ADVANCEMENTS IN SMART CARD AND BIOMETRIC TECHNOLOGY

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 9, 2003

Serial No. 108–133

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

93–034 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
LORI MARTIN, *Professional Staff Member*
URSULA WOJCIECHOWSKI, *Clerk*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

ADVANCEMENTS IN SMART CARD AND BIOMETRIC TECHNOLOGY

TUESDAY, SEPTEMBER 9, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., in room 2154, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) presiding.

Present: Representative Putnam.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Lori Martin, professional staff member; Ursula Wojciechowski, clerk; Suzanne Lightman, fellow; Karen Lightfoot, minority communications director/sr. policy advisor; David McMillen, minority professional staff member; Cecelia Morton, minority office manager; and Anna Laitin, minority assistant communications.

Mr. PUTNAM. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Good morning and welcome, everyone, to today's hearing entitled, "Advancements in Smart Card and Biometric Technology." I hope everyone had a nice August work period and enjoyed a little bit of the break with Congress being out of everybody's hair and back home telling the good people, the good constituents what we've done to them or for them, whichever the case may be.

This is the first hearing of a very ambitious fall schedule for this subcommittee. As you may have noticed from our postings, we will have two hearings this week, three hearings the next week on cybersecurity and related matters. So we have a very aggressive schedule in keeping with the pace that we have set throughout the year, and we certainly appreciate the support that GAO and the other executive agencies have provided this subcommittee in allowing us to prepare for that ambitious a schedule.

Securing government buildings and computer systems is a task which has grown in both importance and challenge over the past number of years. Recognizing this, Federal agencies working with the GSA have begun testing advanced identification technology that will better authenticate the identity of those requiring access to and interaction with the Federal Government.

Specifically, agencies are examining the use of smart cards which offer a number of benefits to Federal agencies including identity authentication of cardholders, increased security over buildings,

safeguarding computers and data and conducting financial and nonfinancial transactions more accurately and efficiently. In fact, some agencies, such as the Department of Defense, have already issued smart cards. The DOD's Common Access Card [CAC], enables physical access to buildings, installations and controlled spaces. It also permits access into DOD's computer networks. The CAC provides the Department of Defense the information, security and assurance necessary to protect vital information resources.

A number of other agencies across the Federal Government are still exploring the possibilities of smart card use; and while some progress has been made, a recent report released by GAO outlines some areas of concern that need to be addressed in order for agencies to move forward in implementing the use of smart cards. As is too often the case, agencies have been unable to sustain an executive-level commitment to this project, according to the GAO. If these types of initiatives fail to be a priority with the leadership of the agency, it is difficult to imagine that adequate resources will be allocated for their implementation.

Some additional noted challenges to progress include: recognizing and understanding resource requirements, integrating physical and IT security practices, focusing on achieving interoperability among smart card systems, maintaining the ongoing security of smart card systems and protecting the privacy of personal information. These are just a few of the issues agencies will need to address as they move forward.

There are other advanced and emerging technologies that have the potential to offer additional assurance to the identity authentication process. Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometry is being explored, developed and even utilized by agencies today, including the FBI, at our borders and by State governments in detecting fraud and abuse of government benefits through identity verification.

Biometric authentication may also be used with smart card technology. Some smart cards have the capability of holding a biometric identifier, such as a fingerprint. This holds the potential to increase the accuracy of the identity authentication process. These possibilities as well as the limitations and challenges presented by this technology should be explored further.

As agencies proceed to explore the use of these advanced identity authentication technologies, government cannot neglect the importance people and process will continue to play in providing a secure environment. Regardless of how well these technologies work on behalf of the Federal Government in authentication and identity management, technology has its limitations. Without the people and process in place to make it work, we will have wasted a lot of money as well as provided a false sense of security.

I'm hopeful that as the Office of Management and Budget working with the GSA and the National Institute of Standards and Technology go forward in setting some guidance for agencies concrete progress in the actual implementation of smart card technology across agencies will be demonstrated in the very near future.

As is always the case with this subcommittee, today's hearing can be viewed live via Web cast by going to reform.House.gov and clicking on the link under live committee broadcast.

[The prepared statement of Hon. Adam H. Putnam follows:]

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

CONGRESSMAN ADAM PUTNAM, CHAIRMAN

OVERSIGHT HEARING
STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic: *"Advancements in Smart Card and Biometric Technology."*

Tuesday, September 9, 2003
10:00 a.m.
Room 2154 Rayburn House Office Building

OPENING STATEMENT

Securing government buildings and computer systems is a task which has grown in both importance and challenge over the past number of years. Recognizing this, Federal agencies, working with the General Services Administration, have begun testing advanced identification technology that will better authenticate the identity of those requiring access to and interaction with the Federal government.

Specifically, agencies are examining the use of smart cards, which offer a number of benefits to Federal agencies including identity authentication of cardholders, increased security over buildings, safeguarding computers and data, and conducting financial and non-financial transactions more accurately and efficiently. In fact, some agencies, such as the Department of Defense, have already issued smart cards. The DoD's Common Access Card, CAC, enables physical access to buildings, installations, and controlled spaces. It also permits access into DoD's computer networks. The CAC provides DoD the information security and assurance necessary to protect vital information resources.

A number of other agencies across the Federal government are still exploring the possibilities of smart card use. And while some progress has been made, a recent report released by GAO outlines some areas of concern that need to be addressed in order for agencies to move forward in implementing the use of smart cards. As is too often the case, agencies have been unable to sustain an executive level commitment to this project, according to findings by GAO. If these kinds of initiatives fail to be a priority with the leadership of an agency, it is difficult to imagine that adequate resources will be allocated for their implementation.

Some additional noted challenges to progress include: recognizing and understanding resource requirements, integrating physical and IT security practices, focusing on achieving interoperability among smart

card systems, maintaining the ongoing security of smart card systems, and protecting the privacy of personal information. These are just a few of the issues agencies will need to address as they move forward.

There are other advanced and emerging technologies that have the potential to offer additional assurance to the identity authentication process. Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometry is being explored, developed and even utilized by some agencies today, including the FBI, at our borders and by state government's in detecting fraud and abuse of government benefits through identity verification. Biometric authentication may also be used with smart card technology. For instance, some smart cards have the capability of holding a biometric identifier, such as a fingerprint. This holds the potential to increase the accuracy of the identity authentication process. These possibilities, as well as the limitations and challenges presented by this technology, should be explored further.

As agencies proceed to explore the use of these advanced identity authentication technologies, government cannot neglect the importance people and process will continue to play in providing a secure environment. Regardless of how well these technologies work on behalf of the Federal government in authentication and identity management, technology has its limitations. Without the people and process in place to make it work we will have wasted a lot of money as well as provided a false sense of security.

I am hopeful that as the Office of Management and Budget, working with GSA and the National Institute of Standards and Technology go forward in setting some guidance for agencies, concrete progress in the actual implementation of smart card technology across Federal agencies will be demonstrated in the near future.

Mr. PUTNAM. It is a pleasure to have a distinguished panel of witnesses with us this morning; and, as is the custom with this subcommittee, I would ask that the witnesses and any supporting cast members who will be answering questions rise and raise your right hands and be sworn in.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all the witnesses responded in the affirmative.

Our first witness this morning is Mr. Joel Willemssen. Mr. Willemssen is the managing director of Information Technology Issues at the U.S. General Accounting Office. In this position, he has overall responsibility for GAO's evaluations of information technology across the government. Specific responsibilities include governmentwide and agency-specific assessments of computer security and critical infrastructure protection, e-government, information collection, use and dissemination and privacy. Mr. Willemssen is very supportive of the work of this subcommittee, as is the rest of GAO, and we welcome your testimony.

Mr. Willemssen, you're recognized for 5 minutes.

STATEMENT OF JOEL WILLEMSSEN, MANAGING DIRECTOR OF IT MANAGEMENT, GENERAL ACCOUNTING OFFICE

Mr. WILLEMSSEN. Thank you, Mr. Chairman. Thank you for inviting us to testify today on the smart cards; and, as requested, I'll briefly summarize our statement.

The Federal Government is increasingly pursuing the use of smart cards for improving the security of its many physical and information assets. Since 1998, numerous smart card projects have been initiated addressing a wide array of capabilities, including better authentication of the identities of people accessing buildings and improved security of computer systems. The largest smart card program, as you mentioned, currently in operation is Defense's Common Access Card program; in addition to enabling access to specific defense systems, this card is also used to better ensure that electronic messages are accessible only by designated recipients.

Even with the progress made governmentwide to use smart cards, there are several key management and technical challenges that need to be overcome to achieve a card's full potential, and one of them, as you mentioned, is sustaining executive commitment. Without executive commitment, it's very difficult to actually see success in smart card efforts.

A second challenge is obtaining adequate resources for projects that can require extensive modifications to technical infrastructures and software.

Third is that integrating security practices across many agencies can be a major task, because it requires collaboration among those organizations who have responsibility for physical security and those organizations that have responsibility for computer and information security.

A fourth challenge is interoperability across the government to try to reduce the potential number of stovepipe systems that cannot easily communicate with one another.

And, finally, although concerns about security are themselves a key driver for why we want to pursue smart cards, the security of

smart card systems is not foolproof and needs to be closely examined as agencies go forward with implementation.

To help address these challenges, several initiatives have been undertaken to facilitate the adoption of smart cards. For example, GSA has set up a governmentwide standards-based contract. In addition, it's adopted a new agencywide credentialing policy, and it's consolidated its special smart card projects within the public building service.

In July, OMB has also shown that it's begun to take action to develop a governmentwide policy framework for smart cards, specifically, a plan to develop a comprehensive policy for credentialing Federal employees. Second, OMB intends to pursue a governmentwide acquisition of authentication technology, including smart cards to achieve governmentwide cost savings. Third, OMB plans to consolidate agency investments in credentials and related services by selecting shared service providers by the end of 2003.

Even with those important steps of OMB and GSA, there is a lot of work remaining to do in the smart card area. For example, reconciling the varying security requirements of Federal agencies to arrive at a stable design for Federal credentialing is going to take a lot of time; and, further, achieving OMB's vision of streamlined Federal credentialing will be challenging in attempting to reach consistency in how agencies perform identity verification.

Mr. Chairman, that concludes a summary of my statement, and I'd be pleased to address any questions you may have. Thank you.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

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

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

ELECTRONIC GOVERNMENT

Challenges to the Adoption of Smart Card Technology

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

GAO
Accountability · Integrity · Reliability

Highlights

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

Why GAO Did This Study

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

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

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

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

September 2003

ELECTRONIC GOVERNMENT

Challenges to the Adoption of Smart Card Technology

What GAO Found

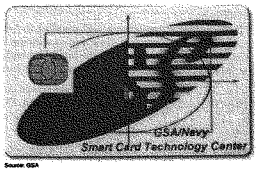
To successfully implement smart card systems, agency managers have faced a number of substantial challenges:

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

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

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

A Typical Smart Card (not to scale)



Source: GSA

Mr. Chairman and Members of the Subcommittee:

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

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

Background

As you know, technology plays an important role in helping the federal government provide security for its many physical and information assets. Today, federal employees are issued a wide variety of identification (ID) cards, which are used to access federal buildings and facilities, sometimes solely on the basis of visual inspection by security personnel. These cards often cannot be used for other important identification purposes—such as gaining access to an agency's computer systems—and many can be easily forged or

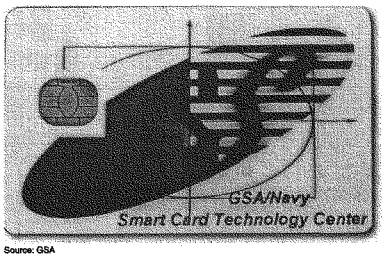
[1] The term "smart card" may also be used to refer to cards with a computer chip that only stores information without providing any processing capability. Such cards, known as stored-value cards, are widely used for services such as prepaid telephone service or satellite television reception. This statement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

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

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.[3]

Smart cards can readily be tailored to meet the varying needs of federal agencies or to accommodate previously installed systems. For example, other media—such as magnetic stripes, bar codes, and optical memory (laser-readable) stripes—can be added to smart cards to support interactions with existing systems and services or to provide additional storage capacity. An agency that has been using magnetic stripe cards for access to certain facilities could migrate to smart cards that would work with both its existing magnetic stripe readers as well as new smart card readers. Of course, the functions provided by the card's magnetic stripe, which cannot process transactions, would be much more limited than those supported by the card's integrated circuit chip. Optical memory stripes (which are similar to the technology used in commercial compact discs) can be used to equip a card with a large memory capacity for storing more extensive data—such as color photos, multiple fingerprint images, or other digitized images—and for making that card and its stored data very difficult to counterfeit.[4] Figure 1 shows a typical example of a smart card.

Figure 1: A Typical Smart Card



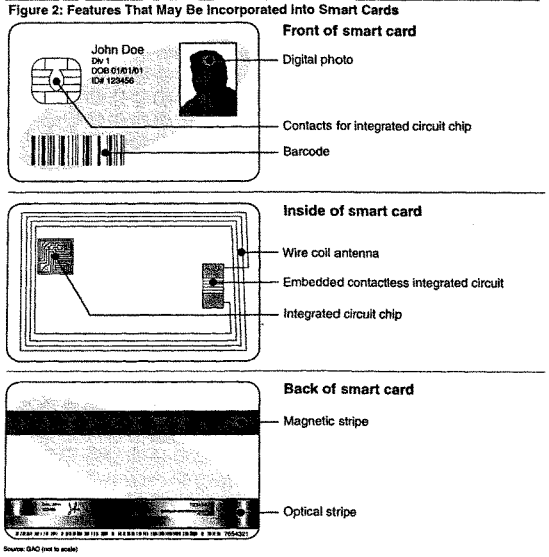
Source: GSA

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

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

Smart cards are grouped into two major classes: contact cards and "contactless" cards. Contact cards have gold-plated contacts that connect directly with the read/write heads of a smart card reader when the card is inserted into the device. Contactless cards contain an embedded antenna and work when the card is waved within the magnetic field of a card reader or terminal. Contactless cards are better suited for environments where quick interaction between the card and reader is required, such as high-volume physical access. For example, the Washington Metropolitan Area Transit Authority has deployed an automated fare collection system using contactless smart cards as a way of speeding patrons' access to the Washington, D.C., subway system. Smart cards can be configured to include both contact and contactless capabilities, but two separate interfaces are needed, because standards for the technologies are very different.

