

SANDRA N. BATES
COMMISSIONER
FEDERAL TECHNOLOGY SERVICE
U.S. GENERAL SERVICES ADMINISTRATION
BEFORE THE SUBCOMMITTEE ON TECHNOLOGY,
INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS
AND THE CENSUS
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
SEPTEMBER 9, 2003



Mr. Chairman, thank you for inviting us to participate in today's hearing on Advancements in Smart Card and Biometric Technology. The Federal government is making great strides in the use of this technology and the General Services Administration (GSA) continues to take innovative actions to help agencies secure their facilities and information. GSA executive leadership remains committed to the governmentwide smart card initiative. GSA continues to participate in governmentwide committees such as the Interagency Advisory Board, Federal Identity Credentialing Committee, the Interagency Security Committee, Card Tech Secure Tech, Smart Card Project Managers Group and the Smart Card Alliance. I'd like to describe what a smart card is, give a brief history of the smart card program and address the concerns in your letter.

Smart cards are credit card like devices that use integrated circuit chip technology. They contain embedded computer chips that enable them to perform computer functions (store and process data, read, write, and calculate) remotely as well as on line. The unique advantage of smart cards, as opposed to cards with more basic technology, such as laser cards, magnetic strip or bar codes, is that smart cards can interact with other systems and process information rather than simply storing data resulting in higher security and convenience.

Smart cards serve as an interface between people and computer systems and can be used as identity credentials for building and computer access but also for a wide variety of applications such as transit rides, airline tickets, credit and debit cards, medical records, training records, etc. The highly secure machine-readability of the cards offers unique high levels of security not found in the magnetic strip cards, more commonly used as bank and credit cards today. And when machine-read for building access, they offer a very significant increase in positively identifying the claimed identity of individuals. In turn, this has the potential of allowing trusted individuals rapid and secure access.

Smart cards can be used to process and exchange encrypted information. They can be programmed to authenticate the identity of an individual processing the card in a far more rigorous way than is possible with the standard ID card. A smart card's processing power allows it to exchange and update many other kinds of information with a variety of external system which can facilitate applications such as financial transactions or other services that involve electronic record keeping. Smart cards can also be used for various administrative applications such as property management, storage of training records and credentials, and storage of medical information.

Smart cards can be used to significantly enhance the security of an organization's computer systems by tightening controls over user access. In general, a user wishing to log on to a computer system 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 or PINS, which provide only modest security because they can be easily compromised.

Smart cards can store a person's biometric data that is unique to that individual, such as a fingerprint or hand geometry, thus providing a much higher level of security than possible with simpler cards. The ability to authenticate users using biometric data was a primary reason the State Department began a pilot program with GSA several years ago here in Washington, DC. State chose smart cards from GSA because of the cards interoperability features and, most importantly, because of their ability to authenticate identity. This made the cards more secure and not easily duplicated.

In addition to helping control logical and physical access, smart cards can also be used in conjunction with public key infrastructure (PKI) technology to better secure electronic messages and transactions. Smart cards are grouped into two major classes: contact cards and 'contactless' cards. Contact cards have gold-colored contacts that connect when a card is inserted into a smart card reader. Contactless cards contain an embedded antenna and work when the card is

waived within the magnetic field of a card reader. Contactless cards are better suited for environments where quick interaction between the card and reader is required, such as high-volume physical access. Washington, DC's Metro subway system uses contactless smart cards known as SmarTrip to help speed local commuters in and out of its system.

GSA acquired the lead role for promoting the benefits of smart card technology in the Federal government at the request of OMB in 1996. Initially the Agency's mission was to provide other Federal agencies with information about the applicability and benefits of smart card technology, establish an organizational entity within GSA that could direct its efforts toward meeting GSA's new role, and institute forums where Federal agencies could come together to share their ideas and requirements and to gather more information from GSA.

GSA began its new role by putting together a Smart Card Virtual Team directly under the Office of the Administrator for General Services. The team was headed by senior agency officials and was staffed with personnel from within GSA. Its primary task was putting together an implementation plan that would further GSA's new responsibilities in promoting smart card technology governmentwide. The team also worked with other Federal agencies and

industry partners to ensure input from other interested organizations was considered in the process. The team's initial plan identified twelve action items to promote knowledge about smart cards and the benefits of smart card technology within the Federal community.

Key items include: awarding a smart card contract, which would provide a vehicle for Federal agencies to obtain smart card services; opening of a Smart Card Technology Center at GSA's Headquarters in Washington; establishing a Smart Card Project Managers Group, which provided a forum for Federal agencies to come together on smart cards; developing pilot projects for smart cards within GSA, such as the Federal Technology Service (FTS) 1999 pilot that demonstrated a single smart card could have many uses and provide many benefits.

