United States Government Accountability Office

GAO

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

September 2004

ELECTRONIC GOVERNMENT

Federal Agencies Continue to Invest in Smart Card Technology

GAO-04-948

September 2004

ELECTRONIC GOVERNMENT

Federal Agencies Continue to Invest in Smart Card Technology

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-948, a report to the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives

Why GAO Did This Study

Smart cards—plastic devices about the size of a credit card—use integrated circuit chips to store and process data, much like a computer. Among other uses, these devices can provide security for physical assets and information by helping to verify the identity of people accessing buildings and computer systems. They can also support functions such as tracking immunization records or storing cash value for electronic purchases. Government adoption of smart card technology is being facilitated by the General Services Administration (GSA), which has implemented a governmentwide Smart Card Access Common ID contract, which federal agencies can use to procure smart card products and services.

GAO was asked to update information that it reported in January 2003 on the progress made by the federal government in promoting smart card technology. Specific objectives were to (1) determine the current status of smart card projects identified in GAO's last review, (2) identify and determine the status of projects initiated since the last review, and (3) identify integrated agencywide smart card projects currently under way. To accomplish these objectives, GAO surveyed the 24 major federal agencies.

In commenting on a draft of this report, officials from GSA and the Office of Management and Budget generally agreed with its content.

www.gao.gov/cgi-bin/getrpt?GAO-04-948.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6249 or koontzl@gao.gov.

What GAO Found

According to GAO's survey results, as of June 2004, more than half of the smart card projects previously reported as ongoing (28 out of 52) had been discontinued because they were absorbed into other smart card projects or were deemed no longer feasible. Of the remaining 24 projects, 16 are in planning, pilot, or operational phases and are intended to support a variety of uses (agencies did not provide current information for 8 projects). Twelve of the 16 projects are large-scale projects intended to provide identity credentials to an entire agency's employees or other large group of individuals. For example, the Department of Defense's (DOD) Common Access Card is to be issued to an estimated 3.5 million DOD-related personnel, and the Transportation Security Administration's Transportation Worker Identification Credential is to be used by an estimated 6 million transportation industry workers. The other 4 projects are smaller in scale, and are intended to provide access or other services to limited groups of people. For example, the Department of Commerce's Geophysical Fluid Dynamics Laboratory Access Card is to be issued to about 612 employees, contractors, and research collaborators. Further, in response to the survey, agencies reported 8 additional smart card projects that were ongoing at the time of the last review. These projects include 4 planned for multiple applications (such as identity credentials and access) and 4 for single applications, including stored value, access to computer systems, and processing travel documents.

Based on GAO's survey of federal agencies, 10 additional smart card projects have been initiated since the last review. These projects vary widely in size and scope. Included are small-scale projects, involving cards issued to as few as 126 cardholders (such as a project in the Department of Labor's Employment and Training Administration), and large-scale agencywide initiatives, such as the Department of Veterans Affairs Authentication and Authorization Infrastructure card, which is to be issued to an estimated 500,000 employees and contractors. Four agencies reported purchases under GSA's Smart Card Access Common ID contracting vehicle, and others likewise have plans to use this contract. Specifically, five agencies—the Departments of Defense, Homeland Security, the Interior, and Veterans Affairs, and the National Aeronautics and Space Administration—are planning to make an aggregated purchase of up to 40 million cards over the next 4 years using the GSA contract.

Finally, nine agencies are developing and implementing integrated agencywide smart card initiatives. These projects are intended to use one card to support multiple functions, such as providing identification credentials, accessing computer systems, and storing monetary values.

Contents

Abbreviations

CAC	Common Access Card
DHS	Department of Homeland Security
DOD	Department of Defense
FICC	Federal Identity Credentialing Committee
GSA	General Services Administration
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PKI	public key infrastructure
TSA	Transportation Security Administration
VA	Department of Veterans Affairs

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

September 8, 2004

The Honorable Adam H. Putnam
Chairman, Subcommittee on Technology, Information Policy,
Intergovernmental Relations, and the Census
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 these cards are 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 the government based on a goal of equipping all federal employees with a standardized smart card for a wide range of services. In support of this goal, GSA has implemented a governmentwide, standards-based contracting vehicle, the Smart Card Access Common ID contract, which federal agencies can use to procure smart card products and services. The contract specifies adherence to the government smart card interoperability[2] specification, which has been developed by the National Institute of Standards and Technology (NIST) and is intended to ensure that government smart card implementations achieve a minimum level of interoperability.

[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.

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

In January 2003, we reported on progress that the federal government had made in promoting the adoption of smart card technology.[3] This report responds to your request that we update this information. Specifically, our objectives were to (1) determine the current status of smart card projects under way at the time of our last review, (2) identify and determine the status of projects initiated since our last review was completed, and (3) identify integrated agencywide smart card projects that are currently under way.