Figure 2: Features That May Be Incorporated into Smart Cards



Source: GAO (not to scale)

Since the 1990s, the federal government has considered the use of smart card technology as one option for electronically improving security over buildings and computer systems. In 1996, OMB tasked GSA with taking the lead in facilitating a coordinated interagency management approach for the adoption of multiapplication smart cards across government. At the time, OMB envisioned broad adoption of smart card technology throughout the government, as evidenced by the President's budget for fiscal year 1998, which set a goal of enabling every federal employee ultimately to be able to use one smart card for a wide range of purposes, including travel, small purchases, and building access. In January 1998, the President's Management Council and the Electronic Processing Initiatives Committee[5] (EPIC) established an implementation plan for smart cards that called for a governmentwide, multiapplication card that would support a range of functions—including controlling access to government buildings—and operate as part of a standardized system. More recently, the Enhanced Border Security and Visa Entry Reform Act of 2002 called for enhancing national security and counterterrorism efforts by using technologies such as smart cards that could provide biometric comparison and authentication to better identify individuals entering the country.[6]

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

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

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

Smart Cards Can Provide a Variety of Benefits to Federal Agencies

The unique properties and capabilities of smart cards offer the potential to significantly improve the security of federal buildings, systems, data, and transactions. For example, the process of verifying the identity of people accessing federal buildings and computer systems, especially when used in combination with other technologies, such as biometrics, is significantly enhanced with the use of smart cards. Since 1998, multiple smart card projects have been launched in the federal government, addressing an array of capabilities and providing many tangible and intangible benefits, including enhancing security over buildings and other facilities, safeguarding computer systems and data, and conducting financial and nonfinancial transactions more accurately and efficiently. Other potential benefits and uses include creating electronic passenger lists for deploying military personnel and tracking immunization and other medical records.

The advantage of smart cards—as opposed to cards with simpler technology, such as magnetic stripes or bar codes—is that smart cards can exchange data with other systems and process information rather than simply serving as static data repositories. By securely exchanging information, a smart card can help authenticate the identity of the individual possessing the card in a far more rigorous way than is possible with simpler, traditional ID cards.

Even stronger authentication can be achieved if smart cards are used in conjunction with biometrics. Smart cards can be configured to store biometric information (such as fingerprints or iris scans) in electronic records that can be retrieved and compared with an individual's live biometric scan as a means of verifying that person's identity in a way that is difficult to circumvent. A system requiring users to present a smart card, enter a password, and verify a biometric scan provides what security experts call "three-factor" authentication, the three factors being "something you possess" (the smart card), "something you know" (the password), and "something you are" (the biometric). Systems employing three-factor authentication are considered to provide a relatively high level of security.[7]

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

Several Agencies Are Pursuing Smart Card Projects

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

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

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

In addition to better securing physical access to facilities, smart cards can be used to enhance the security of an organization's computer systems by tightening what is known as "logical" access to systems and networks. A user wishing to log on to a computer system or network with controlled access must "prove" his or her identity to the system—a process called authentication. Many systems authenticate users by merely requiring them to enter secret passwords, which provide only modest security because they can be easily compromised. Substantially better user authentication can be achieved by supplementing passwords with smart cards. To gain access under this scenario, a user is prompted to insert a smart card

into a reader attached to the computer as well as type in a password. This authentication process is significantly harder to circumvent, because an intruder would need not only to guess a user's password but also to possess the same user's smart card.

Smart cards can also be used in conjunction with public key infrastructure (PKI) technology to better secure electronic messages and transactions. A properly implemented and maintained PKI can offer several important security services, including assurance that (1) the parties to an electronic transaction are really whom they claim to be, (2) the information has not been altered or shared with any unauthorized entity, and (3) neither party will be able to wrongfully deny taking part in the transaction. An essential component is the use of special pairs of encryption codes, called "public keys" and "private keys," that are unique to each user. The private keys must be kept secret and secure; however, storing and using private keys on a computer leaves them susceptible to attack, because a hacker who gains control of that computer may then be able to use the private key stored in it to fraudulently sign messages and conduct electronic transactions. In contrast, if the private key is stored on a user's smart card, it may be significantly less vulnerable to attack and compromise. Security experts generally agree that PKI technology is most effective when deployed in conjunction with smart cards.[8]

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

[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).

plans to add a contactless chip to the card in the future to speed physical access for military personnel to Defense facilities.

Challenges to the Successful Adoption of Smart Cards

The benefits of smart card adoption can be achieved only if key management and technical challenges are understood and met. While these challenges have slowed the adoption of smart card technology in past years, they may be less difficult in the future because of increased management concerns about securing federal facilities and information systems, and because technical advances have improved the capabilities and reduced the cost of smart card systems.

Sustaining Executive-Level Commitment

Maintaining executive-level commitment is essential to implementing a smart card system effectively. For example, according to Defense officials, the formal mandate of the Deputy Secretary of Defense to implement a uniform, common access identification card across Defense was essential to getting a project as large as the Common Access Card initiative launched and funded.[9] The Deputy Secretary also assigned roles and responsibilities to the military services and agencies and established a deadline for defining smart card requirements. Defense officials noted that without such executive-level support and clear direction, the smart card initiative likely would have encountered organizational resistance and concerns about cost that could have led to significant delays or cancellation.

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

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

largely because executive-level priorities had changed, and support for a wide-scale smart card project had not been sustained.

Recognizing Resource Requirements

Smart card implementation costs can be high, particularly if significant infrastructure modifications are required, or other technologies, such as biometrics and PKI, are being implemented in tandem with the cards. Key implementation activities that can be costly include managing contractors and card suppliers, developing systems and interfaces with existing personnel or credentialing systems, installing equipment and systems to distribute the cards, and training personnel to issue and use smart cards. As a result, agency officials have found that obtaining adequate resources is critical to implementing a major government smart card system.

For example, at least $4.2 million[10] was required to design, develop, and implement the Western Governors Association's Health Passport Project to service up to 30,000 customers of health care services in several western states. A report on that project acknowledged that it was complicated and costly to manage card issuance activities. The report further indicated that help-desk services were difficult to manage because of the number of organizations and outside retailers, as well as different systems and hardware involved in the project.[11] Project officials said they expect costs to decrease as more clients are provided with smart cards and the technology becomes more familiar to users; they also believe that smart card benefits will exceed costs over the long term.

The full cost of a smart card system can also be greater than originally anticipated because of the costs of related technologies, such as PKI. For example, Defense initially budgeted about $78 million for the Common Access Card program in 2000 and 2001 and expected to provide the device to about 4 million military, civilian, and contract employees by October 2003. It now expects to expend over $250 million by 2003—more than double the original estimate—and likely will not have all cards distributed until 2004. Many of the increases in Common Access Card program costs were attributed by Defense officials to underestimating the costs of

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

[11] Jenny Bernstein, Robin Koralek, Cheryl Owens, Nancy Pindus, and Barbara Selter, *Final Report—1. Health Passport Project: Assessment and Recommendations* (December 2001).

upgrading and managing legacy systems and processes for card issuance. According to Defense program officials, the department will likely expend over $1 billion for its smart cards and PKI capabilities by 2005. In addition to the costs mentioned above, the military services and defense agencies were required to fund the purchase of over 2.5 million card readers and the middleware to make them work with existing computer applications, at a cost likely to exceed $93 million. The military services and defense agencies are also expected to provide funding to enable applications to interoperate with the PKI certificates loaded on the cards. Defense provided about $712 million to issue certificates to cardholders as part of the PKI program but provided no additional funding to enable applications.[12]

Integrating Physical and Logical Security Practices across Organizations

The ability of smart card systems to address both physical and logical (information systems) security means that unprecedented levels of cooperation may be required among internal organizations that often had not previously collaborated, especially physical security organizations and information technology organizations. Nearly all federal officials we interviewed noted that existing security practices and procedures varied significantly across organizational entities within their agencies and that changing each of these well-established processes and attempting to integrate them across the agency was a formidable challenge.

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

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

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

Achieving Interoperability among Smart Card Systems

Interoperability[13] is a key consideration in smart card deployment. The value of a smart card is greatly enhanced if it can be used with multiple systems at different agencies, and GSA has reported that virtually all agencies agree that interoperability at some level is critical to widespread adoption of smart cards across the government. However, achieving interoperability has been difficult, because smart card products and systems developed in the past have generally been incompatible in all but very rudimentary ways. With varying products available from many vendors, there has been no obvious choice for an interoperability standard.

GSA considered the achievement of interoperability across card systems to be one of its main priorities in developing its Smart Access Common ID Card contract, which is intended to serve as a governmentwide vehicle for obtaining commercial smart card products and services. Accordingly, GSA designed the contract to require awardees to work with GSA and the National Institute of Standards and Technology (NIST)[14] to develop a government interoperability specification. The resulting specification defines a uniform set of command and response messages for smart cards to use in communicating with card readers. Vendors can meet the specification by writing software for their cards that translates their

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

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

unique command and response formats to the government standard. Such a specification previously had not been available.

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

Maintaining the Security of Smart Card Systems and Privacy of Personal Information

Although concerns about security are a key driver for the adoption of smart card technology in the federal government, the security of smart card systems is not foolproof and must be addressed when agencies plan the implementation of a smart card system. Smart cards can offer significantly enhanced control over access to buildings and systems, particularly when used in combination with other advanced technologies, such as PKI and biometrics. Although smart card systems are generally much harder to attack than traditional ID cards and password-protected systems, they are not invulnerable. In order to obtain the improved security services that smart cards offer, care must be taken to ensure that the cards and their supporting systems do not pose unacceptable security risks.

Smart card systems generally are designed with a variety of features designed to thwart attack.[16] For example, cards are assigned unique serial numbers to counter unauthorized duplication and contain integrated circuit chips that are resistant to tampering so that their information cannot be easily extracted and used. However, security experts point out that because a smart-card–based system involves

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

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

many different discrete elements that cannot be physically controlled at all times by an organization's security personnel, there is at least a theoretically greater opportunity for malfeasance than would exist for a more self-contained system.[17]

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

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

In addition to security, protecting the privacy of personal information is a growing concern and must be addressed with regard to the personal information contained on smart cards. Once in place, smart-card–based systems designed simply to control access to facilities and systems could also be used to track the day-to-day activities of individuals, potentially compromising their privacy. Further, smart-card–based systems could be used to aggregate sensitive information about individuals for purposes other than those prompting the initial collection of the information, which

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

could compromise privacy. The Privacy Act of 1974[18] requires the federal government to restrict the disclosure of personally identifiable records maintained by federal agencies, while permitting individuals access to their own records and the right to seek amendment of agency records that are inaccurate, irrelevant, untimely, or incomplete. Further, the E-Government Act of 2002[19] requires that agencies conduct privacy impact assessments before developing or procuring information technology that collects, maintains, or disseminates personally identifiable information. Accordingly, agency officials need to assess and plan for appropriate privacy measures when implementing smart-card–based systems and ensure that privacy impact assessments are conducted when required.

GSA, NIST, and other agency officials indicated that security and privacy issues are challenging, because governmentwide policies have not yet been established, and widespread use of the technology has not yet occurred. As smart card projects evolve and are used more frequently, especially by citizens, agencies are increasingly likely to need policy guidance to ensure consistent and appropriate implementation that ensures an adequate degree of security as well as privacy.

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

Given the significant management and technical challenges associated with successful adoption of smart cards, an ongoing series of initiatives have been undertaken in the federal government to facilitate the adoption of the technology. As I mentioned earlier, GSA was originally tasked in 1996 with coordinating an effort to adopt multiapplication smart cards across the federal government, and it has taken important steps to promote federal smart card use. For example, since 1998, GSA has worked with several other federal agencies to promote broad adoption of smart cards for authentication throughout the federal government. Specifically, GSA worked with the Department of the Navy to establish a technology demonstration center to showcase smart card technology and applications, and it established a smart card project managers'

[18] 5 U.S.C. § 552a.

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

group and Government Smart Card Interagency Advisory Board.[20] The agency also established an interagency team to plan for uniform federal access procedures, digital signatures, and other transactions, and to develop federal smart card interoperability and security guidelines.

For many federal agencies, GSA's chief contribution to promoting federal adoption of smart cards was its effort in 2000 to develop a standard contracting vehicle for use by federal agencies in procuring commercial smart card products from vendors.[21] Under the terms of the Smart Access Common ID Card contract, GSA, NIST, and the contract's awardees worked together to develop smart card interoperability guidelines—including an architectural model, interface definitions, and standard data elements—that were intended to guarantee that all the products made available through the contract would be capable of working together. Several federal smart card projects—including projects at NASA and the Departments of Homeland Security, State, and the Treasury—have used or are planning to use the GSA contract vehicle. This effort is intended to directly address the challenge of achieving interoperability among smart card systems that I mentioned earlier.

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

OMB Has Recently Set New Policy for Governmentwide Smart Card Adoption

In our January report, we also recommended that OMB develop governmentwide policy guidance for adoption of smart cards,

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

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

seeking input from all federal agencies, with particular emphasis on agencies with smart card expertise. We noted that without such guidance, agencies may be unnecessarily reluctant to take advantage of the potential of smart cards to enhance the security of agency facilities and automated systems.

OMB has begun to take action to develop a framework of policy guidance for governmentwide smart card adoption. Specifically, on July 3, 2003, OMB's Administrator for E-Government and Information Technology issued a memorandum detailing specific actions the administration was taking to streamline authentication and identity management in the federal government.[22] The memo sketched out a three-part initiative:

- First, OMB plans to develop common policy for authentication and identity management, including technical guidance to be developed by GSA and NIST, that will result in a comprehensive policy for credentialing federal employees. A newly established Federal Identity and Credentialing Committee is intended to collect agency input on policy and requirements and coordinate this effort.
- Second, OMB intends to execute a governmentwide acquisition of authentication technology, including smart cards, to achieve cost savings in the near term. The memo states that agencies are encouraged to refrain from making separate acquisitions without coordinating with the Federal Identity and Credentialing Committee.
- Finally OMB plans to consolidate agency investments in credentials and PKI services by selecting shared service providers by the end of 2003 and planning for agencies to migrate to those providers during fiscal years 2004 and 2005.

Challenges Remain in Implementing the New Policy

Much work remains to be done to turn OMB's vision of streamlined federal credentialing into reality. According to GSA's smart cards program director, it will be difficult to reconcile the widely varying security requirements of federal agencies to arrive at a stable system design that all agencies can adhere to. Even with a new version of NIST's governmentwide smart card interoperability specification in

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

place, agencies are still not in agreement about definitions for certain basic elements, because advances in technology create endless opportunities to change the specification. For example, the Department of Defense is currently seeking a change in the standard size of a smart card's embedded identifying code, to strengthen the card's internal security. However, implementing such a change may be very expensive for agencies already committed to the existing specification. While it is important to keep technical specifications up to date—and addressing security is a challenge that I've already noted—frequent changes in specifications could nevertheless slow progress in achieving a governmentwide solution. Given the trade-offs that must be considered, achieving governmentwide interoperability of smart cards could take longer than OMB's memorandum anticipates.