GSA's Smart Card Technology Center opened in 1998 and is still functioning today. Several thousand visitors from the government community have been given demonstrations of key smart card applications such as physical access, biometrics, secure access to the Internet, digital certificates (for conducting secure transactions over the Internet), electronic purse, medical applications, applications used by the military, and contactless and administrative applications.

GSA's Center for Smart Card Solutions, which became part of the GSA's Federal Technology Service in 1999, along with GSA's industry partners can service agencies' needs for smart cards and card readers, applications development, technical and administrative support, interoperability, and completed system integration.

Additionally, GSA's smart card personnel support Federal agencies using their expertise in smart card technology, requirements analysis, pilot projects, and acquisition strategy and writing task orders under GSA's smart card contract. GAO's review of the program indicated that GSA has made a key contribution by making it easier for Federal agencies to acquire useful smart card products by implementing its governmentwide smart card contract with its interoperability specifications developed jointly with National Institute of Standards and Technology (NIST).

GSA's Smart Card Project Managers Group currently includes representatives from approximately 50 agencies and it continues to meet regularly. The group covers all of the major issues and programs in smart cards. With regard to smart card programs for GSA itself, the agency has initiated several smart card programs within its main headquarters in Washington and also in its regional offices. Currently, all GSA associates in the Washington, DC area have smart

card IDs and there is a program currently underway in GSA that will provide all GSA associates nationwide with smart cards. One of the earliest and largest of these projects is in GSA's Regional Headquarters in New York. The regional office is currently implementing smart cards at three locations in New York City for physical access. Smart card systems will be placed in 26 Federal Plaza, 290 Broadway and in the Region's parking garage at 209 Center Street. GSA's Regional Office will be using a contact/contactless smart card. The card will also include a biometric (thumb print). Cards are currently being issued to all Federal employees and contractors in the Region. Employees will be able to use the cards to gain access to the building through optical portals and to gain secure access to the parking garage. GSA associates will have the ability to use the contactless function of the card for access to GSA occupied space. Once the initial physical access program is completed, the GSA Regional Office will begin the planning process to implement a smart card solution for computer access. Tenant agencies in the building that will be using the smart card for physical access are HUD, EPA, Corp of Engineers, IRS, SSA, FBI, INS, and DHS.

GSA's Smart Card Contract (known as the Smart Card Common Access ID contract) was awarded in May of 2000 to five prime vendors (KPMG, PRC/Litton, EDS, Logicon, and Maximus). (Please note: KPMG is now called BearingPoint, and PRC and Logicon are now part of Northrop Grumman.) Development of the

contract requirements was a joint effort between GSA and agencies such as the Department of Defense (DoD), the State Department, and Treasury. The contract provides worldwide delivery of smart card services to Federal government agencies.

Initial customers, after the contract was awarded by GSA, included DoD offices, the State Department, the Social Security Administration, and the Department of Veterans Affairs. Since the contract was awarded the number of customers and usage of smart cards has continued to expand steadily. Current customers include the National Science Foundation, the DoD's Biometrics Management Office, the Manpower and Personnel Office, and the Common Access Card Office, the Department of the Interior, the Department of Health and Human Services, the Department of State, Department of the Navy's International Programs Office and Naval Facilities Engineering Command, the Department of Transportation's Maritime Administration, the Department of Homeland Security including its Transportation Security Administration (TSA), the National Aeronautics and Space Administration, the United States Patent and Trade Office, and the U.S. General Services Administration.

A major feature of GSA's smart card contract is the establishment of technical specifications for smart card interoperability. The specifications cover four major areas: physical access, logical access, biometrics, and cryptography. The standards represent the first of their kind for smart cards in the Government.

They represent a joint effort by GSA, industry partners, other Federal agencies such as DoD, the Navy, State Department, Treasury, Army, and NIST. A complete version of the current standards can be found on GSA's smart card web site (www.gsa.gov/smartcard).

GSA's Interagency Advisory Board (IAB) was established after publication of the initial version of the Smart Card Interoperability Specifications. The IAB members include Federal employees, including representatives from the NIST, DHS, DoD, State Department, Treasury, and representatives of the prime smart card contract vendors. The IAB was established to refine and update the Interoperability Specifications that are key to GSA's Smart Access Common ID contract. Subcommittees of the IAB were established to address various applications such as biometrics, PKI, E-purse, physical and logical access.

A recent test, of significant interest, successfully proved interoperability of civilian smart cards. The objective of the test was to demonstrate that multi-agency interoperable smart cards could be used in one Federal agency's physical access system to gain access. The test participants were GSA, State Department, and TSA. Members of the aforementioned agencies inserted their Smart Card ID's in the State Department's readers and were granted access to the building.