To address these objectives, we surveyed the 24 major federal agencies (i.e., agencies covered by the Chief Financial Officers Act as well as the Department of Homeland Security (DHS)) regarding the status of their smart card projects. We also obtained supporting documentation where available and conducted follow-up interviews with agency officials responding to the survey to ensure that the information provided was current and accurate. In addition, we contacted GSA officials to discuss agencies' use of the Smart Card Access Common ID contract and other governmentwide implementation issues. Further details of our objectives, scope, and methodology are given in appendix I.

We performed our work between November 2003 and July 2004, in accordance with generally accepted government auditing standards.

Results in Brief

Of the 52 smart card projects that we reported as ongoing in January 2003, 28 had been discontinued as of June 2004 because they were absorbed into other smart card projects or were deemed no longer feasible. Of the remaining 24 projects, 16 are in planning, pilot, or operational phases and are intended to support a variety of uses (the agencies did not provide current information on the remaining 8). Twelve of the 16 projects are large-scale projects intended to provide identity credentials to an entire agency's employees or other large group of individuals. Examples include the Department of Defense's (DOD) Common Access Card (CAC), which is to be issued to an estimated 3.5 million DOD-related personnel, and the Transportation Security Administration's Transportation Worker Identification Credential, which is to be used by an estimated 6 million transportation industry workers. The other 4 projects are smaller in scale, intended to provide access or other services to limited groups of people.

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

For example, the Department of Commerce's Geophysical Fluid Dynamics Laboratory access card will be issued to about 612 employees, contractors, and research collaborators. Further, in response to our survey, agencies reported 8 additional smart card projects that were ongoing at the time of our last review but not reported at that time.

Based on our survey of federal agencies, 10 additional smart card projects have been initiated since our last review was completed. These projects vary widely in size and scope. Included are small-scale projects, involving cards issued to as few as 126 cardholders (such as a project in the Department of Labor's Employment and Training Administration), and large-scale agencywide initiatives, such as the Department of Veterans Affairs (VA) Authentication and Authorization Infrastructure card, which is to be issued to an estimated 500,000 employees and contractors. Four of these agencies reported purchases under GSA's Smart Card Access Common ID contracting vehicle, and others likewise have plans to use this contract. Specifically, five agencies—including the Departments of Defense, Homeland Security, the Interior, and Veterans Affairs, and the National Aeronautics and Space Administration (NASA)—are planning to make an aggregated purchase of up to 40 million cards over the next 4 years using the GSA contract.

Nine agencies are developing and implementing integrated agencywide smart card initiatives. These projects are intended to use one card to support multiple functions, such as providing identification credentials, accessing computer systems, and storing monetary values.

We received oral comments on a draft of this report from GSA's Associate Administrator, Office of Governmentwide Policy, and from officials of the Office of Management and Budget's (OMB) Office of Information and Regulatory Affairs and its Office of General Counsel. Both GSA and OMB generally agreed with the content in the draft report. Technical comments provided by GSA and OMB have been addressed as appropriate.

Background

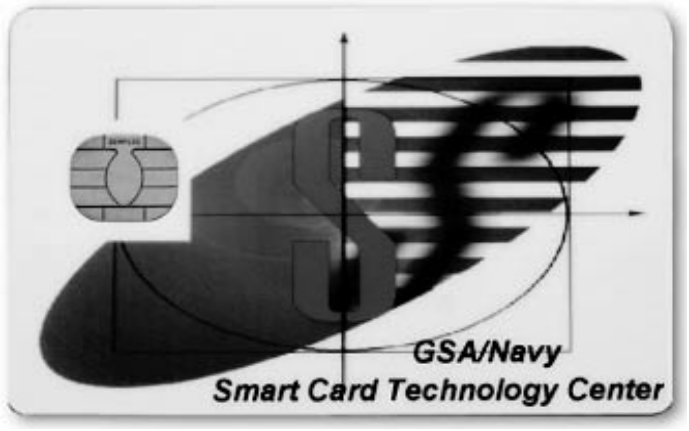
Today, federal employees are issued a wide variety of identification (ID) cards, which are used to access federal buildings and facilities, sometimes solely on the basis of visual inspection by security personnel. These cards often cannot be used for other important identification purposes—such as gaining 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. One means to address such problems is offered by the use of smart cards.

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.[4] 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 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.

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

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.[5]

Smart cards can also be used in conjunction with public key infrastructure (PKI) technology to better secure electronic messages and transactions.[6] A properly implemented and maintained PKI can offer several important security services, including assurance that (1) the parties to an electronic transaction are really who they claim to be, (2) the information has not been altered or shared with any unauthorized entity, and (3) neither party will be able to wrongfully deny taking part in the transaction. Security experts generally agree that PKI technology is most effective when deployed in conjunction with smart cards.

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 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.

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 the 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

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

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

interfaces are needed because standards for the technologies are very different.

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. To make it easier for federal agencies to acquire commercial smart card products, GSA developed the governmentwide Smart Card Access Common ID contracting vehicle, which also specified adherence to the government smart card interoperability specification that NIST developed in collaboration with smart card vendors.