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

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

to rely on credentials issued by other agencies, because they would not know what level of assurance was met in issuing those credentials.

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

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

Contact and Acknowledgements

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

Mr. PUTNAM. Our next witness is Ms. Sandy Bates from the General Services Administration. Ms. Bates was named Commissioner of the Federal Technology Service in March 2000 after 2 years as Deputy Commissioner. FTS is the GSA's information technology and telecommunications organization that provides more than $5 billion in products and services to Federal Government agencies each year. Prior to her work at GSA, Ms. Bates was with NASA where she held various positions in telecommunications, including program manager for NASA's agencywide local service program and for their Program Support Communications Network.

Welcome to the subcommittee. You're recognized for 5 minutes.

STATEMENT OF SANDY BATES, COMMISSIONER OF FEDERAL TECHNOLOGY SERVICES, GENERAL SERVICES ADMINISTRATION

Ms. BATES. Thank you. Mr. Chairman, thank you for the invitation 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 continues to take innovative actions to help agencies secure their facilities and information. We participate in governmentwide committees such as the Interagency Advisory Board, Federal Identity Credentialing Committee, the Interagency Security Committee and the Smart Card Alliance.

I'd like to give you a brief history of the smart card program and address the concerns in your letter.

The GSA Federal Technology Service, along with the industry partners, can today meet agencies needs for smart cards, card readers, applications development, interoperability and complete systems integration. We do this through our governmentwide smart card contract.

With regard to use of smart cards within GSA, the agency has initiated several programs. Currently, all GSA associates in the Washington, DC area have smart card IDs. All GSA associates nationwide will have smart card IDs in fiscal year 2004. GSA's regional office in New York is implementing smart cards at three locations in New York City for physical access. They will be using a contact/contactless smart card. The card will also include a biometric thumbprint. Cards are currently being issued to all Federal employees and contractors at these three locations. Employees will be able to use the cards to gain access to the building through optical portals.

Once the initial physical access program is completed, GSA will begin planning to implement a smart card solution for computer access. Tenet agencies in these buildings that will be using the smart card for physical access include HUD, EPA, the Corps of Engineers, IRS, FBI, INS and Homeland Security.

A major feature of GSA's smart card contract is the establishment of technical specifications for smart card interoperability. These standards are the first of their kind for smart cards in government and represent a tremendous joint effort by GSA, industry partners and other Federal agencies.

The GSA's Interagency Advisory Board was established after publication of the initial version of the standards. The members in-

clude representatives from industry and government. The IAB continues to refine and update the interoperability specifications.

A recent test 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 agency's physical access system to gain access. The test participants were GSA, State Department and the Transportation Security Administration. Representatives from GSA and TSA inserted their smart card IDs in the State Department's readers and were granted access to the building.

Regarding biometrics, GSA is working with other agencies and key nongovernmental organizations such as the Biometrics Consortium to develop worldwide standards. These standards will become part of the GSA specifications.

The GSA Federal Technology Service is also leading the E-Authentication E-Gov initiative. Under this initiative, GSA is leading the Federal Identity Credentialing Committee, which will define the policies for issuance and management of identity credentials 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. Government cost savings can be achieved through standardization, shared services and consolidated purchasing.

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. Thank you.

Mr. PUTNAM. Thank you, Ms. Bates. We appreciate that.

[The prepared statement of Ms. Bates follows:]

SANDRA N. BATES

COMMISSIONER

FEDERAL TECHNOLOGY SERVICE

U.S. GENERAL SERVICES ADMINSTRATION

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.

3

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 it's governmentwide smart card contract with it's 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.

Mr. PUTNAM. Our third witness is Mr. Kenneth Scheflen. Mr. Scheflen is the director of the Defense Manpower Data Center [DMDC], a position he has held since 1977. In this position he's involved in both the management and technical aspects of programs which he supervises. Since 1998, DMDC has been the host for the Common Access Card office, formerly the DOD Smart Card Technology Office, which is in the process of converting the current military ID card to a smart card containing PKI certificates needed to secure the DOD information technology infrastructure and other applications. This project is widely regarded as the most advanced large-scale smart card program in the world.

Welcome to the subcommittee.

STATEMENT OF KENNETH C. SCHEFLEN, DIRECTOR, DEFENSE MANPOWER DATA CENTER, U.S. DEPARTMENT OF DEFENSE

Mr. SCHEFLEN. Mr. Chairman, good morning.

Thank you for all the kind words, those of you that mentioned the CAC this morning. We think it's a real success story, one of the first and probably the world's largest rollout of over 3 million smart cards to date, a multiapplication smart card which incorporates the use of biometrics in its issuance process.

The CAC is an identity-management, identity-assurance tool. It was done relatively quickly, 6 months from approval until it entered beta testing, largely because it was based on standards and best-commercial-practices. The speed and approach is not at all that typical of the way DOD does IT systems. DOD depended on other government organizations like NIST and GSA for help in establishing standards and evaluating products against these standards.

The fielding of the CAC, infrastructure to use it and the PKI credentials it carries is a large and costly enterprise. DOD is fortunate to have the resources to be able to do it. The CAC probably would have not happened without the decision by the Department to field PKI throughout the Department, the need to find a token and an infrastructure to issue PKI tokens.

Essentially PKI, became the killer application for justifying the economic case for smart cards, and I think without that we probably could not have made the economic justification.

The CAC is designed to be a multi-technology, multi-application product. The hope is that we can move people away from the notion that visual inspection of any ID card is sufficient security, and I would note the Washington Post article this morning quoting the GAO investigation of the ease of counterfeiting driver's licenses and then using those as breeder documents to get other things. We have to quit doing that.

We plan to continue to evolve and to improve both the CAC itself, the information it carries on it, the security of its issuance process and the use of its capabilities to take advantage of new technologies and continuously improve the security posture of the Department.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you very much, Mr. Scheflen.

[The prepared statement of Mr. Scheflen follows:]

Not for publication until released by the subcommittee

Prepared Statement of

Ken Scheflen

Director, Defense Manpower Data Center (East)

Before the Government Reform Subcommittee on Technology, Information Policy, Integovernmental Relations and the Census

Oversight Hearing on "Advancements in Smart Card and Biometric Technology"

September 9, 2003

Good morning. As the Director of the Defense Manpower Data Center (DMDC), I am responsible for the development, fielding, and maintenance of a number of DoD-wide systems. I will discuss two of these systems today: The Common Access Card commonly referred to as the CAC, and the Biometric Identification Systems or BIDS.

The CAC is a multi-technology chip-based card or "smart card" which is rapidly replacing the existing military identification/ Geneva Convention card for all uniformed service personnel. It is also being given to DoD civilian employees, Selected Reserve and to contractors who require physical access to DoD facilities or otherwise require logical access to DoD systems. This is the first time there has been a standard ID card for either of these populations. DMDC also continues to field the systems which give ID cards to military retirees and family members of active, reserve, and retired personnel. In all, the DoD issues about 4 million ID cards each year and we have over 11 million people with DoD identification cards. The CAC will be issued to about one-third of the overall population or approximately 4 million people.

I would like to take a moment to summarize the status of the CAC roll out and to discuss a few of the technical issues involved. The CAC is the most advanced major smart card program in the world and has been the recipient of twelve major US and international awards including the highly coveted Federal Leadership or "Gracie" award and for being a Computerworld Honors Worldwide Finalist. It is also one of the few major programs doing local rather than centralized card production and issuance. This is due to the importance of the card to military-affiliated people and to the far flung nature of the DoD enterprise. In order to prepare the infrastructure to issue CACs, installers visited 945 locations in twenty-seven countries to install hardware and

software and train operators on how to use the new system. This infrastructure roll out was completed in July 2003 after about an 18 month effort. CAC cards are issued as soon as the equipment has been installed and to date over 3 million have been issued at a rate of 10-15,000 per day and rising.

At DMDC we like to say that we are in the "identity management" business as opposed to the ID card business. It is very clear that the events of 911 and the subsequent investigations have shown how easily obtainable both genuine and forged documents purporting to assert identity are to acquire. Indeed, there is no easy solution to the world-wide problem of knowing exactly who each person is with absolute certainty and binding that person to an identity document or documents with absolute certainty. DoD has a better chance of doing this than most other organizations because of the vetting that its members go through during the enlistment or hiring process. However, even our process is not perfect and we continue to make improvements to our business processes to take advantage of cutting edge technologies. The CAC, one such new technology, is designed to securely bind the identity of a person encountered in a "face-to-face" situation with a highly secure identity card. The CAC contains two bar codes, a magnetic stripe, printed material, digital photograph and an integrated circuit chip (ICC). It is this latter feature which makes it a Smart Card and which makes it possible to use cryptographic tools to log on to a computer, assert one's identity, conduct secure e-business and e-gov and digitally sign and encrypt email. If used properly in a multi-factor system it can also be used as a physical access tool. In order to actually use the CAC for these purposes, it is necessary for DoD to roll out additional infrastructure-card readers and desk-top middleware and software to enable authentication to web sites using the CAC's digital certificates. This roll out, which is the

responsibility of the individual services and components, is also well under way with over a million workstations now having the required hardware and software.

I mentioned earlier that we are in the identity management business and that we need to have high assurance that the in-the-flesh person we securely bind to CAC credentials is who he or she purports to be. Identity verification is key and this is one reason why we insist on a face-to-face interaction in addition the presentation of an existing ID card or other credential. Going even further, we have been capturing digital fingerprints on military personnel for approximately four years and thus have prints on most all uniformed members. As part of the CAC issuance we capture prints on civilian and contractor personnel. At re-issuance, which is at intervals no greater than three years, the system does a fingerprint check between the live person and the data base to ensure it is the same person. In the event of a non-match, which can occur for a number of reasons, the operator is required to take additional steps to verify identity before issuing a card. DMDC is working to receive digital fingerprints captured at our enlistment processing stations and transmit them to the FBI for criminal records checks prior to entry. These prints would be used to verify identity the first time a person was issued a CAC, further strengthening the identity management process. DMDC is also experimenting with facial recognition software to permit comparisons of digital images in the data base with camera images of the live person for use in cases where fingerprints do not match or are not used, as is the case for family member cards. While considerable investigation or the utility of other biometric measures is going on in the DoD under the auspices of the DoD Biometrics Management Office, current plans for the CAC are limited to fingerprints and facial recognition.

DMDC is engaged in other projects which make use of both identity cards, CAC as well as others, and biometrics. The best developed of these is the system known as BIDS or the Biometric Identification System. This is a force protection system developed initially by DMDC at the request of US Forces Korea. In brief, it uses cards, photographs and fingerprints to control access to all gates to US facilities on the Korean peninsula. All personnel having access are required to go through a registration process where biometrics are captured and cards issued to those who do not already have either CACs or other DoD issued credentials. A "one-to- many" fingerprint check is made to identify anyone already in the data base. A server based data base, which is downloaded to the gates, is available throughout Korea and is designed to operate in the absence of communications if necessary. Gate guards have wireless handheld and other devices capable of scanning a card and determining whether it is genuine and valid, bring up a photograph of the person from the data base and perform a fingerprint check in a matter of seconds. Any or all of these checks can be done depending on the threat conditions. The system notifies guards that someone should be barred or even arrested.

A version of this system is currently being installed in all US facilities in the European Command (EUCOM) Area of Responsibility (AOR). In Europe, this system is known as the Installation Access Control System (IACS). DMDC worked in coordination with the Army to make the changes necessary to meet the unique requirements of the European environment.

A further expansion of BIDS is underway in Kuwait where, in addition to the biometric technologies discussed earlier, hand geometry is being incorporated. This is because there are large numbers of local national day workers who are largely laborers that require physical

access. It is difficult to obtain quality fingerprint readings due to the type of work performed and thus an additional biometric technology has been introduced.

The common characteristic of the BIDS and its related systems is that we are moving the identity management paradigm forward. It is not enough to issue a secure identification card; you must use the technology to positively identify the person at the borders of your enterprise - whether it is for physical or logical access. A guard inspecting an ID card is simply not good enough today, when fakes are easily crafted and motivation for deception is high. The new generation of access systems use the technology embedded on the card to ensure we are granting access to the right person.

I would like to conclude my statement with a few remarks about the importance of using standards-based commercial products whenever possible. The ability to write specification in terms of well-defined and accepted national and international standards, and to have laboratories which can test products and certify that these standards have been met, ultimately reduces the cost to the users and promotes interoperability between and among Federal Agencies, business partners, and other countries. There has been a concerted effort to use such standards in the development and implementation of the CAC and both the General Services Administration (GSA) and the National Institute of Standards and Technologies (NIST) have been critical key partners in this process. Consequently, it is very easy for other organizations to adopt all or part of what DoD has done with CAC, to take advantage of multiple sources of supply based on standards, and to achieve interoperability with DoD and others. DoD and DMDC have worked

and will continue to work in conjunction with other parts of the government wanting our assistance with similar programs or to provide information on valuable lessons learned.

Thank you for the opportunity to address the Subcommittee.

Mr. PUTNAM. Finally, we have Mr. Ben Wu. Mr. Wu is Deputy Under Secretary for Technology at the U.S. Department of Commerce. In this capacity he supervises policy development, direction and management at the Technology Administration, a bureau of over 4,000 employees that includes the Office of Technology Policy, the National Institute of Standards and Technology and the National Technical Information Service.

Welcome to the subcommittee.

STATEMENT OF BENJAMIN WU, DEPUTY UNDER SECRETARY OF COMMERCE FOR TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Mr. WU. Thank you, Mr. Chairman.

As you mentioned, as the Deputy Under Secretary of Commerce for the Technology Administration, I do assist in the direct oversight of the National Institute of Standards and Technology [NIST]. While NIST is one of the crown jewels of our Nation's Federal laboratory system as our Nation's oldest Federal laboratory, it is also at times one of our true hidden gems, despite the significant research expertise of its world-class scientists, including two Nobel Prize winners. So I appreciate the subcommittee's recognition of NIST's vast technical portfolio and its service to our Nation and the opportunity to appear before you today to review NIST's work in smart card and biometric technology.

Mr. Chairman, in these times of heightened national security, I applaud the work of this subcommittee to bring intergovernmental solutions to measures that can protect our homeland security. The Commerce Department shares this subcommittee's focus. Post September 11, Secretary Evans has committed the Department's resources to assist in the administration's homeland security efforts; and, as a result, NIST has been engaged in a number of critical issues, from first responder communications to chemical, biological, nuclear detection to encryption standards as well as the implementation of smart cards within the Federal Government.

