adoption of smart card technology in past years; however, in the future, these challenges may prove less difficult, not only because of increased management attention to securing federal facilities and information systems, but also because technical advances have improved the capabilities and reduced the cost of smart card systems.

GSA's effectiveness in promoting smart card technology in the federal government has been mixed. The agency has contributed significantly to making it easier for federal agencies to acquire commercial smart card products by implementing a governmentwide contracting vehicle based on technical standards developed in collaboration with the National Institute of Standards and Technology (NIST) and smart card vendors. Further, it has taken action to organize federal smart card managers and share information about the technology. While these activities have been helpful, GSA has not taken other important steps to improve smart card initiatives and deployment strategies. For example, GSA's effectiveness in demonstrating the value and readiness of smart card technology to other agencies and officials was limited because of problems implementing its own internal smart card systems and coordinating its smart card policies. Further, the agency has not kept its administrative guidelines or implementation strategy up to date. Nor has it established standards for the use of smart cards as a component of federal building security processes. Finally, GSA has not developed a framework for evaluating smart card implementations to help agencies reduce risks and contain costs.

While GSA can unilaterally take a number of actions to promote smart card adoption, it shares responsibility for governmentwide guidance with the Office of Management and Budget (OMB) and NIST. OMB has statutory responsibility to develop and oversee policies, principles, standards, and guidelines used by agencies for ensuring the security of federal information and systems, but it has not issued policy or guidance specifically addressing smart cards since designating GSA the lead for promoting the technology in 1996. NIST has continuing responsibility for coordinating the development of technical standards required by GSA's governmentwide smart card contract.

To enhance governmentwide security over federal personnel, buildings, and information systems, we are making recommendations to NIST, GSA, and OMB to take actions aimed at better supporting agency efforts to deploy interoperable smart-card-based identification systems.

We received written comments on a draft of this report from the Secretary of Commerce and DOD's Deputy Chief Information Officer. We also received oral comments from officials of OMB's Office of Information and Regulatory Affairs, including the Information Policy and Technology Branch Chief; from the Commissioner of the Immigration and Naturalization Service; from GSA's Associate Administrator for the Office of Governmentwide Policy; and from officials representing FAA, the Maritime Administration, the Transportation Security Administration, and Chief Information Officer of the Department of Transportation. All the agency officials who commented generally agreed with our findings and recommendations.

Background

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 cards—can be forged has contributed to increases in identity theft and related security and financial problems for both individuals and organizations.[5]

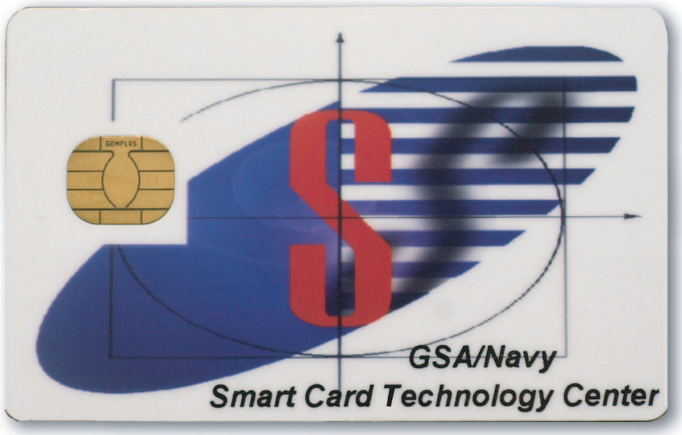
Smart cards are plastic devices about the size of a credit card that contain an embedded integrated circuit chip capable of both storing and processing data.[6] Figure 1 shows a typical example of a smart card. The unique advantage of smart cards—as opposed to cards with simpler technology, such as magnetic stripes or bar codes—is that smart cards can exchange data with other systems and process information rather than simply serving

[5] 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).

[6] 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. While this report includes some information on federal use of stored-value cards, it focuses chiefly on cards with processing capability.

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. A smart card's processing power also allows it to exchange and update many other kinds of information with a variety of external systems, which can facilitate applications such as financial transactions or other services that involve electronic record keeping.

Figure 1: A Typical Smart Card



Source: GSA.

Smart cards can also 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 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.

Even stronger authentication can be achieved by using smart cards in conjunction with biometrics. Smart cards can be configured to store biometric information (such as fingerprint templates 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. The combination of smart cards and biometrics can provide equally strong authentication for controlling access to physical facilities.[7]

Smart cards can also be used in conjunction with 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 electronic encryption keys, called "private keys," that are unique to each user and must be kept secret and secure. For example, storing and using private keys on a user's 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. However, 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]

In addition to enhancing security, smart cards have the flexibility to support a wide variety of uses not related to security. A typical smart card in use today can store and process 16 to 32 kilobytes of data, while newer

[7] For more information about biometrics, see U.S. General Accounting Office, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[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).

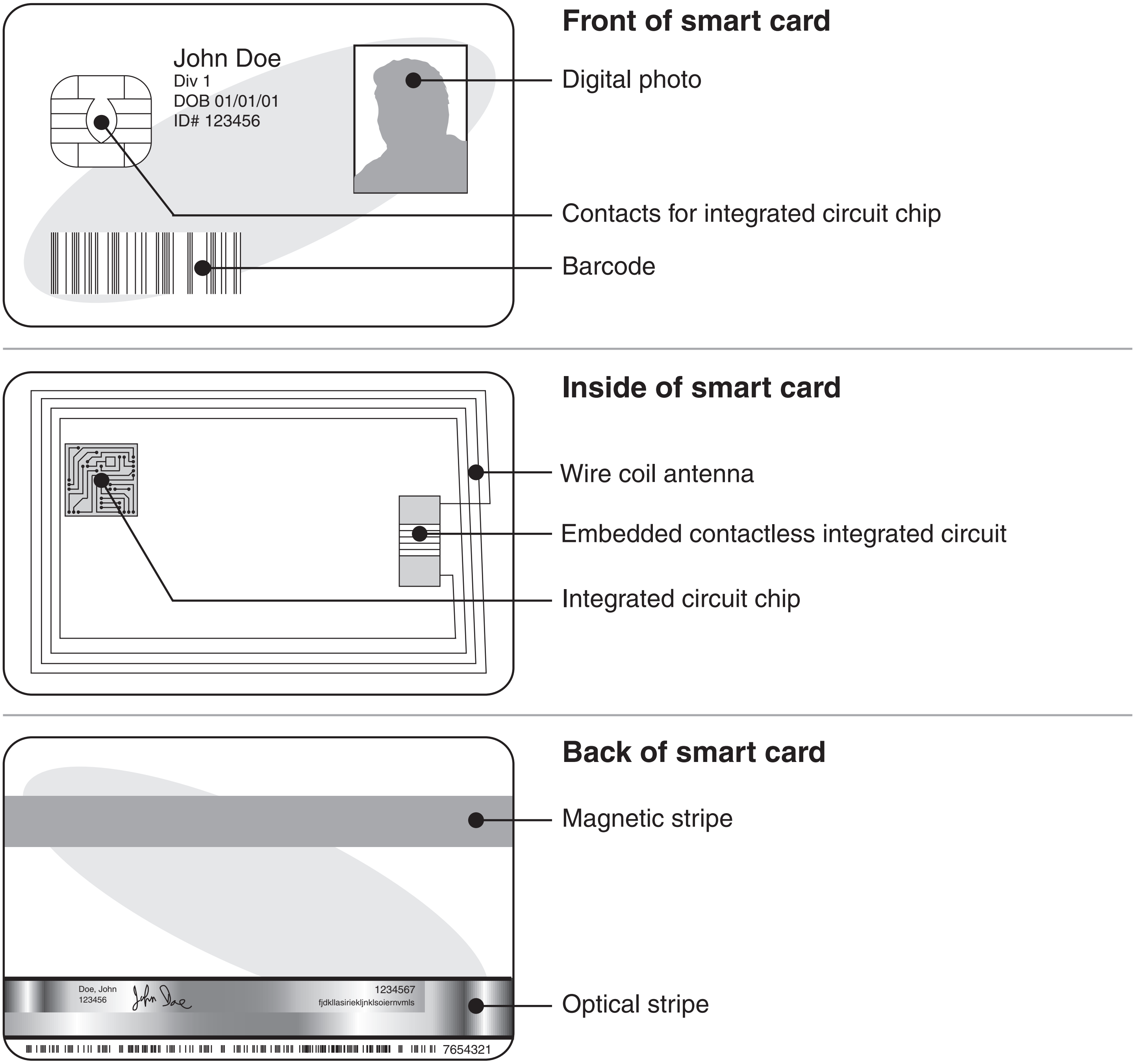
cards can accommodate 64 kilobytes. The larger the card's electronic memory, the more functions can be supported, such as tracking itineraries for travelers, linking to immunization or other medical records, or storing cash value for electronic purchases.