In regard to biometrics, GSA has been working with other agencies and key non-governmental organizations such as the Biometrics Consortium that is developing worldwide standards. These standards, when issued will be part of the GSA specifications too. In the meantime GSA specifically planned for the utilization of biometrics by including a place holder for it in the smart card contract so that agencies could choose a biometric process which would meet their needs.

The January 2003 GAO report on smart cards, entitled "Electronic Government: Progress in Promoting Adoption of Smart Card Technologies" outlined four major recommendations to the Administrator of General Services. I would like to briefly describe GAO's recommendations and GSA's responses to each.

1. GAO's first recommendation was to develop 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. In response, the Administrator has designated the Commissioner of the Public Buildings Service (PBS) responsible for leading the effort within the agency to develop an internal implementation strategy and to implement a common design for a smart card credentialing system throughout GSA. PBS has completed a common design for the GSA internal smart card credential system that will be implemented in GSA nationwide.

The initial implementation began in GSA's Central Office in Washington DC, GSA's National Capital Region, and in the Northeast and Caribbean Region in New York. Plans are to start issuing the new credential smart cards by the end of fiscal year 2003 and further deployment for all GSA regions will follow the guidelines for Federal building security and Government smart card policies being implemented by the Federal Identity Credentialing Committee that address the role of smart card technology.

2. GAO's second recommendation was to update the governmentwide implementation strategy and update the 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. GSA's response pointed out that the original governmentwide implementation strategy was in response to a specific OMB task effort that was successfully completed several years ago. The policy now calls for agencies to develop their own specific implementation strategies on an agency-by agency basis. GSA plans to update the government administrative guidance on implementing smart card systems as recommended by GAO. GSA's Office of Governmentwide Policy (OGP) has lead responsibility for this action. OGP's original report entitled, "Smart Card Policy and Administrative Guidance," which was first published in October 2000, will be updated by the end of this year.

3. GAO's third recommendation was to establish guidelines for Federal building security that address the role of smart card technology. (This recommendation has been transferred to the Department of Homeland Security.) The Interagency Security Committee (ISC), now chaired by the Department of Homeland Security and supported by the Federal Protective Service, is responsible for Federal building security guidelines. GSA remains an active member of this committee. The ISC's Working Group on Long Term Construction Standards is drafting smart card infrastructure criteria as part of an overall update of the ISC Security Design Criteria. A draft document is due from them this year.

4. GAO's final recommendation to GSA was to develop a process for conducting ongoing evaluation of the implementation of smart card based systems by Federal agencies to ensure that lesson learned and best practices are shared across government. To address this recommendation, GSA has already established the Federal Smart Card Project Managers Group, which since 1996 has met bi-monthly to address Federal agency progress in smart cards and related technology implementation efforts. In these meetings, agencies regularly report on their smart card implementation experience, and make presentations on lessons learned to a wide audience. In addition, the Interagency Advisory Board has served as a source of work groups for various related activities, such as the Physical Access Interoperability Work Group, and the Policy Work Group. However, as the

number of Federal smart card implementation increase, GSA agrees that it is becoming necessary to apply more formal assessment methodology to the implementation. GSA's Office of Governmentwide Policy has lead responsibility for this action and is collaborating closely with GSA's Interagency Advisory Board to document guidance for conducting and communicating ongoing evaluations and lessons learned from agency smart card deployments on a continuing basis.

The Federal Identity Credentialing Committee, of which GSA is leading, will define the policies for issuance and management of identity credentials for Federal personnel, contractors and other authorized users that encompass both physical access to buildings and logical access to systems. By implementing standardized credentials across the Federal government, individual access control can be streamlined across multiple organizations and systems. Government cost savings can be achieved through standardization, shared services, and consolidated purchasing. Cryptographic smart cards represent the technology that best meets governmentwide needs for physical credentials while also serving as secure platforms for electronic credentials in accordance with standards and guidelines. As stated in the Administrator for E-Government and Information Technology at OMB, July 3, 2003 memo, "The Federal government is spending in excess of \$160M in FY03 and FY04 on potentially inconsistent or agency-unique authentication and identity management infrastructure. Agencies

also have inconsistent approaches to both physical security and computer security, which lead to increased risks to the Federal government and the people with whom it interacts. Finally, there is a burden on the public in interacting with the government by having to maintain multiple credentials and not being able to access the services they need using those credentials. It is clear that a cross-agency approach for authentication and identity management is a better alternative.”

At the August 2003 IAB meeting, it was decided to begin developing several models of smart card requirements that can be used to make a consolidated purchase for interested government agencies. This will be done in coordination with the Federal Identity Credentialing Committee. This will leverage the government’s buying power to make smart card purchases more cost effective.

In conclusion Mr. Chairman, I am pleased to say that GSA has been instrumental in the development of the Federal Government’s Smart Card program and in its use of biometric technology. Thank you again for this opportunity to appear before this Committee today and I’ll be happy to answer any questions you or the Committee members may have.