In 2003, OMB, in accordance with the President's vision of creating a more responsive and cost-effective government, issued a memorandum to federal chief information officers outlining details of the E-Authentication E-Government initiative on authentication and identity management. OMB also created the Federal Identity Credentialing Committee (FICC) to make policy recommendations and develop the Federal Identity Credentialing component of the Federal Enterprise Architecture, to include services such as identity proofing and credential management for the federal government. In February 2004, FICC issued policy guidance on the use of smart card–based systems in badge, identification, and credentialing systems with the objective of helping agencies plan, budget, establish, and implement credentialing and identification systems for government employees and their agents.

In our January 2003 report on smart cards, we made recommendations to OMB, NIST, and GSA. Specifically, we recommended that

- the Director, OMB, issue governmentwide policy guidance regarding adoption of smart cards for secure access to physical and logical assets;

- the Director, NIST, continue to improve and update the government smart card interoperability specification by addressing governmentwide standards for additional technologies—such as contactless cards, biometrics, and optical stripe media—as well as integration with PKI; and

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

To date, all three agencies have taken actions to address the recommendations made to them. In response to our recommendation, OMB issued a July 3, 2003, memorandum to major departments and agencies directing them to coordinate and consolidate investments related to authentication and identity management, including the implementation of smart card technology. NIST has responded by improving and updating the government smart card interoperability specification to address additional technologies, including contactless cards and biometrics.[7] GSA responded to our recommendations by updating its "Smart Card Policy and Administrative Guidance" to better address security priorities, including minimum security standards for federal facilities, computer systems, and data across the government. However, three of our four recommendations to GSA are still outstanding. GSA officials stated that they are working to address the recommendations to develop an internal GSA smart card implementation strategy, develop a process for conducting evaluations of smart card implementations, and share lessons learned and best practices across government. The responsibility for one recommendation—establishing guidelines for federal building security that address the role of smart card technology—was transferred to DHS.

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

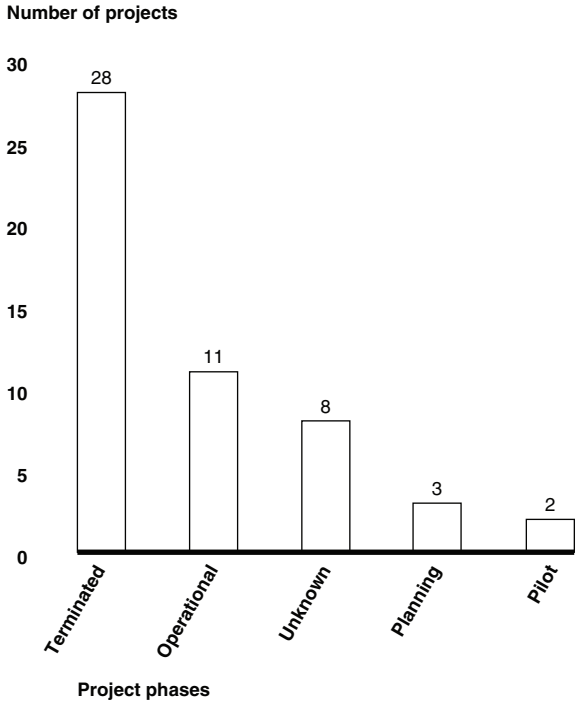
Status of Previously Ongoing Smart Card Efforts

In January 2003, we reported that 18 federal agencies were planning, testing, operating, or completing 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 in varying stages of deployment. Specifically, 17 projects were listed as operational, 13 projects were in the planning stage, and 7 were being piloted. In addition, 10 were reported at that time as having been completed[8] or discontinued for various reasons. No information was provided about the project phase of the remaining 15 initiatives.

In responding to our survey regarding the 52 projects listed as ongoing in our previous report, agencies reported that as of June 2004, 28 had been terminated. Of the remaining projects, 11 were operational, 5 were in the planning or pilot phase, and agencies did not provide current information on 8. The operational and planned projects consist mostly of large-scale projects intended to provide identity credentials to an entire agency's employees or other large groups of individuals. Figure 2 shows the current status of the 52 federal smart card projects that were previously reported as continuing. Table 1 provides summary information on the status of individual projects, providing reasons for any terminations.

[8]"Completed" projects involved applications that were never intended to be permanent, such as smart cards to be used at the 2001 Presidential transition.

Figure 2: Distribution by Project Phase of 52 Federal Projects Previously Reported as Ongoing



Source: GAO.