NIST's smart card program dates back to 1988. Recognizing the potential for smart cards to improve the security of Federal IT systems in our national information infrastructure, NIST chose to invest significant research in smart card technology at an early stage, and as a result NIST has been on the cutting front of many of the early innovations that have been integral to the development of modern smart cards. These include a generic authentication interface for smart cards, the first smart cards to implement the data encryption algorithm and the digital signature algorithm and the first reprogrammable smart card.

In my time with you this morning, I'd like to review NIST's work on smart card interoperability, standardization, conformance testing and further research and development.

Many Federal agencies have a longstanding interest in smart card technology, as you've heard. Since smart cards are capable of cryptic functions, they can perform important security functions such as securely storing digital signatures, holding public key credentials and authenticating a claimed identity based on biometric data. So smart cards can be a crucial element in a range of current and future critical applications such as PKI, transportation worker

identity cards, DOD's CAC, electronic travel documents and a whole host of others.

However, large-scale deployment of smart cards has proven challenging. Agencies have found it difficult to deploy large-scale smart card systems due to a lack of interoperability among different types of smart cards. Without assurances of interoperability, agencies would be locked into a single vendor, and that is why NIST has been working so closely with industry and other government agencies to provide interoperability specifications, guidelines for an open and standard method for using the smart cards.

This issue of interoperability is crucial and has to be addressed before any additional investment can be made. Yet, historically, the smart cards have been driven by requirements arising from specific industry applications in certain domains such as banking, telecommunications and health care, and that has led to a development of smart cards that are customized to those specific domains with little interoperability between those domains. These vertically structured smart cards systems are expensive, difficult to maintain and often based on proprietary technology.

So when GSA created a contract vehicle and a program to procure interoperable smart card systems and services from the Federal sector, NIST took on the task of leading the technical development of a smart card interoperability framework, and this framework was designed to address the interoperability problems preventing governmentwide deployment of smart card technology and was ultimately incorporated into the smart card access common ID contract which GSA operated.

After additional work to address the Federal customer needs identified, NIST published two versions of the Government'S Smart Card Interoperability Specification [GSC–IS], one in June 2002 and the other most recently in July 2003, and both standards can be found on www.smartcard.NIST.gov.

GSC-IS has been well received and is making a significant impact. In fact, many Federal agencies are moving forward with plans to deploy large numbers of GSC-compliant systems. For example, DOD has incorporated the GSC-IS in its CAC, representing millions of cards, and it will be effective in early 2004.

Additionally, NIST responded to the January 2003, GAO report by examining issues associated with the definition of a multi-technology card platform. These technologies include smart card integrated circuits, optical stripe media, bar codes, magnetic stripes, photographs and holograms.

As a first step, NIST hosted a workshop on multitechnology card issues in July 2003, and brought in a number of the stakeholders in industry. This workshop focused on requirements, issues in Federal Government activities associated with multitechnology cards; and, more specifically, it examined technical and business issues, existing voluntary standards, consensus problems, multitechnology integration issues and industry capabilities in the field of ISO, compliance storage and processor card technologies.

Based on this workshop and its followup, NIST is producing a technical report that will identify integration interoperability research topics, identify gaps in standards coverage and also identify

multitechnology composition issues; and we expect that this report will be available for public comment in October 2003.

Then, in July 2003, we also published the most up-to-date GSC-IS, which is known as version 2.1, which I want to tell you a little bit about. This document addresses some of the GAO recommendations by incorporating support for biometrics, countless smart card technologies and public key infrastructure.

As you know, there is keen interest in the convergence of biometrics and smart cards, and NIST has also been working with industry to move forward the standards on an international front, too, working with ANSI and the international standards organizations to try to make the GSC-IS an international standard, and I'm pleased to say that a lot of progress has been made in that front.

Let me also just conclude by touching upon conformance assessment and further research and development needs. Conformance testing programs are important so that we can give assurances to the customers and users that we have a smart card that works well and can conduct business in the way that it's supposed to be advertised; and NIST conformance test engineers and reprogrammers are developing test criteria, building a suite of conformance standards and test tools so that we can just do just that. In addition, in looking at some of the smart card research and development work that needs to be done, this subcommittee is well aware that smart cards and associated technologies hold great promise for meeting many important needs, and we need to, as has been stated by GAO, make sure that there are strong commitments for research and development as well as providing good framework, best practices tools, as well as an educational program that will help with the acceptance and the furtherance of this industry in building it up.

So there's a lot of important issues that remain up front. The Department of commerce is committed in building this industry forward and working with our Federal agency partners to make sure the needs are met.

Thank you very much, Mr. Chairman.

Mr. PUTNAM. Thank you very much, Mr. Wu.

[The prepared statement of Mr. Wu follows:]

Statement of

Benjamin H. Wu

Deputy Under for Technology
U.S. Department of Commerce

Before the

Committee on Government Reform
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

"Advancements in Smart Card and Biometric Technology"

September 9, 2003

Chairman Putnam, Representative Clay, and Members of the Subcommittee, thank you for this opportunity to testify today about the National Institute of Standards and Technology's (NIST) activities related to the advancement of smart card and biometric technologies within the Federal government. NIST, which is part of the Technology Administration, is working with industry and other government agencies to provide interoperability specifications and guidelines to provide organizations with an open and standard method for using smart cards. NIST has also done considerable work in the area of biometrics under the auspices of the Patriot Act. Although this is not the main topic of today's hearing we would be glad to provide background documentation on our biometric program if desired.

Background

Smart cards provide opportunities for improving security of our critical infrastructure, both from a physical and logical perspective. Because they are capable of performing cryptographic functions, they can perform important security services such as securely storing digital signatures, holding public key credentials, and authenticating a claimed identity based on biometric data. As such, smart cards are a crucial element in a range of current and expected critical applications and programs such as Public Key Infrastructure, Transportation Worker Identity Card, Building Entry, DoD's Common Access Card (CAC), Electronic Travel Documents, and many others.

NIST's smart card program dates back to 1988. Recognizing the potential for smart cards to improve the security of Federal IT systems and our national information infrastructure, NIST chose to invest significant research effort in smart card technology at an early stage. The NIST smart card program produced many early innovations in the area such as a generic authentication interface for smart cards, the first cards to implement the Data Encryption Algorithm and the Digital Signature Algorithm, and the first reprogrammable smart card. These innovations are integral to modern smart cards.

Many Federal agencies have a longstanding interest in smart card technology. However, large-scale deployment of smart cards has proven challenging. A survey revealed that agencies found it difficult to deploy large-scale smart card systems due to a lack of interoperability among different types of smart cards and without assurances of interoperability, agencies would be "locked" into a single vendor. Thus, the issue of interoperability had to be addressed before significant investments were made. Additionally, smart card systems have historically been driven by requirements arising from specific application domains such as banking, telecommunications, and health care. This has led to the development of smart cards that are customized to the specific application requirements of each domain, with little interoperability between domains. These vertically-structured smart card systems are expensive, difficult to maintain, and often based on proprietary technology.

GSA created a contract vehicle and program to procure interoperable smart card

systems and services and to promote and facilitate the use of this critical security technology within the Federal sector. After much work to address the federal customer needs identified, NIST published two versions of the Government Smart-Card Interoperability Specification in June 2002 and July 2003, respectively. (Available via http://smartcard.nist.gov/ .)

The GSC-IS has been well received and is making a significant impact: many Federal agencies are moving forward with plans to deploy large numbers of GSC-compliant systems. The Department of Defense's Defense Manpower Data Center, Common Access Card (CAC) Program Office has stated the following about NIST and smart cards:

> *Our department recognizes the ...technical skill and leadership in the area of Smart Card Interoperability and building the Government Smart Card Interoperability Specification... vital to the interests of our Department as well as a major contribution in the Federal Sector regarding national security.*

DoD has adopted the Interoperability Specification for their enterprise-wide CAC deployment, representing millions of cards (to be effective in early 2004.)

Standardization

GSA and other Federal agencies have long sought to avoid the problem of being locked into proprietary, non-interoperable smart card technologies. Recognizing the needs of the Federal customer base, NIST is working with American National Standards Institute (ANSI) and the International Organization for Standardization (ISO) to standardize this (or an evolved) specification. ANSI will carry the draft standard forward to ISO for consideration as an international standard. At a plenary meeting of the National B10 (Identification Cards) meeting last week, a unanimous vote was achieved to support this effort as a new work item.

ANSI formally submitted the GSC-IS, Version 2.1 to ISO in August 2003. NIST was asked by ANSI to chair an *ad hoc* workgroup to manage the standardization process and subsequently to chair a new ANSI subcommittee. This ANSI workgroup was specifically established to address the specification.

The General Accounting Office (GAO) issued a report in January 2003 on the Federal government's progress in adopting smart card technology. The report stated:

> *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, biometrics, and optical stripe media – as well as integration with PKI, to ensure broad interoperability among Federal agency systems.*

In response to these GAO recommendations and identified Federal agency needs, NIST is examining requirements for and issues associated with definition of a multi-technology card platform. Technologies being investigated for utility in a multi-technology platform include smart card integrated circuits, optical stripe media, bar codes, magnetic stripes, photographs, and holograms. As a first step, NIST hosted a workshop on multi technology card issues in July of this year. The workshop focused on requirements, issues, and Federal government activities associated with multi-technology cards. More specifically, it examined general technical and business issues, existing voluntary industry consensus standards, gap areas in standards coverage, and industry capabilities in the field of ISO/IEC 7810-compliant storage and processor card technologies. The workshop also addressed multi technology integration issues, and both inter-jurisdictional and inter-technology interoperability issues.

Based on the proceedings of the workshop and subsequent interviews conducted with the user community, NIST is producing a technical report that will identify integration and interoperability research topics, identify gaps in standards coverage, and identify multi technology composition issues. We expect to post a draft report for public comment in October.

NIST published the GSC-IS, Version 2.1 in July 2003 as NISTIR 6887, 2003 Edition. This document addresses the remaining GAO recommendations by providing support for biometrics, contactless smart card technology, and Public Key Infrastructure.

There is considerable interest in the convergence of biometrics and smart cards. In response to requirements from the GSC customer base and recommendations in the GAO Report, NIST has included 'hooks' for biometric authentication modules in Version 2.1 of the GSC Interoperability Specification. During FY03, NIST also worked with an ANSI M1 ad hoc group to publish an analysis of existing biometric and smart card interoperability standards with respect to their ability to support integrated smart card-biometric systems. The report includes detailed recommendations for designing a GSC biometric plug-in framework. It has been submitted to ANSI B10 to provide a roadmap for integrating full biometric capabilities into the GSC framework during the formal standards development process. Published August 2003, the report is available to the general public on the ANSI/INCITS M1 document register (http://www.incits.org/tc_home/m1htm/docs/m1030398.pdf.).

Moreover, NIST is actively working with Europe and Japan towards a general smart card framework that can harmonize and align a variety of disparate approaches, technologies, and architectures. We believe that this would yield greater interoperability, lower costs and barriers, and enhanced security.

Smart Card Conformance Testing

Conformance testing is an important and integral element of a standards program. It can increase the confidence for consumers that a given product does conform to a given specification reducing the risk to the purchaser. NIST has been developing an

interoperability conformance test program in parallel with the GSC standards effort. The GSC conformance test program will rely on commercial laboratories to validate conformant products, providing customers with increased assurance that these products meet the interoperability requirements of the GSC framework. NIST conformance test engineers and programmers are developing test criteria and building a suite of conformance test tools to be used by commercial laboratories to test and ultimately improve private-sector smart card products.

Further Research and Development

Smart cards and associated technologies hold great promise for meeting many important needs in homeland security. Success in large-scale deployments of smart cards and their associated applications, however, is not assured. As a community, we will have to be innovative in finding ways to fund and develop the needed tools, tests, examples, frameworks, best practices, and research to deliver scalable, secure, and interoperable smart card infrastructure and associated applications.

Some of these tasks include the development of reference implementations, software developer's toolkits, data models, issuance policies, credential management, publication of implementation guidance, pilot projects and continued research and development. An educational program to share information and avoid duplication of effort would be of great benefit as well. Most of the Federal agencies that comprise the GSC community have budgets for their own smart card deployments, but these budgets do not include support for an interagency research and development program. Developing standards is critical to ubiquitous adoption (and achieving the attendant security benefits) of smart cards, and this work will continue to be of great importance.

Summary

The U.S. GSC-IS has generated considerable interest and support in both the U.S. domestic and international smart card communities. Key players in the smart card world, including NIST, are working to eliminate the roadblocks to widespread deployment of smart card technology in the U.S. and to increase competitiveness of the U.S. smart card industry in the global market, while improving the security of our nation's critical infrastructure.

Mr. PUTNAM. Mr. Willemssen, who at the end of the day is in charge of the Federal vision for smart card technology? Is it OMB?

Mr. WILLEMSSEN. From a policy perspective, it is OMB. Historically, OMB has relied heavily on GSA to carry out much of that policy, but I would say OMB reiterated its pre-eminence as the policymaker with their July 3rd memorandum which established a framework for future policy in the smart card arena.

Mr. PUTNAM. Is the goal to have discrete smart card technologies for each agency or a limited number, perhaps one for defense, one for nondefense or one for a particular clearance?

Mr. WILLEMSSEN. I would say the goal is to become, all other factors being equal, as standardized as possible.

Picking up on what Mr. Wu said, to the extent that we can continue updating the interoperability standard and getting everyone to fall in line with that standard, the much more efficiently we can do business smart card-wise across the Federal Government.

I also think that the Department of Defense's project, CAC, since it is so massive, really provides maybe the best laboratory from a lessons-learned perspective and implementation-challenges perspective on how the Federal Government can go forward from this point at additional agencies.

Mr. PUTNAM. But currently agencies have the discretion to move forward with their own smart card technology and Mr. Wu's outfit is playing catch-up to develop interoperability?

Mr. WILLEMSSEN. I would say generally yes, but at the same time one of the aspects of Mr. Forman's July 3rd memo stated that agencies should not be going about acquiring separate technologies without consultation with applicable committees. We would be supportive of that—of not going forward and essentially introducing additional stovepipes into the process.

Mr. PUTNAM. Well, how many stovepipes are there now?

Mr. WILLEMSSEN. I believe when we did our report earlier this year we had identified about 62 different projects at 18 different agencies.

Mr. PUTNAM. So just averaging out, three per agency?

Mr. WILLEMSSEN. Keeping in mind that the size of each of those projects varied dramatically all the way from CAC, which is very large. In addition, Transportation Security Administration has very massive plans on the drawing board to give cards to up to 15 million transportation workers. By contrast, some other projects are just in the pilot phase on a much smaller scale.

Mr. PUTNAM. Everybody has their own rodeo, everybody is running their own circus, and we're tearing down stovepipes on one side of the government and building them right back up on the other.