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 provide additional storage capacity. For example, 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 making that card and its stored data very difficult to counterfeit.[9]

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 shows some of the capabilities and features that can be included in smart cards.

[9] Cards with an optical memory stripe are known as laser cards or optical memory cards.

Figure 2: Features That May Be Incorporated into Smart Cards



Source: GAO.

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, GSA was tasked with taking the lead in facilitating a coordinated interagency management approach for the adoption of multiapplication smart cards across government. The tasking came from OMB, which has statutory responsibility to develop and oversee policies, principles, standards, and guidelines used by agencies for ensuring the security of federal information and systems. 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[10] (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, several legislative bills have been proposed or enacted in the wake of the events of September 11, 2001, to enhance national security and counterterrorism by using smart card and biometric technologies to better identify individuals entering the country or gaining access to mass transportation systems.[11]

Objectives, Scope, and Methodology

Our objectives were to assess (1) the extent to which federal agencies have adopted smart card technologies and realized the associated benefits, (2) the challenges of adopting smart cards within federal agencies, and (3) the effectiveness of GSA in promoting the adoption of smart card technologies within the federal government.

To assess the extent of smart card adoption by federal agencies and identify associated benefits and challenges, we reviewed smart card project documentation, cost estimates, and other studies from GSA; OMB;

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

[11] These bills included the Enhanced Border Security and Visa Entry Reform Act of 2002, P.L. No. 107-173, 116 Stat. 543, and the Department of Transportation and Related Agencies Appropriations Act, 2003, S.2808, 107th Cong. (2002).

the Western Governors' Association (WGA), which was responsible for a smart card project funded in part by the Departments of Agriculture and Health and Human Services; the Department of Justice's Immigration and Naturalization Service; DOD; and the Departments of Interior, Transportation, Treasury, and Veterans Affairs (VA). We also held discussions with key officials from these organizations regarding project benefits and challenges. Discussions were also held with representatives of the Smart Card Alliance, an association of smart card technology vendors, regarding smart card technology benefits and challenges. In addition, we reviewed publicly available materials and reports on smart card technology issues and discussed key issues with representatives of these organizations.

To assess GSA's effectiveness in promoting the governmentwide adoption of smart cards, we reviewed contract task orders, examined pilot project documentation, and assessed smart card plans and other reports obtained from the agency. We also held discussions with key officials in GSA's Office of Governmentwide Policy, Federal Technology Service, and Public Building Service to obtain information on internal pilot projects and other key plans and documents. We analyzed reports and evaluations on the smart card program obtained from GSA's Office of Inspector General. To obtain information on whether GSA had taken an effective leadership role in fostering the adoption of smart card technology across government, we interviewed officials from NIST; DOD; VA; the Departments of Interior, Transportation, and Treasury; and OMB. We also interviewed officials from WGA.

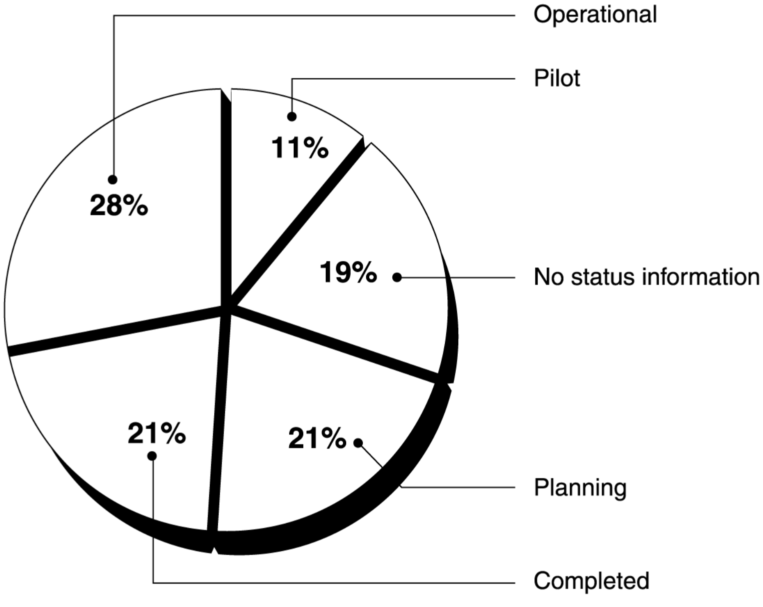
We performed our work between April and October 2002 in accordance with generally accepted government auditing standards.

Many Government Smart Card Projects Are under Way or Planned, Offering a Variety of Benefits

Since 1998, multiple smart card projects have been launched, addressing an array of capabilities and providing many tangible and intangible benefits, such as ways to better authenticate the identity of cardholders, increase security over buildings, safeguard computer systems and data, and conduct financial and nonfinancial transactions more accurately and efficiently. For some federal agencies, the benefits of using smart card technology (such as improving security over federal buildings and systems and achieving other business-related purposes) have only recently been recognized, and many agencies are still planning projects or evaluating the benefits of this technology before proceeding with more wide-scale initiatives. Still, results from several ongoing smart card projects suggest that the technology offers federal agencies a variety of benefits.

According to information obtained from GSA, OMB, and other federal agencies, as of November 2002, 18 federal agencies were planning, testing, operating, or completing a total of 62 smart card projects. These projects varied widely in size and technical complexity, ranging from small-scale, limited-duration pilot projects to large-scale, agencywide initiatives providing multiple services. The projects were reported to be in varying stages of deployment. Specifically, 13 projects were in the planning stage, and 7 were being piloted. An additional 17 projects were listed as operational, and 13 had been completed. No information was provided about the project phase of the remaining 12 initiatives; it is not clear whether these projects had moved beyond the planning or pilot testing phases. Figure 3 shows the status of the 62 federal smart card projects identified by GSA and OMB. Table 1 provides additional summary information about these projects.

Figure 3: Distribution of 62 Federal Projects by Project Phase



Source: GSA and OMB.

Table 1: Summary Information on 62 Federal Smart Card Projects

Federal agency	Number of projects	Status	Description
Agriculture	1	1 operational	Agriculture has implemented a system using a 24k chip card to automatically collect marketing data from peanut farmers under the peanut quota system.
Commerce	5	1 planned 1 pilot (for 3, deployment status information not available)	NIST is in the planning phase of its smart card project and is completing a feasibility study, exploring PKI and biometrics. The Patent and Trademark Office is piloting a smart card for its Patent Work at Home program using two-factor authentication and PKI technology for secure remote logical access. This card is also used as a property pass and as a stored-value card for transit subsidies.
DOD	26	1 planned 3 pilot 10 operational 6 completed (for 6, deployment status information not available)	Most of these pilots/programs were used within bases or among particular deployments and date back to the mid to late 1990s. The majority of the projects, a total of 22, used the smart card's ability to track various types of information: inventory control, food service, manifesting, and personnel accountability. Physical and/or logical access capabilities were a part of a little less than half (10) of the projects. The largest DOD deployment of smart cards (1.4 million cards), to date, is the CAC program, which is still being implemented. DOD has set policy directing that all its previous smart card programs be integrated into the CAC, with the exception of financial applications. CAC is planned for use by more than 4 million individuals and features PKI, physical and logical access controls, and space reserved for organization-specific applications, in addition to several technologies already in use, such as magnetic stripes and barcodes.
Education	1	1 planned	The Student Financial Assistance Office plans to use approximately 1,344 smart cards for physical access, transit benefits, and asset management.
Energy	1	1 operational	Energy has a project to issue cards to 28 employees working to clean up and shut down the Rocky Flats Technology site. The smart cards are to be used for physical access to restricted areas.
GSA	3	1 operational 2 completed	GSA headquarters has a smart card in operation for physical and logical access. Medical and meeting attendance applications have also been developed for use with this card. A completed pilot at GSA's Willow Wood Facility used a smart card for logical and physical access, for property management, and as a travel/purchase/phone card. Smart cards were also used at the 1997 presidential inauguration for access control, housing, and telephone support; they allowed security personnel to monitor movements within the headquarters facility.
HUD	2	1 pilot 1 completed	The completed project used a 2k chip card for internal and physical access at HUD's headquarters building. HUD discontinued the program in 1997 and decided to pursue proximity ID cards.
Interior	3	1 planned 2 pilot (for 1, deployment status information not available)	The National Park Service is planning to implement a Firefighters Training Card that will carry qualification and certification information. The Bureau of Land Management has distributed 1,100 cards to employees at five sites for physical access and limited use with PKI-enabled applications. This pilot will most likely be expanded agencywide. The Minerals Management Service is piloting a smart card with about half its employees (600 cards) and is planning to test its security applications.