Table 1: Summary Information on 52 Projects Reported as Ongoing as of January 2003

Federal agency	Number of projects	Previously reported status	Current status	Comments
Agriculture	1	1 operational	1 terminated	The Farm Service Agency terminated the Peanut Smart Card project after the 2002 Farm Bill ended the Peanut Program.
Commerce	5	1 planned	1 terminated	NIST terminated its Network Security and Access Control project after determining that the technology did not meet its needs and that the project was too costly.
		1 pilot	1 terminated	The Patent and Trademark Office terminated its Patent Work at Home program because of legal and union issues.
		3 of unknown status [a]	1 unknown	Commerce did not provide current information on the previously reported Bureau of Industry & Security project.
			2 operational	The U.S. Census Bureau Travel Management Information System and the National Oceanic and Atmospheric Administration Geophysical Fluid Dynamics Laboratory Remote Access projects are now fully operational.
Defense	20	1 planned	1 terminated	The Naval Academy Campus pilot did not advance past the discussion stage. No funding was provided to support implementation.
		3 pilot	3 terminated	Of the 3 pilot projects, the Common Access Card (CAC) absorbed 2, and 1 was terminated because the project achieved its objectives in the pilot phase.
		10 operational	2 operational	The CAC and Eagle Cash card continue as operational programs.
		6 of unknown status [a]	14 terminated	Of 14 terminated projects, 5 were absorbed by CAC, 3 were absorbed by EZPay (a previously unreported project), 1 was terminated because it did not receive funding for a planned upgrade, and 2 were terminated because there was no funding or sustainment support available for implementation. The last 3 were reported to be CAC applications rather than separate smart card programs.
DHS	1	1 planned	1 pilot	The Transportation Worker Identification Credential program was transferred from the Department of Transportation to DHS as part of the Transportation Security Administration.
Education	1	1 planned	1 terminated	The Financial Student Aid Campus card project was terminated because it was incompatible with an existing proximity card system installed in Education's headquarters buildings.
Energy	1	1 operational	1 unknown	A project was previously reported on the use of smart cards to permit physical access to restricted areas by employees working to clean up and shut down the Rocky Flats Technology site. However, Energy officials did not provide current information about this project.
General Services Administration	1	1 operational	1 terminated	GSA's smart card for physical and logical access was terminated and replaced by GSA's new nationwide ID effort.
Housing and Urban Development	1	1 pilot	1 unknown	Department officials did not provide current information about this previously reported pilot project.

(Continued From Previous Page)

Federal agency	Number of projects	Previously reported status	Current status	Comments
Interior	4	1 planned	1 operational	The Incident Qualification and Certification System (previously reported as the Firefighters Training Card) is now operational.
		2 pilot	1 operational	The Bureau of Land Management previously piloted the E-Authentication project. This initiative is now operational but not fully deployed.
			1 planning	The Minerals Management Service is planning a smart card project to provide credentials for physical and logical access.
		1 of unknown status [a]	1 unknown	No current information was provided for a project that was previously reported at the Fish and Wildlife Service.
Justice	5	2 planned	1 pilot/testing 1 unknown [b]	The FBI is piloting the PKI portion of itsTrilogy program, to provide logical access. This program is a 36-month effort to enhance effectiveness through technologies that facilitate better organization, access, and analysis of information. Department officials did not provide current information about the other previously reported project.
		3 of unknown status [a]	3 unknown	Justice did not provide current information on these previously reported projects.
Labor	1	1 operational	1 operational	The Bureau of Labor Statistics is operating the Internal PKI Infrastructure project to provide logical access to computer systems.
NASA	1	1 planned	1 planning/ testing	NASA is testing a project to use PKI certificates to authenticate and grant employees and contractors physical and logical access at its facilities.
National Science Foundation	1	1 planned	1 terminated	The planned project was terminated for lack of funding.
Social Security Administration	1	1 planned	1 terminated	The planned Property Accountability and Pass Project did not proceed beyond the concept stage.
State	1	1 operational	1 operational	State employees use smart cards, which include PKI certificates, for physical and logical access.
Transportation	2	2 planned	1 operational	The Volpe Security Upgrade Project provides physical access for employees and contractors.
			1 planning	The Federal Aviation Administration Identification Media System project is in the planning phase.
Treasury	2	1 planned	1 operational	The Electronic Treasury Enterprise Card is now operational.
		1 operational	1 operational	The Internal Revenue Service is using smart cards to provide secure dial-in access to its local area network.
Veterans Affairs	3	1 operational	1 terminated	VA terminated the One VA Express registration project because registration data could be obtained using existing network-centric enterprise information systems.
		2 of unknown status [a]	2 terminated	The VA Bronx and VA Tampa Stored Value/ID projects were terminated because of low volumes of activity, as well as operational and technical challenges.

Source: GAO analysis of data reported by federal agencies.

[a]Deployment status information was not provided.

Agencies reported that the majority (28) of the above projects had been terminated since our last review was conducted. According to agency officials, reasons for termination were primarily that the projects were absorbed into other smart card projects or were deemed no longer feasible. For example, DOD terminated 14 of 26 previously reported projects by substituting functionality provided by two large-scale smart card projects, the Common Access Card (CAC) and the EZPay (a project that was not previously reported). DOD's CAC card is to be used to authenticate the identity of nearly 3.5 million military and civilian personnel and to improve security over online systems and transactions. The EZPay program is a stored-value card given to recruits at training installations to accelerate the processing time and thus maximize training time.