Mr. WILLEMSSEN. But I think to be fair to the executive branch, I think there's a recognition of that and an attempt to try to limit that from this point forward. But I agree with you in terms of the comment you just made about stovepipes.

Mr. PUTNAM. Is it technically feasible to have one card that meets all the needs of every government employee?

Mr. WILLEMSSEN. Technically, yes. Managerially and policywise, probably not.

It would probably be very difficult to standardize from a policy and management perspective that you could have one card that meets all the needs of all employees at all different security levels. Different security levels will require different techniques to protect data and assets. Technologically, sure, it could be done but, realistically, probably wouldn't. But I do think we need to standardize on fewer; and, again, linking up to what Mr. Wu said, the work that NIST has done on the interoperability standard can't be underestimated. That's the direction that the Federal Government needs to go.

Mr. PUTNAM. Mr. Wu, 10 years ago at the University of Florida there were 50,000 students. One smart card would give you access to the dorm, access to the computer lab, allow you to pay tuition, allow you to buy a pizza, allow you to debit your book costs, and allow you to use the ATM. A decade later why aren't we further along in the Federal Government's ability to deploy smart card technologies that are interoperable?

Mr. WU. Well, Mr. Chairman, I think that if you were to use the University of Florida in an FSU analogy, you know, the Federal Government is so large. That smart card wouldn't work in Tallahassee that would work in Gainesville. That is the problem we're facing right now, is that we see that each of the agencies, each of the subagencies are purchasing smart card technologies and moving forward along, and they're using applications that are right for their particular mission and purposes.

However, if we're trying to have all of the schools in Florida, say, or all of the agencies in the Federal Government try to talk to each other and be able to use one card in all of its systems, then we need to have interoperability. We need to have a standard that is adopted by industry so that we can create a market out there. We need to have industry agree on this specification, and we also need to be able to build it out on an international front so that we can develop a strong U.S. smart card technology market, and then we can be able to get all the accrual benefits for foreign markets and trade. If we can do it on our own shores, then move it to Asia, Europe and others.

So NIST is trying to do that, working with ANSI at the American National Standards Institute and trying to move the GSC-IS standard to an international fora and have it adopted within the international standards organization system. And if we can do that, then I think ultimately you will be able to see one smart card utilized throughout much of the United States but perhaps throughout the whole world, and we would have U.S. companies, U.S. industry leading that charge. And that's our goal.

Mr. PUTNAM. How smart do these cards need to be? I mean, has anybody really identified what the technical needs are? At what point do we determine that it has reached the level where it can be deployed, knowing that the technology will be changing on a very rapid basis? But has anybody defined what the needs are for a Federal Governmentwide smart card technology?

Mr. WU. Well, in a sense, if you have a multitechnology platform, the sky can be the limit, if you can have the photographs, the holograms, fingerprints, other data built into that platform.

So, once again, I think it comes down to developing a specification, a good standard that industry can then take and apply as many smart items or multitechnology items onto that card.

Mr. PUTNAM. Well, I don't know that really answered the question. I mean, we buy computers every day knowing that the next day they're obsolete to a degree, that we could have bought something bigger and better and faster and more productive; but at some point you have to draw the line and say this is adequate for our needs today, recognizing that the technology will continuously change.

But is the primary purpose of governmentwide smart card technology identity authentication, access control, efficiency so that purchases and financial services and E-travel can be consolidated onto one identification? What are we trying to accomplish? What's it going to cost us and what's it going to save us and at the end of the day what will we have achieved by deploying this technology that all of you are here to discuss?

Mr. WILLEMSSEN. I would say, Mr. Chairman, in a post September 11th environment, the primary purpose of smart cards is identity authentication, both from the standpoint of physical access to facilities and access to systems. There can be other purposes, but I think in today's environment that's the primary goal, is ensuring that you know that person is who they say they are, including thinking in detail about the process of when you give that individual their initial smart card, how are you going to ensure that, again, they are who they say they are.

Mr. PUTNAM. OK. Mr. Wu.

Mr. WU. Thank you.

Mr. Chairman, you raise an excellent question, and NIST has been grappling with that issue actually as everybody in the Federal policymaking sector has been grappling with that issue in relation to border security and the requirements under the USA Patriot Act. I think ultimately that question you raised is one that needs to be decided in conjunction with congressional and executive branch officials as to how far or how much you want on that smart card. With the border security issue, the USA Patriot Act—it requires a number of Federal agencies, specifically FBI, INS and State, to make sure that we have the strongest possible measures for people coming into and leaving the country.

There have been a number of tasks placed upon NIST to try to help create technical benefits that will allow for us to have stronger border patrol, and there have been a number of biometric opportunities with fingerprints, facial recognition, you know, iris retina scan and others that have been thrown into the mix. NIST recommended that we have a dual system of fingerprinting and facial recognition, but ultimately I think that decision is a public policy decision which Congress as well as the executive branch needs to come to a determination on.

Mr. PUTNAM. Can we replace the rubber stamp and ink pad and paper passport with a smart card?

Mr. WU. Well, that's ultimately the intention, to have some sort of biometric or smart card device so that we can have integrity and people coming into our borders who say they are somebody, to make sure they are in fact that person.

Mr. PUTNAM. Is that technically feasible today?

Mr. WU. It depends on—yes, it is. I mean, there are a number of biometric identifiers which could be done, fingerprints, facial recognition, iris scan, gait, even voice, but the question is how much we can afford to do, what is feasible and what isn't too technically complicated in order to get the job done? You need to determine what you need to—or what you want out of this technology, and then we can build the technology and new research onto that.

Mr. PUTNAM. But it sounds like the technology is already there.

Mr. WU. The technology is there. It's a matter of trying to incorporate it all in, and that's why I think the multitechnology platform and the standardization issue is so important.

Mr. PUTNAM. I'm just not sure what we're waiting on. I don't hear what magic technology we're waiting on to be developed before we can deploy this. We have the ability to do it now. What are we waiting on? What's the next step?

And if we're waiting for foolproof—one of the witnesses said that smart cards are not foolproof. Well, paper passports certainly aren't foolproof; and as long as the technology is moving forward to design these systems, there will be a technology moving forward to fake those systems. And that's just life. So let's move on.

Mr. Willemssen, in GAO's testimony, you said DOD has spent over $700 million to have digital certificates on smart cards, but they can't be used because no funding was provided to enable DOD applications to accept the certificates. Is that correct?

Mr. WILLEMSSEN. That was an issue at the time we did our review, yes, sir. Mr. Scheflen may have updated information that they have gotten that funding at this point.

Mr. PUTNAM. Mr. Scheflen.

Mr. SCHEFLEN. Well, I can't address the question in terms of where the money is. I don't believe that there is a problem in DOD with funds to smart card enable or PKI enable applications.

I have to be a little bit cautious because there's not one big pot of money somewhere that somebody is sitting on and doling out. There are different pots of money, and different parts of the organization have the responsibility for doing it. In this particular case the applications enabling side is the responsibility for funding and accomplishing on the individual services in the military departments.

The issuance of the cards and the digital certificates is more centrally funded and some in my budget and some in NSA and Defense Information Systems Agency. I don't believe that the services would be spending the money they have spent to install smart card readers on all of their computers and software at every desktop if they were not going forward with the applications enabling expenditures as well. The best example is probably NMCI, the Navy's rollout of their desktop systems where they from the beginning planned for smart cards to be used for cryptographic log-on to those systems.

I'm not aware there is anybody at DOD saying I don't have the money to do the implementation so that we can actually use the product, but I will take the question for the record, Mr. Chairman, if you'd like more information.

Mr. PUTNAM. I would. I would. Thank you.

July's OMB memo recognized that we've recreated a bunch of stovepipes. Somebody was kind of slow to pick up on that, I would assume. We've got 60 plus systems already out there; shouldn't we recommend everybody really ought to stop trying to develop their own systems? I assume we're waiting on NIST. Is that fair?

Mr. WILLEMSSEN. NIST has made progress. Actually, I think one of the big items to be waiting on right now is establishing a governmentwide employee credentialing policy which I believe is the focus of the committee that Commissioner Bates mentioned. That's really one of the key next steps.

Again, keeping in mind that if our primary purpose is to authenticate individuals and we want to move to a more standardized environment technologically then we need to move to more of a standardized policy on how Federal employees are going to be credentialed and focus on how that process is going to work; and once you set that policy, then the technology and the standards can follow, but you can't do them in reverse. Otherwise, you again run the risk of stovepiping.

The other thing I would mention is I think it will be instructive for the rest of the Federal Government to look at the experience of DOD with CAC, because that is by far the most massive effort. They've had some successes. I'm sure they've had some challenges, too, and to the extent that we can learn from that and not repeat any of the challenges, so to speak, I think that would be very beneficial.

Mr. PUTNAM. Mr. Willemssen, you said that different security policies within the agencies cause problems for implementation. Is that information security or physical security policies that differ?

Mr. WILLEMSSEN. Well, an example would be, historically, physical security organizations within Federal agencies like to rely on ID cards, and they like to see those ID cards, look at them, these days maybe touch them to make sure they're authentic. Again, I'm generalizing here, but many of those organizations are probably less likely and less culturally accepting of a smart card device. They're not used to that, and I'm sure that's an issue at the Department of Defense where you have a smart card that can both be used for physical access and access to computer systems. You may find a situation that many of the guards over at the Department of Defense still want this other card to identify the individuals rather than a smart card, and I think that can still be an issue at many agencies who run into those kinds of barriers.

The other thing I would point out is, just from a security level perspective, depending on the value and the sensitivity of the data and assets, you're going to have to vary the level of controls you're going to put in the card, as simple as, are we going to require biometrics for this given individual given what access they have, or is simply a password and a smart card without biometrics good enough? It depends on the value of the data, and the higher the value of that data, the more controls you'll have to put in place on the card.

Mr. PUTNAM. Today, what is the typical life of a card? What is the useful life of a given card before we would have to update them?

Mr. SCHEFLEN. Our life is 3 years, and that is not tied to how long the card could last but to the lifetime of the digital certificates that are contained on the card.

Normally, in DOD the ID cards that the military members get are tied to a number of things. One of them is their term of enlistment. Another may be the rank. There's a natural turnover of cards and it was 3 or 4 years with the existing cards before we had smart cards. Going to a fixed 3-year limit because of the lapsing of the digital certificates didn't reflect that much of a change.

The good thing about it is that it allows a natural ability to introduce new technology on a gradual basis. You don't have to say "we're going to stop today and recall all the cards. We can phase them in over a period as the cards naturally expire or as people come and go. We have 3,000 or 4,000 people coming and going just on the uniform side, so it's a fair number.

If I might add a couple of comments to Mr. Willemssen's—yes, I think he has the physical security material down and about right. We clearly experience those same kinds of problems in DOD. The physical security community is much more comfortable with badges that are locally issued which they recognize and look at. It is a continuing issue for us to try to get away from the notion that looking at something provides security, which in my opinion, it doesn't today.

Another common misunderstanding by a lot of people inside the Department is that the issuance of a CAC card with all the various credentials it has on it somehow conveys some privileges, but in truth it doesn't. The privileges to enter a building, to log onto a computer, or to get on an airplane or whatever are still authorized by those that are in charge of granting those privileges. The same thing happens with the notion of an ID card that would be a DOD card that could be accepted for entry into the State Department.

The holding of a card itself doesn't necessarily authorize me to go anywhere. What would presumably happen is someone at the State Department would say, I'm coming to visit, and they would put me in the system. When I arrive there they would authenticate me against my card and say, yes, let him in the building. The same thing with computers. The systems administrator needs to establish an account and say, yes, I have the ability to log on to that system and I use my card to authenticate who I am when I log on in the morning.

The other thing that has happened a little bit and this is sort of where smart cards have come from and as far as where I think they're going. I used to be one of those guys that carried around a piece of paper that said things you can do with a smart card, and it was scrape snow off your windshields, scrape mud off your boot, and try to open a door with it. The point of that is while we certainly had smart cards out there and they were not all that expensive to buy, if you didn't build the infrastructure to use them, you really didn't have a product that was worth much, and so the infrastructure costs and the enabling technologies are the ones that are the hard part to do because you must make a change in the way people do business and in their business processes.

When we first started dealing in this business, the reason people wanted smart cards was to carry data on them, and they wanted

to carry data because we had a lot of systems that were not interoperable within the Department. A good example was the Army's levelization processing, they used the card to carry on it when was your last dental exam, had you done a will, and had you had certain shots. The reason they did that is because all of those things were in computers, but they were in computers in different place on the base that didn't talk to each other. Putting that data on a card and being able to put the card in there gave the commander a quick picture of what this guy needed to do in order to be able to deploy. I would refer to that as a datacentric approach to smart cards.

What has happened over the last 5 or 6 years is people have begun rethinking the way they do business. Particularly in the Department as we've modernized our business processes. We're trying to get away from going to an office to fill out a form or to change tax withholding information and trying to make those things Web-enabled type of applications. If you're going to do Web-enabled business, you need to have something that authenticates you to the Web and allows you to digitally sign an action that is important like a tax withholding form or something like that.

A lot of the interest in the use of cards, particularly within DOD, has moved away from carrying a large amount of data around to more being an authenticator to systems that are now Web enabled and allow you to do business processes in a much more efficient way which will do away with the need to walk to an office and fill out a form.

Mr. PUTNAM. I think that you've outlined very eloquently where we're headed, which is that the technology is there today to have a miniature smart card replace the dog tag which could be swiped on the battlefield to let somebody know what their blood type is, that they're allergic to penicillin, that they received certain wounds at a different time or that they're diabetic. It would also enable them to access their computer when they're not on the battlefield or get into the installation. Is that not the case?

Mr. SCHEFLEN. I think that with the exception of the medical stuff, the real question is, when you're looking at what happens on a battlefield, is it realistic, to pull somebody's smart card out of his uniform and put it in a reader to check blood type? In fact, that is not the way they do that kind of medicine at the frontline. People are triaged and evacuated back to rear echelons. Generally, if that happens quickly enough, by the time they get back they have connectivity back to the main data bases.

I'm not sure of the medical one and the medical people are one of the communities within DOD which have the potential for large amounts of storage requirements. They have been refining it over a period of years, and we still don't really have a complete version of what the medical folks would like to install on the card. It's largely been defined as sometimes people are—they're deployed in Iraq and they're away from all the systems that would normally keep track of what immunizations they have. The card might be a temporary carrier of information on treatment until they get back into, you know, the communications end where that information will be uploaded back to the rest of their automated medical records.

By and large, you have it right. We see it as a device that will be used to swipe, to manifest an airplane, to go through food services, to change your allotments remotely. If you think about it, to a certain extent, it's almost like it's e-commerce within the Defense Department. We don't do a lot of government-to-citizen transactions, because most of the people are somehow captive to us. But most of the other departments think of it as government-to-citizen and to a certain extent our citizens are the military members, the retirees, and their dependents. What we're trying to do is give them a way of doing e-business with the Defense Department.