(Continued From Previous Page)

Federal agency	Number of projects	Status	Description
Justice	5	2 planned (for 3, deployment status information not available)	The organizations within Justice undertaking smart card projects are the Management Division, Civil Division, Federal Bureau of Investigation, Office of Inspector General, and National Drug Intelligence Center.
Labor	1	1 operational	Labor has 720 smart cards in use.
NASA	1	1 planned	PKI certificates will be used to authenticate and grant NASA employees and contractors physical and logical access at NASA facilities.
National Science Foundation	1	1 planned	The National Science Foundation plans to issue 1,500 smart cards.
Social Security Administration	1	1 planned	Within the Social Security Administration, 8,868 cards will be used to track government property.
State	1	1 operational	Approximately 1,250 cards have been issued to State employees for physical and logical access. The cards also carry State PKI certificates. Plans call for 20,000 employees in the national capital region to receive this card in the near future.
Transportation	3	3 planned	Transportation is planning three pilot projects to implement smart card technology. First, the FAA Identification Media project plans to issue over 10,000 cards to federal employees and contract personnel primarily for physical access to FAA facilities. Second, the Transportation Security Administration's Transportation Worker Identification Card is planned to be issued to approximately 10–15 million transportation workers for physical and logical access to facilities and systems. Third, a stored value card is planned to be issued to 25,000 Transportation employees as part of the Federal Transit Administration Assistance program. Information gathered using this card will provide better data for ridership analysis and transit route planning.
Treasury	2	1 planned 1 operational	Treasury planned to distribute 10,500 cards to test various uses including physical and logical access, property management, biometrics, and food service eligibility. Upon validation, officials expect the project to be expanded agencywide. IRS is using smart cards to obtain secure dial-in access to the IRS local area network.
U.S. Agency for International Development	1	1 completed	The U.S. Agency for International Development implemented a pilot smart-card-based national electronic payment system in Armenia. The project has been discontinued.
Veterans Affairs (VA)	3	1 operational (for 2, deployment status information not available)	VA has issued 24,038 cards containing demographic, emergency, and eligibility data as well as PKI certificates to allow digital signatures on electronic service delivery transactions at two sites. An additional two VA hospital locations separately tested smart cards as ID badges and for electronic purchases to be used for vending, cash registers, and automatic teller machines.

Source: GSA and OMB.

Many pilot projects initiated in the late 1990s deployed smart cards for specific, limited purposes in order to demonstrate the usefulness of the technology. For example, GSA distributed smart cards to approximately

3,000 staff and visitors at the 1997 presidential inauguration to control physical access to that event. The cards contained information that granted individuals access to specific event activities and allowed security personnel to monitor movements within the event's headquarters facility as well as maintain records on those entering secure areas.

Likewise, many smart card pilot projects were implemented by the military services to demonstrate the technology's usefulness in enhancing specific business operations, such as creating electronic manifests to help deploy military personnel more efficiently, managing medical records for military personnel, and providing electronic cash to purchase goods and food services at remote locations. Officials at military bases and installations participating in these pilots reported that smart cards significantly reduced the processing time required for deploying military personnel—from several days to just a few hours.

Recently, broader and more permanent projects have begun. Among federal agencies, DOD has made a substantial investment in developing and implementing an agencywide smart card system. DOD's CAC is to be used to authenticate the identity of nearly 4 million military and civilian personnel and to improve security over on-line systems and transactions. The cards are being deployed in tandem with the rollout of a departmentwide PKI. As of November 2002, DOD had issued approximately 1.4 million CACs to military and civilian personnel and had purchased card readers and middleware[12] for about 1 million of its computers. More information about DOD's program appears in appendix I.

The Department of Transportation is also developing two large smart card pilot projects, which will be focused on controlling access to and improving security at the nation's many transportation hubs as well as at federal facilities controlled by the department. One pilot aims to distribute smart cards to approximately 10,000 FAA employees and contractor personnel for access to the department's facilities. Subsequent phases will be implemented across the agency to approximately 100,000 employees. In the second pilot, transportation worker identification cards will be issued to about 15 million transportation workers across the United States and is intended to improve physical and logical access to public transportation

[12] Middleware is software that allows a software application running on another system to communicate and exchange data with the integrated circuit chip on a smart card.

facilities. Transportation plans to document results from the pilot project, including benefits and costs.

Other federal agencies are now using smart cards for controlling logical access to computer systems and networks. For example, the Internal Revenue Service (IRS) distributed smart cards to approximately 30,000 of its revenue agents and officers for use when accessing the agency's network remotely through notebook computers. According to an IRS official, the cards are still in use and working well.

In July 2002, the Department of the Treasury announced plans to launch a pilot project to assess the use of smart cards for multiple purposes, including both physical and logical access. Treasury plans to distribute smart cards equipped with biometrics and PKI capabilities to approximately 7,200 employees during its pilot test. Treasury's main department offices and five Treasury bureaus will be involved in the pilot test: U.S. Secret Service; IRS; Bureau of Alcohol, Tobacco, and Firearms; Bureau of Engraving and Printing; and the Federal Law Enforcement Training Center. According to Treasury officials, if the smart card pilot proves successful, it will be implemented across the department.

While efforts such as these represent a recent trend toward adopting agencywide smart cards for security functions, almost half (42 percent) of the projects that have been undertaken to date, as identified by GSA and OMB, involved storing either cash value on the cards for use in making small purchases or other information for use in processing electronic payment transactions, transit benefits, or agency-specific applications. Many of these projects (45 percent) used smart cards that supported a combination of media, such as magnetic stripes, bar codes, and optical memory stripes. Further, the majority (86 percent) of these non–security-oriented projects involved cards used internally, usually to support formerly paper-based functions. For example, in October 1994, the 25th Infantry Division in Hawaii was issued 30,000 smart cards configured to support medical documentation, mobility processing, manifesting, personnel accountability, health care, and food service. In this pilot, the most notable benefit was seen in deployment readiness. The deployment process, which normally took a day or more, was reduced to a matter of hours.

In another example of a stored-value card project, the Departments of Agriculture and Health and Human Services supported a project by the WGA to issue smart cards to approximately 12,000 individuals—including pregnant women, mothers, and children—who were eligible for electronic benefits transfer (EBT) programs such as the Women, Infants, and Children program, Head Start, Food Stamps, and other public health programs in three different states. The smart cards contained a circuit chip that included demographic, health, appointment, and EBT information, as well as a magnetic stripe that included Medicaid eligibility information. The smart cards also allowed grocery and retail establishments to track food purchases and rebate offers or coupon redemptions more accurately. Users helped control information stored on the card with a personal identification number and were provided with kiosks to read or view information stored on the card. According to WGA officials, the pilot was a success because participants had immediate access to healthcare appointment and immunization records. In addition, federal and state agencies were able to track benefits and baby formula purchases more accurately, resulting in manufacturers no longer questioning the process used by these government organizations to collect millions in rebate offers.

To demonstrate that a single smart card could have many uses and provide many benefits, GSA's Federal Technology Service introduced a multipurpose smart card to its employees during a pilot project conducted in the summer of 1999. The card functioned as a property management device, boarding pass for American Airlines, credit card for travel, and stored-value calling card. The card used fingerprint biometric technology, as well as digital certificates for use in signing E-mail messages. In addition, the card contained a contactless interface—an embedded antenna—that allowed cardholders to access transit services by waving the card near a card reader to electronically pay for these services.

Appendix I provides more detailed information about smart card projects at several government agencies.