Table 2 provides further details on the remaining 16 ongoing projects. As the table shows, 12 of these are large-scale projects. Agencywide smart card projects are ongoing at NASA and the Departments of Defense, the Interior, State, and the Treasury.

These and other large projects will serve populations ranging up to 6 million. The cards will be used for identity credentials, physical access to buildings, logical access to computer systems, and stored value. The remaining 4 projects are used for similar purposes. However, they are smaller in scale, serving populations ranging from 612 to 3,100 individuals. For example, the Interior's Minerals Management Service is planning a smart card program for use as identity credentials, and physical and logical access for about 2,100 employees.

Table 2: Detailed Status of 16 Previously Reported Projects That Remain Active as of June 2004

Federal agency	Number of projects	Status	Size[a]	Number of cards issued[b]	Population to be served	Description
Commerce	2	1 operational	Large	5,313	As needed	The U.S. Census Bureau's Travel Management Information System Plus is an administrative travel application that provides users with the capability to process transactions using electronic technology.
		1 operational	Small	204	612	National Oceanic and Atmospheric Administration's Geophysical Fluid Dynamics Laboratory has remote access cards to facilitate login to computer systems.
Defense	2	1 operational	Large	2,750,859	3,457,975	The CAC is an agencywide standard identification card for DOD. This is the principal card used to enable physical access to buildings, installations, and controlled spaces; it will also be used to enable information technology systems and applications that access the department's computer networks.
		1 operational	Large	46,105	15,000 per year	The Department of the Army's EagleCash card is a stored-value card that replaces U.S. currency, minimizes counterfeiting, and improves financial controls and administration at deployed overseas military bases.
DHS	1	1 pilot	Large	0	6 million	The Transportation Security Administration's Transportation Worker Identification Credential (TWIC)[c] is to be issued to each worker requiring unescorted physical or logical access to secure areas of the nation's transportation facilities (including maritime, aviation, transit, rail, and other surface modes).
Interior	3	1 planning	Small	0	2,100	The Minerals Management Service is planning a program to provide smart cards for identity credentials and for physical and logical access.
		1 operational	Large	0	70,000	The Incident Qualification and Certification System (IQCS)—previously reported as the Firefighters Training Card—is an interagency application within the fire management community, including the National Park Service, Bureau of Land Management, Fish and Wildlife Service, Bureau of Indian Affairs, and the U.S. Forest Service. IQCS cards will be used during incidents (such as wildland fires) for identification, basic personal information used to track personnel on the incident, and individual qualifications. The Bureau of Land Management is the managing partner for this project.

(Continued From Previous Page)

Federal agency	Number of projects	Status	Size[a]	Number of cards issued[b]	Population to be served	Description
		1 operational	Large	7,100	90,000	The Bureau of Land Management is the lead agency for the agencywide E-Authentication project, which is intended to provide identification, physical, and logical access for Interior employees. Interior plans to implement this project agencywide by fiscal year 2005.
Justice	1	1 pilot	Large	31	50,000	The FBI is piloting the PKI portion of its Trilogy Program, for logical access.
Labor	1	1 operational	Small	768	3,100	The Bureau of Labor Statistics has partially implemented an Internal PKI Infrastructure project for accessing computer systems.
NASA	1	1 planning/ testing	Large	0	85,000	The One NASA Smart Card Badge Project is agencywide and is being designed to provide cards for identity, physical access, and login to computer systems.
State	1	1 operational	Large	25,000	25,000	The Domestic Smart Card Access Control project is a joint effort with the department's PKI effort. This project is agencywide and is responsible for badge creation and physical access tokens.
Transportation	2	1 operational	Small	1,200	1,200	The Volpe Security Upgrade Project is partially operational and developed for physical access. Smart cards are issued to federal employees and contractors.
		1 planning	Large	0	98,853	The Federal Aviation Administration Identification Media System project is planned to provide cards for identity credentials and for physical and logical access. The Federal Aviation Administration plans to issue the cards to both federal employees and contractors.
Treasury	2	1 operational	Large	2,500	7,500	The Electronic Treasury Enterprise Card is currently in proof of concept operation at the Treasury Headquarters and the Bureau of Engraving and Printing. Agencywide deployment is planned to occur pending funding approval.
		1 operational	Large	30,528	75,000	The Internal Revenue Service is operating agencywide Secure Dial In cards for logical access.

Source: GAO analysis of data reported by federal agencies.