Mr. PUTNAM. OK. Well, let's take it from a different side. If you disregard or if you set aside the datacentric approach, and you focus on the access, this is not just DOD, it is governmentwide, you can go to a Super 8 Motel and get a card that lets you in room 208, but not 210. It lets you charge your lunch downstairs, it lets you build a minibar for your specific account, and at midnight, the day you're supposed to check out, or 11 a.m., it's worthless. And you could leave it in the room, you could throw it on the ground, you could hand it to someone on the sidewalk, and its of no value to that person. And that's a very smart technology.

So what is our impediment to employ smart cards if our focus, as has largely been stated here, is access control for physical security and access control for information security? Why don't we have something that works for frontline special security administration workers all around this country, of Forest Service firefighters or people who work in Federal buildings all around this country who don't have particularly complicated security clearances? They're really just interested in whether they have any business being in that particular building or accessing a particular file of a particular taxpayer who's coming in. Why is this so difficult?

Ms. BATES. Mr. Chairman, I certainly can't address why is it necessarily so difficult, but I think that you've identified that the technology is there. So we're not necessarily talking about the technology problem, as great strides have been made in interoperability and standards.

As my colleague also mentioned, we're now talking about culture change, and there are some barriers. There are those that say that the culture change or the change process should be well along before the technology is introduced, because the technology cannot change the culture by itself. Whether it be a common access into buildings where—as he spoke about the guards, perhaps prefer something else, or getting all agencies to agree that these are the minimum set of criteria we will all recognize to be on a card for building access. I've experienced going to cities where a different ID card for building access is required for each building. So an agency that occupies several buildings within a city will not even have the same ID card that looks the same.

Certainly the technology's there, but there are costs associated with the technology which need to be budgeted and planned for, but it is a gaining acceptance, and, as stated in the GAO report in your opening comments, getting top management support to say, OK, we're going to do this, and making it a priority, it's a difficult task.

Mr. PUTNAM. You're the chairman of that committee, right, the Federal Identity?

Ms. BATES. It's my organization. We have the chair of the e-Governorship, e-authentication, and are working on the Federal Credentialing Committee, yes.

Mr. PUTNAM. You seem like a very determined woman. I have no doubt that you will get these cultures changed. It's absurd. This is totally absurd. We hear that all of you are in agreement that the technology exists to do this, and all of you are in agreement, I think, that culture is the biggest impediment. And so we have these agencies with different cards, different access, within the same city, and different mindsets where we can't stand to just see, touch and feel that plastic card that's dangling from everyone's neck.

So there's a hearing on funding, a hearing on the technology of emerging biometrics and smart-card technology. All of that is really just an academic exercise is what I'm hearing, because it doesn't matter. The secretaries, they've got other things to worry about, the assistant secretaries, the deputy under assistant secretary to the deputy underling, they have other things to do, and so this is all for naught. That's really what I'm hearing.

Let me throw something else out: The access control, the identity authentication for facilities, is one of the purposes behind this push for smart-card technology. The second major push, as I understand it, and correct me if I'm wrong, is access to computers.

Now, the Navy has 67 different payroll systems, or whatever it is that we've heard before, 10,000 legacy systems. Everybody buys whatever flavor-of-the-month computer system that particular office in that particular agency in that particular city feels like meets their needs. So regardless of all of your hard work on standardizing interoperability of smart cards, does it really ever get off the ground until we have true interoperability of the tens of thousands of systems that are in the Federal Government, or are we going to have to build the access infrastructure for each one of these legacy systems so that the smart card actually gets you into the program that you need to get into? Can we do one without the other?

Mr. Wu.

Mr. WU. Well, if that's your underlying goal is to be able to have somebody from the east coast tap onto a system that controls operations in the west coast, you do need to have some sort of interoperability of systems, and smart card will only get you the access as you pointed out. So, if that is your underlying goal, then interoperability of systems, which is another issue that NIST is working on as well, working with the IT industry, that is something that needs to be looked at.

Mr. SCHEFLEN. Mr. Chairman, I don't think that's quite as dire or as unpromising as maybe the picture you painted. Basically, if we look at where the smart card industry was 3 or 4 years ago, it was the University of Florida model you described. You had deployed campus systems that were really proprietary to a particular vendor. If you looked at that particular system, you would find that the same vendor made the readers, the cards, and ran the LAN information that tracked everything down. Right after September 11 we saw the vendors out there that did produce various systems to

protect bases or facilities have a field day trying to sell their systems to everybody that felt they had need to protect it, and, of course, had that gone forward, we would have ended up with systems that were completely proprietary to every base or building.

What happened with the GSA contract and with the standards over 3 years, we basically said to the industry, we're not going to play that game anymore. It would be the equivalent of you saying, I need some floppies for my computer, and going to the computer store and saying, what kind of floppy drive do you have for your computer, because you need these cards or these cards or these cards, depending on which one you have or what kind of software you're running, so I can sell you a different product.

That's the way the industry was, and working with the GSA and NIST and lots of others in the government, we said we're not going to play that game; that we're going to buy cards. We're going to say we want a 64K card that has these characteristics, and, you know, we want to buy from the low bidder that meets the spec, not one that has a proprietary problem, because we have those kinds of readers. We did the same thing with readers, and we're trying to do the same thing with middleware.

So what we've tried to do is change industry so that anybody who uses the products that are sold through the GSA contracts and evaluated by NIST will really be interoperable, and I think that we are moving in that direction. We see far fewer of these closed proprietary systems that are characterized as the campus systems. That had been the only success story of smart cards in the United States. It's not been a great story here. It's been more of a European success story.

I think we are making progress, and I think that my colleagues at GSA and NIST are a large reason why the government is in a position to move forward now, and the things that they implement will be interoperable.

Having said that, it's still hard to do. There are cultural issues, and guards like to look at cards rather than have you put them in a computer and authenticate with a fingerprint. We actually have systems in DOD, one of them goes by the acronym of BIDS, Biometric Identification System, that uses the cards that we issue as ID credentials. At the gate, the cards are swiped, it prints up a photograph from the data base and also tells them whether the card is good. They can do a fingerprint check on a hand-held wireless device and authenticate who they're letting into the bases.

These kinds of things are happening, the interoperability is there, and I think that the government is moving in the right direction. I think the biggest problem is some of the things that they're thinking are so massive that they're almost unaffordable. If you say, we're going to give something to 30 million truck drivers, how do you do that and what kind of products do you use and——

Mr. PUTNAM. You do it every day with a driver's license. What's the marginal increase of cost to take today's driver's license, make it smart or add whatever component is necessary? What is the marginal cost of that on 30 million?

Mr. SCHEFLEN. Well, the driver's license people will talk about what it takes to do that. I think getting 50 States to agree is a problem, but the larger problem is the one my GAO colleague

talked about, which is how do you really know who you are giving a secure credential. I guess what I would look at is you're saying, I've got a very secure credential, and I'm going to biometrically bind the identity of the person to whom I'm giving it. Now, I've done that, and that's what we do in the DOD, but, without some assurance that the person who you have in front of you is really who he purports to be, and the problem there is with the feeder documents that are often counterfeited, to get various types of credentials, you may create a false sense of security, you know what I mean? We now have very securely bound a phony identity to this type of document.

Mr. PUTNAM. The CAC card.

Mr. SCHEFLEN. Yes, sir?

Mr. PUTNAM. Do you use it for computer access, or is it strictly for facility access?

Mr. SCHEFLEN. No, sir. I use it but it's not sitting in my computer at the moment because it's around my neck. When I get back to my office, I will put it in a reader on my computer, and it'll ask me to enter my PIN number, and it will then allow me to log onto the system. If I am away from or if I don't use the system for about 5 minutes or 10 minutes, it'll go blank, and I'll have to reenter the PIN.

Because it's my ID card when I leave my office, I need to take it out. That locks my system down; nobody else can use it. It's really interesting. Most security computer people who have come in and evaluated computer security say that the weakest link is usually passwords; people give them to others, they write them down, they have them on their desk, and they often break systems doing that. This is an attempt to, not to eliminate a password because you still have a password in a sense because you have a PIN, but you really require two things: you require the PIN and the——

Mr. PUTNAM. If a plane crashes into your office in the Pentagon, can you put that card in another Defense computer and access all of the information?

Mr. SCHEFLEN. The answer to that, that's a theoretical yes. Depends on a lot of things.

Yes, other card readers will accept my credential. Obviously the system administrator for that particular system I'm on would have to authorize me to use it, and whether I could access my computer or not would depend on whether we have remote access facilities set up. The answer to that, I think, is that it certainly is possible, and there are a lot of companies that are thinking about virtual offices, where they go with a thin client, what's called a thin client type of approach, where most of the information is not stored on my desktop, but on a server somewhere. And I can access that wherever I am by simply authenticating to that server, and that's, I think, the kind of model you're talking about.

Mr. PUTNAM. That is. I mean, if you're at Pearl Harbor, and then your next tour is in Germany——

Mr. SCHEFLEN. Right.

Mr. PUTNAM [continuing]. How much effort is required to allow you access at your new posting on your new tour, and does it require a new card, does it just require a few keystrokes of updating your current card? If you change billet and you go from naval pub-

lic affairs to naval financial management, do you have to get a new card? Does it require just a few keystrokes to allow you access to the new items that you are now allowed to view and shut down the items that are no longer appropriate for you to access?

Other than getting in the front door and allowing us to have a better connection between the person entering and who they actually are with some biometric identifier, are we not shortchanging the potential of smart-card technology?

Mr. SCHEFLEN. No. I think, if anything, the emphasis in Defense has probably been more on the IT side than it has been on the getting in the front door side for a lot of the reasons that GAO described, the cultural difficulties. It is really a large focus on the getting onto the systems and accessing Web sites where I do business. That is more the current usage of the card than even physical access.

Now, keep in mind that in the case of DOD, this ID card also is a Geneva Convention card that has to have certain information when people go into a war zone, that's different than a physical access card. It is an ID card as well.

I think that, in answer to how much has to happen if you change jobs, a little bit of that is the business process of the components in terms of how they want to do that, but by and large unless you went from one component to the other because your visual certificates would have to change, and if you're a civilian and went to work for the Army and went to work for the Navy, for example, you would get a new ID card. If you changed jobs within the Army, there wouldn't be a need to do that.

Mr. PUTNAM. Ms. Bates.

Mr. SCHEFLEN. Well, military side is a little more complex, but normally people don't change components. If you changed your e-mail address because you could be reassigned—i.e., an Army guy could be assigned to a defense agency where his PKI credentials may need to be different, and so he would have to go back but wouldn't necessarily need a new card. He could have new certs put on the card.

Mr. PUTNAM. OK. Well, let's switch to the civilian side——

Mr. SCHEFLEN. OK.

Mr. PUTNAM [continuing]. Because that would be a good lick, too, if we could just fix that.

Someone who lives outside of Washington, DC, works for one of the many agencies that accesses documents about private information about American citizens, with IRS, Social Security, HUD, Health and Human Services, generally stay there a while, live in the same city, work in the same building, what are we really trying to accomplish with the smart card, and what are the barriers to the plan in that type of situation?

Ms. BATES. I can speak generally and not specifically about each agency because each agency may have their own program going, but——

Mr. PUTNAM. Well, but we'll change that, right?

Ms. BATES. Right. Right.

Mr. PUTNAM. We're not going to be able to say that much longer, I hope.

Ms. BATES. And that'll be good. That'll be good.

I think given that we're not the Defense Department, and other agencies are independent, if we take it incrementally, perhaps in groups of steps, of you start with a common identification card where your badge or your ID card, which is part of a smart card, that they are all alike or have common fields. This is what we're trying to implement—GSA is implementing in New York City, which I referenced earlier; in the three buildings with the tenant agencies, have agreed that the badges look the same, and they are. Everybody entering those buildings goes through the contact, the scanner, and you get that acceptance. You can begin to add other elements to those cards, whether it's the computer system access or whether it is the purchase card or the other elements, but having it be against the same set of standards, an agreement that this is what all the cards are going to have, a minimum capability.

You can then—as Mr. Wu stated, have people who are in position to say, OK, I, Sandra Bates, have authorized this, this, and this; you have to have that, but at least you have the common card. That would lead to some group purchasing where you can say, OK, we're going to do X amount, we're going to purchase the cards and the readers in bulk, and leverage the government's buying power. That would achieve savings and also give some central oversight against a set of companies that have been predetermined. If you have the top down support and then the methodology outlined to implement, you can move forward, but you do it incrementally.

I think that each agency will always have some unique requirements, and that's OK, but they should be able to be accommodated. If we could establish a base line, for example to get into certain types of buildings let's say, everybody has to do X, and you agree on it—here again I'm not talking about a technology problem. It is a management and implementation issue, one that certainly could be resolved, and I think that if we had a governmentwide policy that said this is what we're going to do, and then we leverage the government's buying power and implement, whether it be across all Federal buildings or Federal installations.

The other area that would be addressed in all of this, and I think we've alluded to it, and I've said it outside this room, culture. The people who are doing IT security are very well attuned today about cybersecurity and generally have a technical background. They are the keepers, and the users have been indoctrinated so that they understand they need security.

On the physical access side, it's a different group of people. It's managed separately, and the expectations are different on the part of the people who manage it and on the part of people of what is required to come into a building. The same person can have different expectations to their computer security versus their physical security, but I think we need to pull that together and manage it as one. And we've had that—those are the things as we move toward success.

Maybe you would still be frustrated as to say this is not moving fast enough, but an initiative that allowed for an incremental approach where you moved quickly incrementally rather than one big, you know, throw the Hail Mary pass, I think government responds better to incremental approaches.

Mr. PUTNAM. Thank you all very much.

Mr. Willemssen.

Mr. WILLEMSSEN. I wanted to add something to an item you mentioned before, Mr. Chairman, and you had talked about all of us possibly agreeing that culture was the biggest impediment.

What I would say is that top management commitment and sustaining that commitment is the largest impediment, and consistent with our prior recommendation, as I mentioned, OMB did come out with that July memo laying out a policy framework.

I think the next step, in terms of your concern about what's holding us up, is looking at the Federal Identity and Credentialing Committee. They obviously have a mission now, and that's to come up with a common policy for credentialing Federal employees. So how are they going to achieve that mission, and when are they going to do it? What are the tasks and milestones associated with that? And I think to the extent you can get an answer to that question, then you're that much closer to knowing when these barriers are going to be overcome.

Mr. PUTNAM. Thank you very much.

Mr. Wu, did you have a final comment?