Successful Adoption of Smart Cards Can Be Achieved If Challenges Are Met

The benefits of smart card adoption identified by agency officials 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, not only because of increased management concerns about securing federal facilities and information systems, but also because technical advances have improved the capabilities and reduced the cost of smart card systems. Major implementation challenges include

- sustaining executive-level commitment;

- recognizing resource requirements;
- coordinating diverse, cross-organizational needs and transforming organizational security practices;
- achieving interoperability among smart card systems; and
- maintaining security and privacy.

Sustaining Executive-Level Commitment

Nearly all the officials we interviewed indicated that maintaining executive-level commitment is essential to implementing a smart card system effectively. According to officials both within DOD and in civilian agencies, the formal mandate of the Deputy Secretary of Defense to implement a uniform, common access identification card within DOD was essential to getting a project as large as the CAC initiative launched and funded.[13] The Deputy Secretary also assigned roles and responsibilities to the military services and agencies and established a deadline for defining smart card requirements. DOD officials noted that without such executive-level support and clear direction, the smart card initiative likely would have encountered organizational resistance and cost concerns that would have led to significant delays or cancellation.

Treasury and Transportation 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 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

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

biometrics and PKI, are being implemented in tandem with the cards. However, in light of the benefits of better authenticating personnel, increasing security over access to buildings, safeguarding computer systems and data, and conducting financial and nonfinancial transactions more accurately and efficiently, these costs may be acceptable. 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 stated that obtaining adequate resources was critical to implementing a major government smart card system.

For example, Treasury's project manager estimated the overall cost for the departmentwide effort at between $50 and $60 million; costs for the FAA pilot project, which have not yet been fully determined, are likely to exceed $2.5 million.

At least $4.2 million[14] was required to design, develop, and implement the WGA Health Passport Project (HPP) in Nevada, North Dakota, and Wyoming and to service up to 30,000 clients. A report on that project acknowledged that it was complicated and costly to manage card issuance activities. The states encountered problems when trying to integrate legacy systems with the smart cards and had difficulty establishing accountability among different organizations for data stored on and transferred from the cards. The report 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; costs for this service likely would be about $200,000 annually.[15] WGA 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 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, DOD initially budgeted about $78 million for the CAC program in

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

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

2000 and 2001 and expected to provide the device to about 4 million military, civilian, and contract employees by 2003. It now expects to expend over $250 million by 2003—more than double the original estimate. Many of the increases in CAC program costs were attributed by DOD officials to underestimating the costs of upgrading and managing legacy systems and processes for card issuance. Card issuance costs likely will exceed $75 million out of the over $250 million now provided for CAC through 2003, based on information provided by DOD. These costs are for installing workstations, upgrading legacy systems, and distributing cards to personnel.

According to DOD 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 by 2003. 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. DOD provided about $712 million to issue certificates to cardholders as part of the PKI program but provided no additional funding to enable applications.[16]

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 IT organizations. Nearly all federal officials we 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. Individual bureaus and divisions often have strong reservations about supporting a departmentwide smart card initiative because it would likely result in substantial changes to existing processes for credentialing individuals, verifying those credentials when presented at building entrances, and accessing and using computer systems.

[16] 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).

DOD officials stated that it has been difficult to take advantage of the multiapplication capabilities of its CAC for these very reasons. 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. DOD only recently has begun to consider ways to use the CAC across the department to better control physical access over military facilities. Few DOD facilities are currently using the card for this purpose. DOD 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 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 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 governmentwide Smart Access Common ID Card contract. Accordingly, GSA designed the contract to require awardees to work with GSA and NIST[17] to develop a government interoperability specification. The specification, as it currently stands, includes an architectural model, interface specifications, conformance testing requirements, and data models. A key aspect of the specification is that it addresses aspects of smart card operations that are not covered by commercial standards. Specifically, the 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. Version 2,[18] released in June 2002, is a significant improvement, providing better definitions of many details, such as how smart cards should exchange information with software applications and card readers. The revised specification also supports DOD's CAC data model in addition to the common data model developed for the original specification. However, it may take some time before smart card products that meet the requirements of version 2 are made available, because the contractors and vendors (under the Smart Access Common ID contract) will have to update or redesign their products to meet the enhanced specification. Further, potential interoperability issues may arise for those agencies that purchased and deployed smart card products based on the original specification.

While version 2 addressed important aspects of establishing interoperability among different vendors' smart card systems, other aspects remain unaddressed. For example, the version 2 specifications for

[17] NIST is the lead agency in the Standards Technical Working Group, which was established by the Government Smart Card Interagency Advisory Board (GSC-IAB) 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.

[18] *Government Smart Card Interoperability Specification, Version 2.0*, NIST Internal Report 6887 (June 27, 2002).

“basic services interface” provide for just 21 common functions, such as establishing and terminating a logical connection with the card in a specified reader. Other fundamental functions—such as changing personal ID numbers and registering cards when they are issued to users—are not included in the basic services interface. For such functions, vendors must use what are known as “extended service interfaces.” Because vendors are free to create their own unique definitions for extended service interfaces and associated software, interoperability problems may occur if interface designs or software programs are incompatible. NIST officials stated that, at the time the specification was finalized, it was not possible to define a standard for the functions not included in the basic services interface because existing commercial products varied too widely. According to the NIST officials, greater convergence is needed among smart card vendors' products before agreement can be reached on standards for all important card functions—including changing passwords or personal identification numbers—as part of extended service interfaces.

In addition, the guidelines do not address interoperability for important technologies such as contactless smart cards, biometrics, and optical memory stripes. GSA and NIST officials indicated that federal agencies are interested in adopting contactless and biometric technologies but that more needs to be done to evaluate the technologies and develop a standard architectural model to ensure interoperability across government. The government has not yet adopted industry-developed contactless and biometric standards, which are generally not extensive enough to ensure interoperability among commercial products from different vendors. According to one NIST official, a thorough risk assessment of optical stripe technology needs to be conducted first, because the security issues for a “passive” technology such as optical stripes are different from those of “active” chip-based smart cards.[19] Although there is no work under way to include optical stripe technology as an option within the Government Smart Card Interoperability Specification, the guidance does not preclude the use of this technology.

[19] Optical stripe technology is considered “passive” because it simply serves as a platform to store data; it cannot perform any processing functions. Chip-based cards, however, are capable of actively processing information and interacting with other systems.

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. As discussed in the background section of this report, 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.[20] 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.[21]

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)

[20] 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.

[21] 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.

As with any information system, the threats to a smart card system must be analyzed thoroughly and adequate measures developed to address potential vulnerabilities. Our 1998 report on effective security management practices used by leading public and private organizations[22] and a companion report on risk-based security approaches[23] identified key principles that can be used to establish a management framework for an effective information security program. In addition, the National Security Agency's draft guidelines[24] for placing biometrics in smart cards include steps that could be taken to help protect information in smart card systems, such as encrypting all private keys stored in the smart card and defining a system security policy with a user certification process before access to the system is granted.

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

[22] U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[23] U.S. General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D.C.: Nov. 1999).

[24] National Security Agency, *Guidelines for Placing Biometrics in Smartcards*, Draft Version 1.0 (Sept. 15, 1998).

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[25] 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. Accordingly, agency officials need to assess and plan for appropriate privacy measures when implementing smart card systems.

To address privacy concerns, officials with the WGA indicated that some participants in the HPP were made aware of the information that would be stored on their cards. Kiosks were installed in some grocery stores to encourage individuals to view the information stored on the cards. Similarly, GSA officials provided employees access to information stored on their headquarters ID cards and said they received few complaints about the cards.

While individuals involved in these projects had few concerns, others may require more assurances about the information stored on smart cards and how government agencies will use and share data. GSA, NIST, and other agency officials indicated that security and privacy issues are challenging, because governmentwide policies have not yet 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.

GSA's Effectiveness in Facilitating Federal Smart Card Adoption Has Been Limited

GSA's efforts to promote smart card technology in the federal government have focused on coordination and contracting-related activities. The agency has taken several useful actions to organize federal smart card managers and coordinate planning for the technology. Its chief contribution has been to make it easier for federal agencies to acquire commercial smart card products by implementing a governmentwide contracting mechanism based on a standard developed in collaboration with NIST and smart card

[25] 5 U.S.C. § 552a.

vendors. However, GSA has been less successful in other areas that are also important for promoting adoption of smart cards. For example, officials from other federal agencies indicated that GSA's effectiveness at demonstrating the technology's readiness for deployment was limited by its lack of success in implementing smart cards internally or developing a consistent agencywide position on the adoption of smart cards. Further, the agency did not keep its implementation strategy or administrative guidelines up to date. Nor has the agency established standards for the use of smart cards as a component of federal building security processes. Finally, GSA has not developed a framework for evaluating smart card implementations to help agencies reduce risks and contain costs.