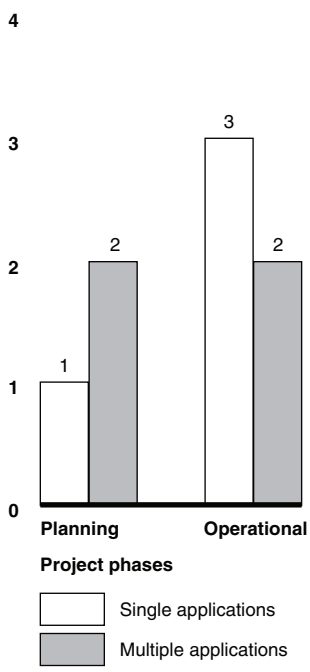
[a]Categorized by the population served. Small projects have issued fewer than 5,000 cards. Large-scale projects had 5,000 or more cards issued.

[b]In our survey, we asked agencies to report the number of cards issued as of December 31, 2003.

[c]At the time of our previous report, the TWIC was listed as a Department of Transportation project.

In response to our survey, agency officials reported 8 additional smart card projects that were ongoing at the time of our last review but not previously reported.[9] Four of the 8 projects were planned for multiple applications such as identity credentials and physical and logical access. The remaining 4 projects were planned for single applications such as stored value, logical access to computer systems and networks, or processing travel documents. Figure 3 shows the number of these projects by the type of applications planned and the stage of reported deployment. Table 3 provides more detailed status information on these projects.

Figure 3: Deployment Phases for 8 Projects That Were Not Previously Reported



Source: GAO.

[9]The information in our previous report was based primarily on data collected by OMB and GSA. In contrast, for the current review, we conducted an independent survey of 24 major federal departments and agencies.

Table 3: Status of 8 Ongoing Smart Card Projects That Were Not Previously Reported

Federal agency	Number of projects	Status	Cards issued [a]	Population to be served	Project description
Defense	2	1 operational	16,724	350,000	The Navy Cash System is a joint Treasury/Navy program and manages personal funds for Navy and Marine Corps deployed members. It is a "cashless" ATM system on Navy ships that allows members access to home banks or credit unions when deployed. The application supported is stored value.
		1 operational	578,197	300,000 per year	The EZPay program provides cards at all U.S. Army and Air Force basic training installations to accelerate recruit processing and maximize training time. This initiative is a partnership involving the Defense Finance and Accounting Service, the Treasury, and the Army. The application supported is stored value.
Environmental Protection Agency (EPA)	1	1 planning	0	1,820	The Region 2 EPA Access Card is an identity credential and physical access card initiative. The project is integrated with GSA's smart card project at the New York Federal Civic Center.
Health and Human Services	2	1 operational	18	2,950	The Food and Drug Administration's Office of Regulatory Affairs is implementing a Trust Service and Identity Management with Level 4 Assurance Project to provide identity credentials for physical and logical access. The purpose of this project is to establish a trust framework that can be combined with infrastructure security services to provide confidentiality, integrity, authentication through digital signatures, and nonrepudiation of electronic transactions.
		1 operational	133	150	The Centers for Disease Control and Prevention is implementing a September Compliance Project that uses smart cards. Planning for this identity credential and physical access application began in April 2002.
DHS	1	1 planned	0	Not provided	DHS has established the United States Visitor and Immigrant Status Indicator Technology (US VISIT) project to collect, maintain, and share information, including biometric identifiers, on selected foreign nationals who travel to the United States. The smart-card phase of the US-VISIT project is currently in planning.
Social Security Administration	1	1 operational	15,490	As needed	The Virtual Private Network Smart Card became fully operational in November 2000. The purpose of this smart card is to provide remote access to designated computer network users. The agency intends to purchase additional cards as needed.
Transportation	1	1 planning	1	Not provided	The National Highway Traffic Safety Administration Smart Card Project is in the planning phase. The purpose is to provide identity credentials, physical and logical access, and asset management applications. Additional cards are to be issued when the project becomes operational.

Source: GAO analysis of data reported by federal agencies.

[a]As of December 31, 2003.

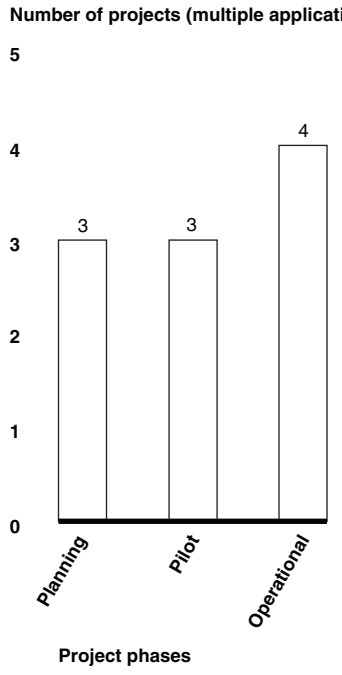
Agencies across the Government Continue to Invest in Smart Card Projects

In response to our survey, agencies reported 10 smart card projects that were initiated since our last review was completed. Based on these reported projects, more agencies are using GSA's Smart Card Access Common ID contracting vehicle to acquire smart card technology.

Federal Investments in Smart Card Projects

The 10 new projects identified in response to our survey vary in size, scope, and stage of deployment: planning, pilot, and operational. All of the projects are planned for multiple applications such as identity credentials and physical and logical access. Figure 4 shows the number of these projects by the type of application planned and the stage of reported deployment.