Mr. WU. As we conclude today's hearing, or at least this panel, I just wanted to note that you raised some very strong issues. And certainly the Federal Government has certain unique needs and requirements, but as we move forward to try to seek solutions and try to achieve the goals that you would like, I would urge that you also include the industry voice, because as we try to take into account this change in culture, we need to have customer acceptance, customer confidence, and if we allow the industry to do that as it promulgates itself internationally and domestically, I think that'll be best, because trying to achieve a market-driven solution would be the ultimate scenario that would be successful for all of us.

Mr. PUTNAM. Thank you all very much. We appreciate the contributions of panel one. If you can, I'd encourage you to stay for panel two and listen to some of the private sector comments, that industry voice Mr. Wu referred to. And, with that, we will recess for about a minute and a half while panel one dismisses itself and panel two is seated.

[Recess.]

Mr. PUTNAM. If you all are ready, I'll swear you all in.

[Witnesses sworn.]

Mr. PUTNAM. Note, for the record, all the witnesses responded in the affirmative.

I'd like to welcome panel two of this hearing and appreciate your participation in this important topic. Our second panel of witnesses includes three distinguished individuals. Mr. Keith Rhodes is our first witness. He joined the General Accounting Office in 1991. He is currently the chief technologist at the Center for Technology and Engineering, where he has contributed to a variety of technically complex reports and testimony. Before holding this position, Mr. Rhodes was the Technical Director in GAO's Office of the Chief Scientist for Computers and Telecommunications. As Technical Director he provided assistance throughout GAO for issues relating to computer and telecom technology.

Welcome to the subcommittee. You're recognized for 5 minutes.

STATEMENT OF KEITH RHODES, CHIEF TECHNOLOGIST, GENERAL ACCOUNTING OFFICE

Mr. RHODES. Thank you Mr. Chairman.

I have my statement which I would submit for the record. Thank you.

Mr. Chairman and members of the subcommittee, I appreciate the opportunity to participate in today's hearing on the use of smart cards and biometrics in the Federal Government. A holistic security program includes three integral concepts: protection, detection and reaction. To provide protection of assets, such as physical buildings, information systems at our national border, a primary function is to control people into or out of protected areas. People are identified by three basic means: By something they know, something they have, or something they are.

As you've already heard, smart cards can have secure identification documents, something that people have. Biometrics can automate the identification of people by one or more of their distinct physical or behavioral characteristics, something that people are. The use of these technologies in combination can help provide more security than the use of these technologies in isolation.

Last year we completed a large body of work that assessed the use of biometrics for border security. In that report we discussed the current maturity of several biometric technologies, the possible implementation of these technologies in current border control policies, and the policy considerations and key considerations of using these technologies. While we examined the use of biometrics in a specific border control context, many of the issues that we identified apply to the use of biometrics for any security system, which I will address in my remarks today.

Biometric technologies vary in complexity, capability and performance. They are essentially pattern recognition devices that use cameras and scanning devices to capture images and measurements of a person's characteristics and store them for future comparisons. The first step in a biometric system is enrollment, when a person first presents their biometric and an identifier, and the system is trained to recognize that person. After enrollment biometric systems can be used to either verify a person's identity, conducting a one-to-one match, or to identify a person out of a data base, conducting a one-to-many match.

In my prepared statement we briefly discuss certain leading biometric technologies, including fingerprint recognition, facial recognition, iris recognition and hand geometry. Our technology assessment report provides more detail on each of these. However, it's important to realize that no biometric technology is perfect. Even more mature technology such as fingerprint recognition are not 100 percent accurate.

Systems sometimes falsely match an unauthorized person with a legitimate biometric identity in a data base. Other times a system fails to make a match and rejects a legitimate person. These error rates are inversely related and must be assessed in tandem. Acceptable risk levels must be balanced with the disadvantages of inconvenience. Different applications can tolerate different levels of risk.

Also, not all people will be able to enroll in a biometric system; for example, the fingerprints of people who work extensively at manual labor are often too worn to be captured.

Better technology offerings can minimize these error rates, but no product can completely eliminate these errors. These limitations of biometric technology need to be considered in the development of any security program using biometrics.

Biometric technology has been used in several Federal applications, including access control to buildings and computers, criminal identification, and border security. In the last 2 years, laws have been passed that will require a more extensive use of biometric technologies in the Federal Government for border and transportation security. Biometric technologies are available today. They can be used in security systems to help protect assets.

However, it is important to bear in mind that effective security cannot be achieved by relying on technology alone. Technology and people must work together as part of an overall security process. Weaknesses in any of these areas diminishes the effectiveness of the security process. Poorly defined security processes or insufficiently trained people can diminish the effectiveness of any security technology.

We have found that three key considerations need to be addressed before a decision is made to design, develop, and implement biometrics into a security system. One, decisions must be made on how the technology will be used. Two, a detailed cost-benefit analysis must be conducted to determine that the benefits gained from a system outweigh the costs. Three, a tradeoff analysis must be conducted between the increased security, which the use of biometrics would provide, and the effect on areas such as privacy and convenience.

Security concerns need to be balanced with practical costs and operational considerations as well as political and economic interests. A risk-management approach can help Federal agencies identify and address security concerns. A risk management approach helps agencies define and analyze the assets that need to be protected, the threats to those assets, the security vulnerabilities that could be exploited by adversaries, security priorities, and appropriate countermeasures.

As Federal agencies consider the development of security systems with biometrics, they need to define what the high-level goals of this system would be and develop a concept of operations that would embody the people, processes and technologies required to achieve these goals. With these answers, the proper role of biometric technology in security can be determined.

Mr. Chairman, that concludes my statement. I would be pleased to answer any questions that you may have.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Rhodes follows:]

United States General Accounting Office

GAO

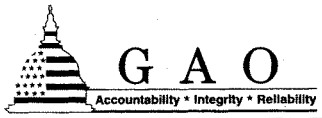
Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives

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

INFORMATION SECURITY

Challenges in Using Biometrics

Statement of Keith A Rhodes
Chief Technologist
Applied Research and Methods



GAO-03-1137T

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-1137T, a testimony for the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives

Why GAO Did This Study

One of the primary functions of any security system is the control of people into or out of protected areas, such as physical buildings, information systems, and our national border. Technologies called biometrics can automate the identification of people by one or more of their distinct physical or behavioral characteristics. The term biometrics covers a wide range of technologies that can be used to verify identity by measuring and analyzing human characteristics – relying on attributes of the individual instead of things the individual may have or know. In the last 2 years, laws have been passed that will require a more extensive use of biometric technologies in the federal government.

Last year, GAO conducted a technology assessment on the use of biometrics for border security. GAO was asked to testify about the issues that it raised in the report, the use of biometrics in the federal government, and the current state of the technology.

www.gao.gov/cgi-bin/getrpt?GAO-03-1137T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Keith Rhodes at (202) 512-6412 or rhodesk@gao.gov.

September 9, 2003

INFORMATION SECURITY

Challenges in Using Biometrics

What GAO Found

Biometric technologies are available today that can be used in security systems to help protect assets. Biometric technologies vary in complexity, capabilities, and performance and can be used to verify or establish a person's identity. Leading biometric technologies include facial recognition, fingerprint recognition, hand geometry, iris recognition, retina recognition, signature recognition, and speaker recognition. Biometric technologies have been used in federal applications such as access control, criminal identification, and border security.

However, it is important to bear in mind that effective security cannot be achieved by relying on technology alone. Technology and people must work together as part of an overall security process. Weaknesses in any of these areas diminishes the effectiveness of the security process. The security process needs to account for limitations in biometric technology. For example, some people cannot enroll in a biometrics system. Similarly, errors sometimes occur during matching operations. Procedures need to be developed to handle these situations. Exception processing that is not as good as biometric-based primary processing could also be exploited as a security hole.

We have found that three key considerations need to be addressed before a decision is made to design, develop, and implement biometrics into a security system:

1. Decisions must be made on how the technology will be used.
2. A detailed cost-benefit analysis must be conducted to determine that the benefits gained from a system outweigh the costs.
3. A trade-off analysis must be conducted between the increased security, which the use of biometrics would provide, and the effect on areas such as privacy and convenience.

Security concerns need to be balanced with practical cost and operational considerations as well as political and economic interests. A risk management approach can help federal agencies identify and address security concerns. As federal agencies consider the development of security systems with biometrics, they need to define what the high-level goals of this system will be and develop the concept of operations that will embody the people, process, and technologies required to achieve these goals. With these answers, the proper role of biometric technologies in security can be determined. If these details are not resolved, the estimated cost and performance of the resulting system will be at risk.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing on the use of smart cards and biometrics in the federal government. One of the primary functions of any security system is the control of people into or out of protected areas, such as physical buildings, information systems, and our national border. People are identified by three basic means: by something they know, something they have, or something they are. People and systems regularly use these means to identify people in everyday life. For example, members of a community routinely recognize one another by how they look or how their voices sound—by something they are. Automated teller machines (ATM) recognize customers from their presentation of a bank card—something they have—and their entering a personal identification number (PIN)—something they know. Using keys to enter a locked building is another example of using something you have. More secure systems may combine two or more of these approaches.

Technologies called biometrics can automate the identification of people by one or more of their distinct physical or behavioral characteristics. The term biometrics covers a wide range of technologies that can be used to verify identity by measuring and analyzing human characteristics—relying on attributes of the individual instead of things the individual may have or know.

As requested, I will provide an overview of biometric technologies that are currently available, describe some of the current uses of these technologies, and discuss the issues and challenges associated with the implementation of biometrics. My testimony today is based on a body of work we completed last year examining the use of biometrics for border control. In that report, we discussed the current maturity of several biometric technologies, the possible implementation of these technologies in current border control processes, and the policy implications and key considerations for using these technologies.[1] We performed our work in accordance with generally accepted government auditing standards.

[1]U.S. General Accounting Office, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

Biometric Technologies for Personal Identification

When used for personal identification, biometric technologies measure and analyze human physiological and behavioral characteristics. Identifying a person's physiological characteristics is based on direct measurement of a part of the body—fingertips, hand geometry, facial geometry, and eye retinas and irises. The corresponding biometric technologies are fingerprint recognition, hand geometry, and facial, retina, and iris recognition. Identifying behavioral characteristics is based on data derived from actions, such as speech and signature, the corresponding biometrics being speaker recognition and signature recognition.

Biometrics can theoretically be very effective personal identifiers because the characteristics they measure are thought to be distinct to each person. Unlike conventional identification methods that use something you have, such as an identification card to gain access to a building, or something you know, such as a password to log on to a computer system, these characteristics are integral to something you are. Because they are tightly bound to an individual, they are more reliable, cannot be forgotten, and are less easily lost, stolen, or guessed.

How Biometric Technologies Work

Biometric technologies vary in complexity, capabilities, and performance, but all share several elements. Biometric identification systems are essentially pattern recognition systems. They use acquisition devices such as cameras and scanning devices to capture images, recordings, or measurements of an individual's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics. Because the process is automated, biometric decision-making is generally very fast, in most cases taking only a few seconds in real time.

Depending on the application, biometric systems can be used in one of two modes: verification or identification. Verification—also called authentication—is used to verify a person's identity—that is, to authenticate that individuals are who they say they are. Identification is used to establish a person's identity—that is, to determine who a person is. Although biometric technologies measure different characteristics in substantially different ways, all biometric systems involve similar processes that can be divided into two distinct stages: enrollment and verification or identification.

Enrollment

In enrollment, a biometric system is trained to identify a specific person. The person first provides an identifier, such as an identity card. The biometric is linked to the identity specified on the identification document. He or she then presents the biometric (e.g., fingertips, hand, or iris) to an acquisition device. The distinctive features are located and one or more

samples are extracted, encoded, and stored as a reference template for future comparisons. Depending on the technology, the biometric sample may be collected as an image, a recording, or a record of related dynamic measurements. How biometric systems extract features and encode and store information in the template is based on the system vendor's proprietary algorithms. Template size varies depending on the vendor and the technology. Templates can be stored remotely in a central database or within a biometric reader device itself; their small size also allows for storage on smart cards or tokens.

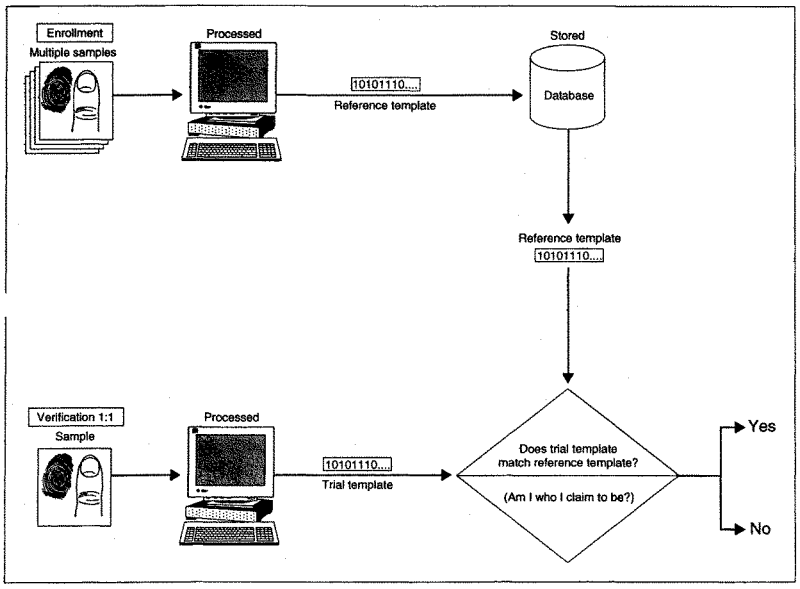
Minute changes in positioning, distance, pressure, environment, and other factors influence the generation of a template, making each template likely to be unique, each time an individual's biometric data are captured and a new template is generated. Consequently, depending on the biometric system, a person may need to present biometric data several times in order to enroll. Either the reference template may then represent an amalgam of the captured data or several enrollment templates may be stored. The quality of the template or templates is critical in the overall success of the biometric application. Because biometric features can change over time, people may have to reenroll to update their reference template. Some technologies can update the reference template during matching operations.

The enrollment process also depends on the quality of the identifier the enrollee presents. The reference template is linked to the identity specified on the identification document. If the identification document does not specify the individual's true identity, the reference template will be linked to a false identity.

Verification

In verification systems, the step after enrollment is to verify that a person is who he or she claims to be (i.e., the person who enrolled). After the individual provides whatever identifier he or she enrolled with, the biometric is presented, which the biometric system captures, generating a trial template that is based on the vendor's algorithm. The system then compares the trial biometric template with this person's reference template, which was stored in the system during enrollment, to determine whether the individual's trial and stored templates match (see figure 1).

Figure 1: The Biometric Verification Process



Source: GAO.