GSA Has Addressed Many Planned Tasks Associated with Promoting Smart Cards

GSA has advanced federal adoption of smart card technology by addressing many of the major tasks outlined in the 1998 EPIC plan—which called for a standard governmentwide, multipurpose smart card system—and by developing its own smart card plan.[26] In response to OMB's 1996 tasking that GSA take the lead in promoting federal adoption of smart cards, the agency first established a technology office to support its smart card initiative and work with the President's Management Council on deploying the technology across government.[27] Beginning in 1998, GSA took steps to address tasks identified in the EPIC plan and its own plan, many of which required the collaboration and support of multiple agencies. For example, GSA worked with the Department of the Navy to establish a technology demonstration center to showcase smart card technology and applications and established a smart card project managers' group and Government Smart Card Interagency Advisory Board (GSC-IAB).[28] 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. GSA's Office of Governmentwide Policy was similarly established to better coordinate and

[26] GSA, *Office of Smart Card Initiatives—Overview and Concepts* (May 1998). The document includes 13 key objectives for implementation in 1998.

[27] This office was eventually moved into the Federal Technology Service so that it could also monitor 13 pilot projects aimed at fostering the adoption of smart card technology.

[28] 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.

define governmentwide electronic policies and technology standards in collaboration with other federal agencies and stakeholders.

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.[29] Under the terms of the 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. Major federal smart card projects, including DOD's CAC and Transportation's planned departmentwide smart card, have used or are planning to use the GSA contract vehicle.

GSA's achievements in promoting the federal adoption of smart card technology can be gauged by the progress it has made in addressing tasks laid out in the EPIC plan and its own smart card plan. Table 2, which provides more detailed information on major tasks from the EPIC and GSA plans and their current status, shows that GSA has taken steps to address many of these tasks.

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

Table 2: Status of Major Tasks from the EPIC and GSA Smart Card Plans

Task	Source	Milestone	Status	Comments
Form a customer advisory board to provide ongoing advice on the government's card service program	EPIC plan	July 1997	Addressed	GSA established a GSC-IAB in 2000 and smart card project managers' group in 1998.
Establish interagency team to evaluate several specific smart card applications	EPIC plan	January 1998	Partially addressed	GSC-IAB and NIST helped evaluate some smart card applications and standards, but not all issues have been addressed.
Establish a federal card services risk management forum	EPIC plan	March 1998	Open	Some agencies have completed risk assessments and shared the information with the smart card project managers group, but no forum has been established to address outstanding issues across government.
Establish contract for common access ID program	EPIC, GSA plans	September 1998	Addressed	The Smart ID contract was made available for agency use in May 2000.
Develop and issue final federal smart card interoperability guide	EPIC, GSA plans	June 1998	Addressed	Working with NIST, GSA issued the first version of the guidelines in August 2000 and revisions in June 2002.
Prototype multiapplication cards	EPIC plan	September 1998	Addressed	Since 1998, GSA and several other agencies have prototyped multiapplication cards.
Establish a Web-based clearinghouse for smart cards	EPIC plan	May 1998	Addressed	GSA established its smart card Web site at www.smart.gov.
Establish interagency work groups to address common access and core card applications	GSA plan	September 1998	Addressed	Through the GSC-IAB and NIST, common access and core card applications and interfaces have been addressed.
Implement and evaluate pilot projects	GSA plan	March 1999	Partially addressed	GSA launched several pilot projects but did not always evaluate the initiatives, according to the Office of Inspector General.
Work with international governments and establish on-line services	GSA plan	October 1998	Partially addressed	GSA and NIST are working with several international standards groups, but no on-line services have been established.
Develop and implement a smart card pilot project to improve electronic building access	GSA plan	September 1998	Partially addressed	Some limited pilot project testing has been completed to improve electronic building access.
Work with Sandia National Laboratories to develop a high-level vulnerability assessment framework for smart card access controls	GSA plan	September 1998	Partially addressed	Framework is not yet complete, though some initial analysis has been conducted.

(Continued From Previous Page)

Task	Source	Milestone	Status	Comments
Develop a joint security access program and technology center to demonstrate smart card technology	GSA plan	September 1998	Open	Although a technology center has been established, no work has been completed on a joint security access program. NIST and the Department of State recently established an Interagency Interoperability Task Force to address some of these issues.
Launch pilot internally and explore business lines for smart cards	GSA plan	December 1999	Addressed	GSA established a business line for smart cards in 1999.
Develop biometric application interface program for smart cards and conduct pilot projects	GSA plan	September 1998	Partially addressed	GSC-IAB, GSA, NIST, and DOD are considering standards for biometrics and some pilots are under way.
Develop interagency framework for managing card services across government, including evaluating and testing for compliance	GSA plan	Fall 1998	Open	GSC-IAB, GSA, and NIST are considering evaluation and testing suites for smart cards but have not yet developed an interagency framework.

Source: GAO.

GSA Has Not Fully Addressed Other Key Promotion Activities

Although GSA accomplished many of the tasks for promoting smart card adoption that were planned in 1998, many additional activities essential to advancing the adoption of smart cards across government still need to be addressed. Evolving federal security needs and steady advances in smart card technology mean that federal agency needs likely have changed since 1998. For example, in the wake of the events of September 11, 2001, increased management attention has been paid to security both for access to federal buildings as well as for protecting information systems. At the same time, advances in smart card technology have led to commercial products that are both cheaper and more capable, potentially altering cost/benefit calculations that agencies may have made in the past. Thus far, OMB has not issued any further policy or guidance related to smart card technology, although it was in the process of identifying and examining smart card technology issues at the time of our review.

In light of factors that have arisen or changed since GSA's smart card promotion objectives were set in 1998, we identified the following four specific issues that have not been addressed by GSA:

- *Showing leadership by successfully adopting smart cards internally.* A key element of effectively promoting the adoption of a new technology such as smart cards is to demonstrate the technology's effectiveness in an operational setting by successfully undertaking well-coordinated pilot projects that demonstrate the technology's benefits. One of the objectives in GSA's 1998 smart card plan was to lead by example in implementing and showcasing smart cards. Yet GSA's pilot projects have generally not allowed the agency to lead by example. According to a report completed by GSA's Office of Inspector General (OIG) in September 2000, there has been "no continued centralized management or direction of GSA's internal smart card implementation, nor any coordination and monitoring of pilots."[30] For example, the OIG reported that some of GSA's projects lacked management support and adequate funding, resulting in delays and partially completed project tasks. In terms of coordination, GSA has been unable to develop and implement a strategy to deploy smart card technology in a standard manner across the agency. For example, two divisions within GSA, the Federal Supply Service and the Public Building Service, while operating in areas where smart cards have a known benefit, did not use GSA's standard governmentwide contracting vehicle, which requires adherence to the government smart card interoperability specification. In addition, draft guidance on implementing a standard smart-card-based identification system across GSA was not prepared until April 2002 and is still incomplete and unapproved.

Officials at three federal agencies, actively engaged in developing their own smart card systems, said that GSA's internal track record for implementation had raised doubts about its ability to promote smart cards governmentwide. A Department of the Interior official stated that GSA had not been successful in building a business case for smart card adoption, and that, as a result, the Public Building Service was not supporting the Federal Technology Service's efforts to implement smart card technology at government facilities, causing problems for tenant agencies looking to move to smart-card-based systems. Similarly, a DOD official stated that GSA did not have the expertise to successfully implement smart cards or assist others attempting to do so because it lacked practical experience deploying the technology internally and working collaboratively with different organizations on management and technical issues.