Figure 4: Deployment Phases for 10 Recently Initiated Projects



Source: GAO.

These 10 projects vary widely in size, including small-scale projects—involving smart cards issued to as few as 126 cardholders—as well as much larger scale initiatives. For example, Department of Labor officials reported that the Employment and Training Administration physical access control smart card was issued to 126 federal employees and contractors as of December 2003. This card is operational and will be issued to 175 cardholders when fully deployed; it is used for identity credentials and physical access to buildings and other facilities. In contrast, VA plans to issue an estimated 500,000 smart cards to employees and contractors under its Authentication and Authorization Infrastructure Project. Through this initiative, smart cards will be used for identity credentials, accessing buildings or other facilities, and accessing computer systems. Production began in July 2004.

Another example of a large-scale project is GSA's Nationwide ID card. GSA plans to issue cards to 61,000 federal employees, contractors, and tenant agencies. Using this card, GSA plans to implement nationwide uniform credentials based on smart card technology by providing a single standard credential card for identification, building access, property management, and other applications. Table 4 provides status information on the 10 recently initiated smart card projects.

Table 4: Status of 10 Recently Initiated Smart Card Projects

Federal agency	Number of projects	Status	Cards issued [a]	Population to be served	Project description
Commerce	1	1 planning	2,626	10,700	The U.S. Patent and Trademark Office has established an Internal PKI/Smart Card Project. Applications supported are identity credentials and physical and logical access.
General Services Administration	1	1 operational	40,000	61,000	GSA is implementing nationwide uniform credentials based on smart card technology, so that every GSA associate, contractor, and visitor will be able to use a single standard credential card for identification, building access, property management, and other applications.
Health and Human Services	1	1 operational	30	100	The Food and Drug Administration is implementing Select Agent Labs that will be equipped with biometric readers that will use smart cards. The planning phase began in October 2003. Applications supported are identity credentials and physical access.

(Continued From Previous Page)

Federal agency	Number of projects	Status	Cards issued [a]	Population to be served	Project description
DHS	3	1 pilot	0	Not provided	The Transportation Security Administration's Registered Traveler Program is intended to improve the security screening process at airports by identifying approved travelers that will be allowed to go through expedited security screening.
		1 planning	0	Not provided	The Transportation Security Administration's Armed Law Enforcement Officer verification smart card program will test the use of biometric technology to verify the identity of armed law enforcement officers boarding commercial airplanes. Project applications planned are identity credentials and physical access.
		1 pilot	600	250,000	The DHS Identification and Credentialing Program is intended to serve as a comprehensive identification and credentialing program for the entire department when it is fully deployed. Applications supported include identity credentials, physical and logical access, asset management, and stored value.
Labor	2	1 planning	0	900	The E-Authentication Smart Card pilot began in February 2004. The goal is to provide credentials that employees can use to electronically access departmental resources in a manner that is compatible with the federal government's E-Authentication Gateway. Applications supported are identity credentials and physical and logical access. Full implementation across the department is planned for fiscal year 2007.
		1 operational	126	175	The Office of Technology Physical Access Control project addresses the Employment and Training Administration's security requirements for access control to its facilities and sensitive areas. Applications supported are identity credentials and physical access.
State	1	1 operational	0	72,000	The Global Look ID project, a joint effort with the State Department's Domestic Smart Card Access Control project, is designed to support badge creation. Applications supported are identity credentials, physical and logical access, e-mail, and Web-based access controls.
Veterans Affairs	1	1 pilot	250	500,000	The Authentication and Authorization Infrastructure Project is intended to provide the capability to authenticate users and systems with certainty and grant them access to information systems necessary to perform business functions.

Source: GAO analysis of data reported by federal agencies.

[a]As of December 31, 2003.

Agencies' Reported Use of GSA's Contracting Vehicle

GSA developed the Smart Card Access Common ID contracting vehicle to help make it easier for federal agencies to acquire commercial smart card products and services. According to the director of GSA's Center for Smart Card Solutions, further guidance is planned that will require agencies to

use the contracting vehicle or provide justification for not using it. The Director also stated that using GSA's contract should help reduce the cost of smart cards and ensure that vendors incorporate interoperability specifications. Between December 2004 and December 2008, five agencies—including NASA and the Departments of Defense, Homeland Security, the Interior, and Veterans Affairs—are planning to make an aggregated purchase of up to 40 million cards through the GSA contract. As a part of this purchase, these agencies are scheduled to begin making quarterly procurements beginning in December 2004 of approximately 1.2 million cards.

In response to our survey, the majority of the agencies (4 of 7) that reported new initiatives told us that they purchased smart cards under the GSA contract. The remaining agencies cited reasons for not acquiring smart cards under the GSA contract, such as purchase arrangements with another agency or purchases under other types of contracts.