- *Maintaining an up-to-date implementation strategy and smart card guidelines.* GSA's implementation strategy for smart cards consists of

[30] Office of Inspector General, GSA, *Review of Smart Card Initiatives*, Report Number A000874 (Sept. 11, 2000), p. 5.

the plan it prepared in 1998 as well as the EPIC plan, also developed in 1998. Neither addresses recent issues related to smart card implementation, such as advances in smart card technology or increased federal security concerns since the attacks of September 11, 2001. In 2002, GSA began to survey federal agencies, through the GSC-IAB, on smart card implementation issues they were experiencing.[31] According to GSA officials, the GSC-IAB survey will provide input to the agency that can be used to update its agenda for promoting federal smart card adoption. However, GSA has not yet committed to developing a new planning document with revised objectives and milestones.

GSA also has not updated its smart card administrative guidelines since 2000. In October 2000, GSA issued its guidelines for implementing smart cards in federal agencies.[32] GSA developed the guidelines "to provide step-by-step guidance for those agencies wishing to utilize the Smart Identification Card contract vehicle to procure and implement an interoperable employee identification card." Although the stated purpose of this document was to complement the Smart Identification Card contract, the section discussing standards and specifications does not refer to the government smart card interoperability specification recently developed by GSA and NIST, nor does it provide explicit guidance on using the interoperability specification or other critical technologies, such as contactless cards and biometrics.

- *Coordinating the adoption of standard federal building security processes.* GSA has not taken action to develop and coordinate standard procedures for federal building security, which would help agencies implement smart-card-based ID systems in a consistent and effective manner. GSA is responsible for managing security at over 7,300 federal facilities, with widely varying security needs.[33] In 1999, several internal

[31] GSA contracted with Maximus, a private consulting firm, to conduct a survey of agencies, private sector partners, and others to help identify issues critical to the smart card initiative and define future goals and objectives for the GSC-IAB.

[32] GSA, *Smart Card Policy and Administrative Guidelines* (Oct. 20, 2000).

[33] The Department of Justice established five security categories for federal buildings, ranging from facilities that require limited security (category 1) to buildings that require a maximum level of security mechanisms or safeguards (category 5). No criteria exist on the security or electronic devices that need to be installed at facilities that fall within these categories.

GSA organizations—including the Office of Governmentwide Policy, the Federal Technology Service, the Federal Supply Service, and the Public Building Service—proposed working together to develop a standard approach for federal building security using smart card technology. However, this proposal has not been adopted, nor has any alternative strategy been developed for deploying smart card technology at federal facilities. Officials in the Federal Technology Service and the Public Building Service said that they intended to work together to develop a strategy for smart card use at federal facilities, but they have not yet begun to do so.[34]

Although not part of a concerted standards setting process, the Federal Technology Service's recently launched pilot smart card project could serve in the future as a basis for a federal building security standard. The pilot involved upgrading and standardizing building security systems at three government facilities in Chicago, Illinois. The project is based on smart cards with biometric capabilities to identify employees entering these facilities. At least three federal agencies are expected to participate in the project, and its costs have been estimated to range between $450,000 and $500,000. If the project is successful, it may serve as an example for other federal agencies interested in using smart card technology for their building security processes.

- *Evaluating projects to reduce implementation risks and costs.* Although GSA has developed administrative and business case guidelines to help agencies identify smart card benefits and costs, as well as establishing the smart card program managers' group and the GSC-IAB to discuss project issues, it has not established a framework for evaluating smart card projects to help agencies minimize implementation costs and risks and achieve security improvements. In September 2000, the GSA OIG reported that measurable standards were needed to assess smart card projects and help GSA lead the smart card program. It also suggested that more information and lessons learned from smart card pilot projects were needed to make improvements in the federal smart card program and to better ensure success.[35] GSA

[34] For a discussion of the full range of building security technologies, including smart cards, see U.S. General Accounting Office, *National Preparedness: Technologies to Secure Federal Buildings*, GAO-02-687T (Washington, D.C.: Apr. 25, 2002).

[35] Office of the Inspector General, GSA, *Review of Smart Card Initiatives*, Report A000874 (Sept. 11, 2000).

agreed with the issues identified by the OIG but has not yet taken action to address recommendations cited in the report.

Officials from other agencies indicated that more information is needed on smart card implementation costs and opportunities for cost savings to help agencies make a business case for the technology and to address implementation challenges. According to one agency official, more information sharing is needed on smart card implementation strategies that work and that help reduce project management costs and problems with software and hardware implementation. Agency officials also indicated that measures are needed to determine whether smart cards are working as intended to improve security over federal buildings, computer systems, and critical information, as called for by the President's Management Agenda and the Office of Homeland Security. GSA officials indicated that many of these issues likely would be addressed by the GSC-IAB at some later date but that no specific milestones for doing so had been set.

Conclusions

Progress has been made in implementing smart card technology across government, with increasingly ambitious projects, such as DOD's CAC, being initiated in recent years as federal managers focus on implementing smart cards to enhance security across organizations. To successfully implement smart-card-based systems, agency managers have faced a number of substantial challenges, including sustaining executive-level commitment, obtaining adequate resources, integrating physical and logical security practices, achieving interoperability among smart card systems, and maintaining system security and privacy of personal information. As both technology and management priorities evolve, these challenges may be becoming less insurmountable, particularly with the increased priority now being placed on heightened security practices to better maintain homeland security. Further, the interoperability challenge may be significantly reduced as continuing efforts are made to increase the scope and usefulness of the government smart card interoperability specification.

However, without overall guidance and budgetary direction from OMB, agencies may be unnecessarily reluctant to take advantage of the potential of smart cards to enhance security and other agency operations. Although OMB has statutory responsibility to develop and oversee policies, standards, and guidelines used by agencies for ensuring the security of federal information and systems, it has not issued any guidance or policy on governmentwide adoption of smart cards since 1996, when it designated GSA the lead for promoting federal adoption of the technology.

GSA continues to play an important role in assisting agencies as they assess the potential of smart cards and move to implement them. GSA has already provided important technical and management support by developing the Smart Access Common ID contract vehicle, supporting NIST's development of the government smart card interoperability specification, and setting up the GSC-IAB. However, GSA has not taken all the steps it could have to provide full support to agencies contemplating the adoption of smart cards. Its implementation strategy and administrative guidance have not been kept up to date and do not address current priorities and technological advances. Nor have building security standards been adopted or an evaluation process developed that address implementation of smart card systems. If such tasks were addressed, federal agency IT managers would face fewer risks in deciding how and under what circumstances to implement smart-card-based systems.

Recommendations

We recommend that the Director, OMB, issue governmentwide policy guidance regarding adoption of smart cards for secure access to physical and logical assets. In preparing this guidance, OMB should seek input from all federal agencies that may be affected by the guidance, with particular emphasis on agencies with smart card expertise, including GSA, the GSC-IAB, and NIST.

We recommend that the Director, NIST, continue to improve and update the government smart card interoperability specification by addressing governmentwide standards for additional technologies—such as contactless cards, biometrics, and optical stripe media—as well as integration with PKI, to ensure broad interoperability among federal agency systems.

We recommend that the Administrator, GSA, improve the effectiveness of its promotion of smart card technologies within the federal government by

- developing an internal implementation strategy with specific goals and milestones to ensure that GSA's internal organizations support and implement smart card systems, based on internal guidelines drafted in 2002, to provide better service and set an example for other federal agencies;

- updating its governmentwide implementation strategy and administrative guidance on implementing smart card systems to address current security priorities, including minimum security standards for federal facilities, computer systems, and data across the government;

- establishing guidelines for federal building security that address the role of smart card technology; and

- 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.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Secretary of Commerce and DOD's Deputy Chief Information Officer. We also received oral comments from officials of OMB's Office of Information and Regulatory Affairs, including the Information Policy and Technology Branch Chief; from the Commissioner of the Immigration and Naturalization Service; from GSA's Associate Administrator for the Office of Governmentwide Policy; and from officials representing FAA, the Maritime Administration, the Transportation Security Administration, and Chief Information Officer of the Department of Transportation. All the agency officials who commented generally agreed with our findings and recommendations.

In addition, Commerce commented that a governmentwide smart card program was needed and that a central activity should be created to manage and fund such an initiative. However, we believe that, with sufficient policy guidance and standards to ensure broad interoperability among agency systems, agencies can effectively develop smart card programs tailored to their individual needs that also meet minimum requirements for governmentwide interoperability.

DOD commented that NIST should be tasked with taking the lead in developing and maintaining interoperability standards for smart cards and biometrics. DOD also stressed the importance of biometric technology interoperability with smart cards in support of the adoption of a single set of authenticating credentials for governmentwide use. Finally, DOD also commented that the use of smart card technology for federal building security should be strengthened. We believe our recommendations are consistent with the department's comments.

GSA noted that significant work had gone into developing smart card technology and provided additional details about activities it has undertaken that are related to our recommendations.

In addition, each agency provided technical comments, which have been addressed where appropriate in the final report.

Unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Ranking Minority Member, Subcommittee on Technology and Procurement Policy, Committee on Government Reform, and other interested congressional committees. We will also send copies to the Director, OMB; the Director, NIST; and the Administrator, GSA. Copies will be made available to others upon request. In addition, this report also will be available at no charge on our home page at http://www.gao.gov.

If you have any questions concerning this report, please call me at (202) 512-6240 or send E-mail to koontzl@gao.gov. Other major contributors included Barbara Collier, Jamey Collins, John de Ferrari, Steven Law, Freda Paintsil, and Yvonne Vigil.

Sincerely yours,

Linda D Koontz

Linda D. Koontz
Director, Information Management Issues

Appendix I

Information about Selected Government Smart Card Projects

As part of our review, we examined smart card projects managed by the Departments of Defense (DOD), Interior, Transportation, Treasury, and Veterans Affairs (VA), as well as the Immigration and Naturalization Service (INS) and the Western Governors' Association (WGA). These projects supported a variety of applications and used or considered smart card technology to improve logical and physical controls over systems and facilities, as well as to store information for other purposes, such as conducting financial transactions. The following provides more information on these projects.

Department of Defense

In 1999, the Deputy Secretary of Defense issued a policy directive that called for the implementation of a standard smart-card-based identification system for all active duty military personnel, DOD civilian employees, and eligible contractor personnel, to be called the Common Access Card (CAC) program.[36] The directive assigned the Department's Chief Information Officer overall responsibility to develop departmentwide smart card policy and conduct oversight of the program. Further, the Department of the Navy was made responsible for developing departmentwide interoperability standards for using smart card technology, and the National Security Agency was given the lead for developing a departmentwide public key infrastructure (PKI) program to be integrated with the CAC.

In October 2000, Defense began initial rollout with plans to distribute cards to approximately four million individuals across the department by 2003. The CAC is equipped with a 32-kilobyte chip formatted in a standard manner to ensure interoperability among the military services and defense agencies. It also includes a set of PKI credentials, including an encryption key, signing key, and digital certificate. To obtain a CAC, individuals must produce multiple forms of identification. DOD's PKI-enabled computer systems then examine the digital certificate produced by a user's card to determine whether the cardholder is granted access to specific DOD systems. DOD is working to adapt its E-mail systems to work with PKI to better ensure that electronic messages are accessible only by designated recipients. In addition, according to DOD, cardholders will be able in the future to electronically sign travel vouchers using the digital certificates on their cards.

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

In the future, DOD plans to add biometrics and other advanced capabilities to the CAC. Biometric data will be stored on the card and could include fingerprints, palm prints, iris scans, or facial features. To store these data, the amount of memory on the card would be doubled from 32 kilobytes to 64 kilobytes. DOD also plans to improve physical security controls over installations and bases by adding a contactless chip to the CAC to avoid delays when military personnel enter facilities.

Department of the Interior

In January 2002, the Department of the Interior's Bureau of Land Management (BLM) launched a smart card pilot project to help improve security over its sites and employees. The bureau has 164 major sites and approximately 13,000 full- and part-time employees, including contractors. About 1,100 employees were given smart cards for personal identification and to improve safeguards at pilot sites in Nevada and Arizona. The pilot's goal was to demonstrate the feasibility and interoperability of smart cards and to communicate their potential to employees throughout the bureau. In addition to distributing 1,000 more smart cards to bureau employees by November 2002, the bureau expects to equip about 1,000 of the existing cards with PKI certificates to be used with PKI-enabled software applications to improve security over systems and electronic transactions. According to bureau officials, the project has been a success, and it plans to continue the rollout of smart cards to remaining employees.

The bureauwide rollout is scheduled to begin in January 2003. The total estimated cost of the effort is $5.8 million, and according to the bureau's business case, this effort will break even in 2004. This includes all contracts, labor costs, software, hardware, and maintenance costs over a 5-year life cycle. The full implementation of the smart card system is expected to eliminate redundant administrative processes for personal identification and open up opportunities for additional applications by establishing digital certificates for creating digital signatures. All new and future building locations are planned to be equipped with the smart card technology necessary to pursue this effort, and many existing sites are being upgraded. BLM has reported experiencing a 70 percent drop in the cost of physical access systems since the cards' initial deployment. In one of the pilot locations, all processes are to be outsourced (except for human resources, physical access, and security officer functions), with bureau employees making all policy and business decisions.

Department of Transportation

The Department of Transportation currently has two large smart card projects targeted for deployment. In the first pilot, the Federal Aviation Administration (FAA) plans to distribute smart cards internally to approximately 10,000 employees and on-site contractor support personnel primarily to secure physical access to the agency's facilities. Recently, the FAA released a request for proposal outlining minimum requirements for smart card credentials. The agency plans to procure smart cards through the General Services Administration (GSA) Smart Access Common ID contract and will apply GSA's interoperability specification. The card is planned to be a Java-based[37] hybrid (contact and contactless) card, containing a 32-kilobyte chip as well as a magnetic stripe and barcode. The card will likely also feature a biometric for enhanced authentication (most likely fingerprint data).

The second pilot is being managed by the Transportation Security Administration (TSA), which is scheduled to be transferred to the Department of Homeland Security on March 1, 2003. For this pilot, the TSA plans to issue smart identification (ID) cards to up to 15 million "transportation workers"—defined as any persons who require unescorted access to a secure area in any transportation venue. The pilot project will be focused on major airports, seaports, and railroad terminals and will include all modes of transportation. TSA's goal is to create a standardized, universally recognized and accepted credential for the transportation industry. Initially, the transportation worker ID will be used for obtaining physical access to transportation facilities. Subsequently, a phased approach will be used to add logical access capabilities to the card. According to agency officials, the card will be designed to address a minimum set of requirements, but it will remain flexible to support additional requirements as needed. The card will be used to verify the identity and security level of the cardholder, and local authorities will grant access in accordance with local security policies.

TSA has established working groups for various aspects of system development, such as card design, identity documentation requirements, and card policy. To share costs and leverage existing resource investments,

[37] Java is a high-level, object-oriented programming language developed by Sun Microsystems that is well suited for use on the World Wide Web. Java card technology supports multiple, independently secure applications with a single smart card and is compatible with existing smart card standards from many organizations, such as the internationally recognized International Standards Organization.

TSA is currently working with INS on its entry/exit project to use established land, air, and sea ports as checkpoints. In addition, TSA has established working relationships with industry groups and coordinated with other agencies, such as Treasury and the Federal Bureau of Investigation, and is looking to develop cost sharing strategies for future implementations.

TSA's budget for fiscal year 2003 was not determined at the time of our review, and agency officials said that the availability of funds would determine how quickly the pilot would be implemented. The pilot will likely be implemented within the next 3 years. According to one agency official, the TSA program, if implemented successfully, would likely become the largest civilian agency smart card initiative to date.

Department of the Treasury

The Department of the Treasury plans to launch a proof of concept project to assess several smart card technologies for possible agencywide use for both physical and logical access. The project is being funded and managed by Treasury's Chief Information Officer Council at a cost of $2.8 million. Six Treasury organizations are participating in the pilot: the Secret Service; the Internal Revenue Service; the Bureau of Alcohol, Tobacco and Firearms; the Bureau of Engraving and Printing; the Federal Law Enforcement Training Center; and the main department. The Secret Service has been designated the lead bureau and will also lead the future departmentwide smart card project. In total, Treasury plans to issue about 10,000 smart cards. These cards are to be Java-based devices with 32 kilobytes of storage, capable of supporting multiple technologies for use in various configurations. For example, the cards will support both contact and contactless access, although not all will contain biometrics. All the cards are expected to contain PKI certificates for creating digital signatures and encrypting E-mail messages. The cards are also expected to be equipped with two-dimensional barcodes and a magnetic stripe to enable integration with existing systems.