Implementation of Agencywide Smart Card Initiatives

Agencies continue to move towards integrated agencywide initiatives that use smart cards as identity credentials that agency employees can use to gain both physical access to facilities, such as buildings, and logical access to computer systems and networks. In some cases, additional functions, such as asset management and stored value, are also being included. Nine agencies reported such projects: 4 of these were reported in our prior report, and 5 are recently initiated efforts. These projects are in various stages of deployment.

One of the largest agencywide efforts is DHS's identification and credentialing project. The agency plans to issue 250,000 cards to employees and contractors. This is a comprehensive identification and credentialing effort that will use PKI technology for logical access and proximity chips for physical access. Authentication will rely on biometrics with a personal identification number as a backup. Other recently initiated agencywide smart card projects include GSA's Nationwide Identification, VA's Authentication and Authorization Infrastructure Project, and the Department of Labor's E-Authentication project. Table 5 summarizes both previously reported and recently initiated agencywide smart card efforts.

Table 5: Agencywide Smart Card Projects

Federal agency	Project name	Reported status	Estimated completion	Applications supported
Defense	Common Access Card (CAC)	Operational	Apr. 2004	Identity credential Physical access Logical access
Homeland Security	Identification and Credentialing Program	Pilot	—	Identity credential Physical access Logical access Asset management Stored Value
General Services Administration	Nationwide Identification	Operational	Dec. 2004	Identity credential Physical access
Interior	E-Authentication	Operational	Jan. 2006	Identity credential Physical access Logical access E-signature
Labor	E-Authentication	Planning	Apr. 2005	Identity credential Physical access Logical access
NASA	One NASA Smart Card Badge	Planning/pilot	Sept. 2004	Identity credential Physical access Logical access
State	Global Look ID	Operational	Sept. 2006	Identity credential Physical access Logical access E-mail (signature & encryption)
Treasury	Electronic Treasury Enterprise Card	Operational	Sept. 2004	Identity credential Physical access Logical access Asset management
Veterans Affairs	Authentication and Authorization Infrastructure Project	Pilot	Sept. 2007	Identity credential Physical access Logical access

Source: GAO analysis of data reported by federal agencies.

Summary

Agencies across the government continue to invest in smart card projects with plans to issue millions of new cards to employees and other personnel. These projects are intended to provide a range of benefits and services, ranging from verifying the identity of people accessing buildings and computer systems to managing assets and storing monetary value. Agencies are also moving toward integrated agencywide credentialing

projects, with several agencies planning to consolidate their smart card purchases through GSA's Smart Card Access Common ID contract.

Agency Comments and Our Evaluation

We received oral comments on a draft of this report from GSA's Associate Administrator, Office of Governmentwide Policy, and from officials of OMB's Office of Information and Regulatory Affairs and its Office of General Counsel. Both GSA and OMB generally agreed with the content in the draft report. In addition, each agency provided technical comments, which have been addressed where appropriate in the final report.

We will provide copies of this report to the Director of OMB and the Administrator of GSA, and the report will be available at no charge on the GAO Web site at http://www.gao.gov.

Should you have any questions on matters contained in this report, please contact me at (202) 512-6240 or John de Ferrari, Assistant Director, at (202) 512-6335. We can also be reached by e-mail at koontzl@gao.gov and deferrarij@gao.gov, respectively. Other key contributors to this report were Tonia Brown, Barbara Collier, Felipe Colón, Pamlutricia Greenleaf, and Joel Grossman.

Sincerely yours,

Linda D. Koontz
Director, Information Management Issues

Objectives, Scope, and Methodology

Our objectives were to (1) determine the current status of smart card projects under way at the time of our last review, (2) identify and determine the status of projects initiated since our last review was completed, and (3) identify integrated agencywide smart card projects that are currently under way.

To address these objectives, we developed a questionnaire and surveyed 24 federal agencies. These included agencies that are subject to the provisions of the Chief Financial Officers Act as well as the Department of Homeland Security. The survey included the 18 agencies pursuing smart card projects that were identified in our previous report.

The practical difficulties of conducting any survey may introduce errors. For example, differences in how a particular question is interpreted, the sources of information available to respondents, or the types of people who do not respond can introduce unwanted variability into the survey results. We included steps in both the data collection and data analysis stages for the purpose of minimizing such errors.

We analyzed information obtained through the survey to develop summary results and identify trends. To ensure the reliability of the information reported through the survey, we obtained available supporting documentation—such as project plans and descriptions—to verify (1) reported planning and implementation dates and (2) the numbers of smart cards issued as of December 31, 2003, or planned for issuance. As needed, we conducted follow-up interviews with agency officials responding to the survey to further ensure that the information provided was current and accurate. In addition, we contacted GSA officials to discuss agencies' use of the Smart Card Access Common ID contract and other governmentwide implementation issues.

We performed our work in Washington, D.C., and Atlanta, Georgia, between November 2003 and July 2004, in accordance with generally accepted government auditing standards.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

United States
Government Accountability Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00