Like DOD, Treasury plans to allocate space on the card for individual bureaus to use in creating their own applications, such as the Federal Law Enforcement Training Center's plan to use the cards when issuing uniforms to students. A Treasury official believes that using smart cards will simplify certain processes, such as property and inventory management, that are currently paper-based and labor-intensive.

Information from this proof of concept project will be used to launch an agencywide smart card project. GSA's Smart Access Common ID Contract and interoperability guidelines will be used to ensure that appropriate smart card technologies are evaluated. The proof of concept is expected to last about 6 months, with the pilot ending in January 2003. At that time, a report will be completed, and a business case for an agencywide smart card solution will likely be prepared. Preliminary cost estimates for implementing a Treasury-wide smart card system, which would support around 160,000 employees, is in the range of $50 to $60 million.

Department of Veterans Affairs

In April 2001, the Department of Veterans Affairs (VA) began issuing cards for its VA Express Registration Card pilot project. Initiated in 1999, the project was to provide agency customers with a smart card carrying medical and personal information that could be used to speed up registration at VA hospitals. The card was also intended to be usable by non-VA hospitals equipped with the necessary readers to access patients' VA benefits information.

At the time of our review, about 24,000 smart cards had been issued through two VA hospitals located in Milwaukee, Wisconsin, and Iron Mountain, Michigan. The cards are PKI enabled and can also be used throughout VA's network of hospitals—the majority of which do not have smart card readers—because they include all the same patient information found printed on the front of the older Veteran Identification Cards, which are still in use. The PKI capabilities of the card allow patients with a home computer and card reader to securely access their information on-line and digitally sign forms, saving time and offering convenience for both the patient and the agency. For those without Internet access, kiosks were installed at the two pilot locations, allowing Express Card holders to access their information, make any necessary changes, or request PKI certificates. The VA Express Card program used GSA's Smart Access Common ID contract for procurement and technical assistance.

According to agency officials, using the Express Card reduced registration time at hospitals by 45 minutes. Patients involved in the pilot project had access to express registration services, thus saving time. However, although the Express Card program is still in use, VA officials have decided not to expand beyond the two pilot locations. The reasons given were the expense of back-end automation, complications integrating the new system with legacy systems, and the lack of an existing card reader infrastructure at other VA hospitals. The agency maintains card management, support, and issuance capabilities at the pilot locations to support the smart cards that are still in use.

Immigration and Naturalization Service

The Department of Justice's INS currently has a card-based project under way to control access at the nation's borders. The project includes two types of cards—Permanent Resident Cards and Border Crossing Cards (also known as "Laser Visas"). As part of the Border Crossing Cards project, INS is working with the Department of State to produce and distribute the cards. Under the Illegal Immigration Reform and Immigrant Responsibility Act of 1996,[38] every Border Crossing Card issued after October 1, 2001, is required to contain a biometric identifier and be machine readable. The Laser Visas will store biographical information along with a photograph of the cardholder and an image of the cardholder's fingerprints. The Permanent Resident Cards will store similar information. Information from the Laser Visas is stored in a central INS database. As of June 2002, more than five million Laser Visas and approximately six million Permanent Resident Cards had been issued.

The Permanent Resident Card and Laser Visa make use of optical stripe technology, with storage capacity ranging from 1.1 megabyte to 2.8 megabytes, to store large amounts of information, but they do not contain integrated circuit chips to process data. As part of a cost-benefit analysis conducted in 1999, INS considered implementing chip-based smart cards and determined that smart card technology was not the best solution. This decision was based, in part, on the limited storage capacity of smart cards at the time. INS examined smart cards with 8 kilobytes of memory, which did not provide enough memory to store the fingerprint data required by law. Smart cards now have a storage capacity of up to 64 kilobytes and are capable of storing color photo images of individuals as well as full fingerprint images.

Western Governors' Association

In June 1999, WGA launched the Health Passport Project (HPP) in three states—Nevada, North Dakota, and Wyoming—to evaluate and test a range of applications and technologies based on a common smart card platform.

[38] The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 was enacted as division C of the Omnibus Consolidated Appropriations Act, P.L. No. 104–208, 110 Stat. 3009-546 (1996).

The project was to be conducted within an 18-month demonstration period and be integrated with other state-administered prenatal, physician care, nutrition, and early childhood education programs. Each state was expected to maintain common demographic information as well as clinical data on individuals participating in the pilot project. Selected sites also tested unique applications related to electronic benefits transfer (EBT), insurance eligibility, and health appointment information. WGA had overall responsibility for managing the HPP contract, and each state was responsible for providing on-site management, technical support, and funding as needed. The Departments of Agriculture and Health and Human Services also provided project funding and support, with GSA providing technical assistance as requested. The HPP initiative involved the distribution of 2,348 cards to individuals in Bismarck, North Dakota; 991 cards in Cheyenne, Wyoming; and 8,459 cards in Reno, Nevada. With additional state funding, the HPP initiative has continued to operate beyond the demonstration period, which concluded in December 2001.

The HPP platform consists of smart cards, special card readers attached to health providers' personal computers, card readers installed at grocery or retail establishments and register systems, servers to maintain backup databases, kiosks, and a network. The health passport card contains an 8-kilobyte chip, storing demographic, health, and benefit information on participants as well as a magnetic stripe for Medicaid eligibility information. Smart card readers are used to read and write information to the card. These devices are linked to HPP workstations and to the Women, Infants, and Children EBT application, which allows benefits to be stored on the card and used at grocery and retail establishments that have card readers installed at point-of-sale register locations. Kiosks are free-standing machines that operate by a touch screen feature and read information stored on the card.

In December 2001, the Urban Institute and the Maximus consulting firm prepared a report for WGA, which reviewed the results of the HPP initiative. The report stated that HPP was successful in bringing a concept to life. HPP enabled participants to use the EBT and healthcare appointment and immunization information more effectively and conveniently, because information was stored on the card. Project participants also liked using the cards and kiosks to access their personal information, and many liked being able to electronically track appointments and health care records. In addition, retailers liked the cards and the ability to track EBT data more accurately. WGA officials further noted that HPP has helped federal and state governments maintain more accurate information on EBT distributions and baby formula purchases, which can be used to request coupon rebates from manufacturers. More accurate sales information is available and shared with manufacturers to resolve disputes over rebates and to obtain more timely refunds.

Glossary

Attack

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.

Authentication

The process of confirming an asserted identity with a specified or understood level of confidence.

Biometrics

Measures of an individual's unique physical characteristics or the unique ways that an individual performs an activity. Physical biometrics include fingerprints, hand geometry, facial patterns, and iris and retinal scans. Behavioral biometrics include voice patterns, written signatures, and keyboard typing techniques.

Biometric template

A digital record of an individual's biometric features. Typically, a "livescan" of an individual's biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database or on an integrated circuit chip card.

Card edge

The set of command and response messages that allow card readers to communicate effectively with the chips embedded on smart cards.

Contactless smart card

A smart card that can exchange information with a card reader without coming in physical contact with the reader. Contactless smart cards use 13.56 megahertz radio frequency transmissions to exchange information with card readers.

Confidentiality

The assurance that information is not disclosed to unauthorized entities or processes.

Digital signature

A special encrypted code, attached to an electronic message, that can be used to prove to a third party that the message was, in fact, signed by the originator. Digital signatures may also be attached to other electronic information and programs so that the integrity of the information and programs may be verified at a later time.

Electronic government

Government's use of technology, particularly Web-based applications, to enhance the access to and delivery of government information and services to citizens, business partners, employees, other agencies, and government entities.

Identification

The process of determining to what identity a particular individual corresponds.

Interoperability

The ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Middleware

Software that allows a software application running on another system to communicate and exchange data with the integrated circuit chip on a smart card.

Nonrepudiation

The assurance that the identity of the sender of an electronic message can be proven and that delivery of the message to the recipient can also be proven so that neither party can later deny having processed the message.

Privacy

The ability of an individual to decide when and on what terms elements of his or her personal information should be revealed.

Public key infrastructure (PKI)

A system of hardware, software, and policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and nonrepudiation—that are important in protecting sensitive communications and transactions.

Smart card

A tamper-resistant security device—about the size of a credit card—that relies on an integrated circuit chip for information storage and processing.

GAO's Mission

The General Accounting Office, the 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 daily E-mail alert for newly released products" under the GAO Reports 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

PRINTED ON ♻ RECYCLED PAPER

[redacted]