Verification is often referred to as 1:1 (one-to-one) matching. Verification systems can contain databases ranging from dozens to millions of enrolled templates but are always predicated on matching an individual's presented biometric against his or her reference template. Nearly all verification systems can render a match–no-match decision in less than a second. A system that requires employees to authenticate their claimed identities before granting them access to secure buildings or to computers is a verification application.

Identification

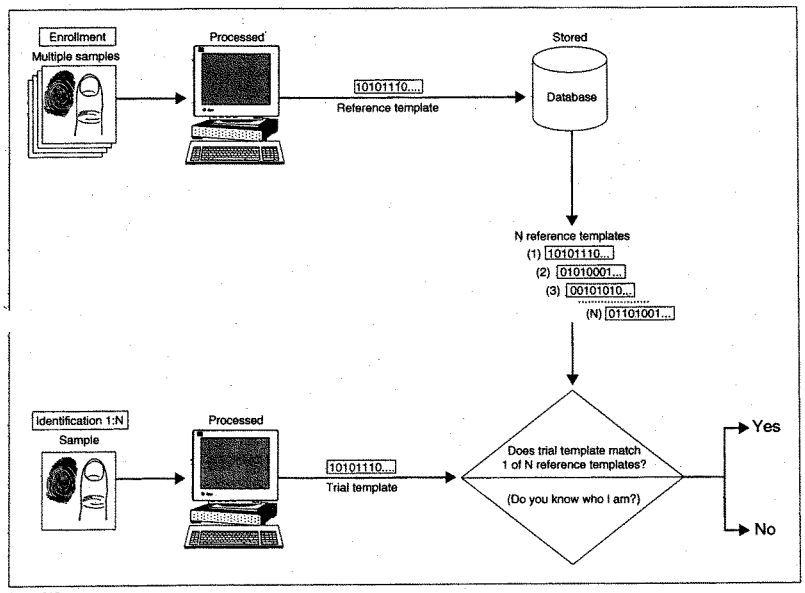
In identification systems, the step after enrollment is to identify who the person is. Unlike verification systems, no identifier need be provided. To find a match, instead of locating and comparing the person's reference template against his or her presented biometric, the trial template is compared against the stored reference templates of all individuals enrolled in the system (see figure 2). Identification systems are referred to as 1:*N* (one-to-N, or one-to-many) matching because an individual's biometric is compared against multiple biometric templates in the system's database.

There are two types of identification systems: positive and negative. Positive identification systems are designed to ensure that an individual's biometric is enrolled in the database. The anticipated result of a search is a match. A typical positive identification system controls access to a secure building or secure computer by checking anyone who seeks access against a database of enrolled employees. The goal is to determine whether a person seeking access can be identified as having been enrolled in the system.

Negative identification systems are designed to ensure that a person's biometric information is not present in a database. The anticipated result of a search is a nonmatch. Comparing a person's biometric information against a database of all who are registered in a public benefits program, for example, can ensure that this person is not "double dipping" by using fraudulent documentation to register under multiple identities.

Another type of negative identification system is a surveillance system that uses a watch list. Such systems are designed to identify people on the watch list and alert authorities for appropriate action. For all other people, the system is to check that they are not on the watch list and allow them normal passage. The people whose biometrics are in the database in these systems may not have provided them voluntarily. For instance, for a surveillance system, the biometrics may be faces captured from mug shots provided by a law enforcement agency.

Figure 2: The Biometric Identification Process



Source: GAO.

No match is ever perfect in either a verification or an identification system, because every time a biometric is captured, the template is likely to be unique. Therefore, biometric systems can be configured to make a match or no-match decision, based on a predefined number, referred to as a threshold, that establishes the acceptable degree of similarity between the trial template and the enrolled reference template. After the comparison, a score representing the degree of similarity is generated, and this score is compared to the threshold to make a match or no-match decision. Depending on the setting of the threshold in identification

systems, sometimes several reference templates can be considered matches to the trial template, with the better scores corresponding to better matches.

Leading Biometric Technologies

A growing number of biometric technologies have been proposed over the past several years, but only in the past 5 years have the leading ones become more widely deployed. Some technologies are better suited to specific applications than others, and some are more acceptable to users. We describe seven leading biometric technologies:

- Facial Recognition
- Fingerprint Recognition
- Hand Geometry
- Iris Recognition
- Retina Recognition
- Signature Recognition
- Speaker Recognition

Facial Recognition

Facial recognition technology identifies people by analyzing features of the face not easily altered—the upper outlines of the eye sockets, the areas around the cheekbones, and the sides of the mouth. The technology is typically used to compare a live facial scan to a stored template, but it can also be used in comparing static images such as digitized passport photographs. Facial recognition can be used in both verification and identification systems. In addition, because facial images can be captured from video cameras, facial recognition is the only biometric that can be used for surveillance purposes.

Fingerprint Recognition

Fingerprint recognition is one of the best known and most widely used biometric technologies. Automated systems have been commercially available since the early 1970s, and at the time of our study, we found there were more than 75 fingerprint recognition technology companies. Until recently, fingerprint recognition was used primarily in law enforcement applications.

Fingerprint recognition technology extracts features from impressions made by the distinct ridges on the fingertips. The fingerprints can be either flat or rolled. A flat print captures only an impression of the central area between the fingertip and the first knuckle; a rolled print captures ridges on both sides of the finger.

An image of the fingerprint is captured by a scanner, enhanced, and converted into a template. Scanner technologies can be optical, silicon, or

ultrasound technologies. Ultrasound, while potentially the most accurate, has not been demonstrated in widespread use. Last year, we found that optical scanners were the most commonly used. During enhancement, "noise" caused by such things as dirt, cuts, scars, and creases or dry, wet, or worn fingerprints is reduced, and the definition of the ridges is enhanced. Approximately 80 percent of vendors base their algorithms on the extraction of minutiae points relating to breaks in the ridges of the fingertips. Other algorithms are based on extracting ridge patterns.

Hand Geometry

Hand geometry systems have been in use for almost 30 years for access control to facilities ranging from nuclear power plants to day care centers. Hand geometry technology takes 96 measurements of the hand, including the width, height, and length of the fingers; distances between joints; and shapes of the knuckles.

Hand geometry systems use an optical camera and light-emitting diodes with mirrors and reflectors to capture two orthogonal two-dimensional images of the back and sides of the hand. Although the basic shape of an individual's hand remains relatively stable over his or her lifetime, natural and environmental factors can cause slight changes.

Iris Recognition

Iris recognition technology is based on the distinctly colored ring surrounding the pupil of the eye. Made from elastic connective tissue, the iris is a very rich source of biometric data, having approximately 266 distinctive characteristics. These include the trabecular meshwork, a tissue that gives the appearance of dividing the iris radially, with striations, rings, furrows, a corona, and freckles. Iris recognition technology uses about 173 of these distinctive characteristics. Formed during the 8th month of gestation, these characteristics reportedly remain stable throughout a person's lifetime, except in cases of injury. Iris recognition can be used in both verification and identification systems.

Iris recognition systems use a small, high-quality camera to capture a black and white, high-resolution image of the iris. The systems then define the boundaries of the iris, establish a coordinate system over the iris, and define the zones for analysis within the coordinate system.

Retina Recognition

Retina recognition technology captures and analyzes the patterns of blood vessels on the thin nerve on the back of the eyeball that processes light entering through the pupil. Retinal patterns are highly distinctive traits. Every eye has its own totally unique pattern of blood vessels; even the eyes of identical twins are distinct. Although each pattern normally remains stable over a person's lifetime, it can be affected by disease such

as glaucoma, diabetes, high blood pressure, and autoimmune deficiency syndrome.

The fact that the retina is small, internal, and difficult to measure makes capturing its image more difficult than most biometric technologies. An individual must position the eye very close to the lens of the retina-scan device, gaze directly into the lens, and remain perfectly still while focusing on a revolving light while a small camera scans the retina through the pupil. Any movement can interfere with the process and can require restarting. Enrollment can easily take more than a minute.

Signature Recognition

Signature recognition authenticates identity by measuring handwritten signatures. The signature is treated as a series of movements that contain unique biometric data, such as personal rhythm, acceleration, and pressure flow. Unlike electronic signature capture, which treats the signature as a graphic image, signature recognition technology measures how the signature is signed.

In a signature recognition system, a person signs his or her name on a digitized graphics tablet or personal digital assistant. The system analyzes signature dynamics such as speed, relative speed, stroke order, stroke count, and pressure. The technology can also track each person's natural signature fluctuations over time. The signature dynamics information is encrypted and compressed into a template.

Speaker Recognition

Differences in how different people's voices sound result from a combination of physiological differences in the shape of vocal tracts and learned speaking habits. Speaker recognition technology uses these differences to discriminate between speakers.

During enrollment, speaker recognition systems capture samples of a person's speech by having him or her speak some predetermined information into a microphone a number of times. This information, known as a passphrase, can be a piece of information such as a name, birth month, birth city, or favorite color or a sequence of numbers. Text independent systems are also available that recognize a speaker without using a predefined phrase. This phrase is converted from analog to digital format, and the distinctive vocal characteristics, such as pitch, cadence, and tone, are extracted, and a speaker model is established. A template is then generated and stored for future comparisons.

Speaker recognition can be used to verify a person's claimed identity or to identify a particular person. It is often used where voice is the only available biometric identifier, such as telephone and call centers.

Accuracy of Biometric Technology

Biometrics is a very young technology, having only recently reached the point at which basic matching performance can be acceptably deployed. It is necessary to analyze several metrics to determine the strengths and weaknesses of each technology and vendor for a given application.

The three key performance metrics are false match rate (FMR), false nonmatch rate (FNMR), and failure to enroll rate (FTER). A false match occurs when a system incorrectly matches an identity, and FMR is the probability of individuals being wrongly matched. In verification and positive identification systems, unauthorized people can be granted access to facilities or resources as the result of incorrect matches. In a negative identification system, the result of a false match may be to deny access. For example, if a new applicant to a public benefits program is falsely matched with a person previously enrolled in that program under another identity, the applicant may be denied access to benefits.

A false nonmatch occurs when a system rejects a valid identity, and FNMR is the probability of valid individuals being wrongly not matched. In verification and positive identification systems, people can be denied access to some facility or resource as the result of a system's failure to make a correct match. In negative identification systems, the result of a false nonmatch may be that a person is granted access to resources to which she should be denied. For example, if a person who has enrolled in a public benefits program under another identity is not correctly matched, she will succeed in gaining fraudulent access to benefits.

False matches may occur because there is a high degree of similarity between two individuals' characteristics. False nonmatches occur because there is not a sufficiently strong similarity between an individual's enrollment and trial templates, which could be caused by any number of conditions. For example, an individual's biometric data may have changed as a result of aging or injury. If biometric systems were perfect, both error rates would be zero. However, because biometric systems cannot identify individuals with 100 percent accuracy, a trade-off exists between the two.

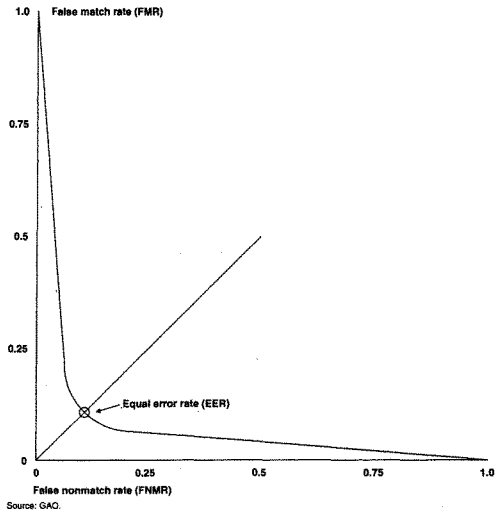
False match and nonmatch rates are inversely related; they must therefore always be assessed in tandem, and acceptable risk levels must be balanced with the disadvantages of inconvenience. For example, in access control, perfect security would require denying access to everyone. Conversely,

granting access to everyone would result in denying access to no one. Obviously, neither extreme is reasonable, and biometric systems must operate somewhere between the two.

For most applications, how much risk one is willing to tolerate is the overriding factor, which translates into determining the acceptable FMR. The greater the risk entailed by a false match, the lower the tolerable FMR. For example, an application that controlled access to a secure area would require that the FMR be set low, which would result in a high FNMR. However, an application that controlled access to a bank's ATM might have to sacrifice some degree of security and set a higher FMR (and hence a lower FNMR) to avoid the risk of irritating legitimate customers by wrongly rejecting them. As figure 3 shows, selecting a lower FMR increases the FNMR. Perfect security would require setting the FMR to 0, in which case the FNMR would be 1. At the other extreme, setting the FNMR to 0 would result in an FMR of 1.

Vendors often use equal error rate (EER), an additional metric derived from FMR and FNMR, to describe the accuracy of their biometric systems. EER refers to the point at which FMR equals FNMR. Setting a system's threshold at its EER will result in the probability that a person is falsely matched equaling the probability that a person is falsely not matched. However, this statistic tends to oversimplify the balance between FMR and FNMR, because in few real-world applications is the need for security identical to the need for convenience.

Figure 3: The General Relationship between FMR and FNMR



Source: GAO.

Note: Equal error rate is the point at which FMR equals FNMR.

FTER is a biometric system's third critical accuracy metric. FTER measures the probability that a person will be unable to enroll. Failure to enroll (FTE) may stem from an insufficiently distinctive biometric sample or from a system design that makes it difficult to provide consistent biometric data. The fingerprints of people who work extensively at manual labor are often too worn to be captured. A high percentage of people are unable to enroll in retina recognition systems because of the precision such systems require. People who are mute cannot use voice systems, and people lacking fingers or hands from congenital disease, surgery, or injury cannot use fingerprint or hand geometry systems. Although between 1 and 3 percent of the general public does not have the body part required for

using any one biometric system, they are normally not counted in a system's FTER.

Using Multiple Biometrics

Because biometric systems based solely on a single biometric may not always meet performance requirements, the development of systems that integrate two or more biometrics is emerging as a trend. Multiple biometrics could be two types of biometrics, such as combining facial and iris recognition. Multiple biometrics could also involve multiple instances of a single biometric, such as 1, 2, or 10 fingerprints, 2 hands, and 2 eyes. One prototype system integrates fingerprint and facial recognition technologies to improve identification. A commercially available system combines face, lip movement, and speaker recognition to control access to physical structures and small office computer networks. Depending on the application, both systems can operate for either verification or identification. Experimental results have demonstrated that the identities established by systems that use more than one biometric could be more reliable, be applied to large target populations, and improve response time.

Federal Applications of Biometric Technologies

Biometrics have been used in several federal applications including access control to facilities and computers, criminal identification, and border security. In the last 2 years, laws have been passed that will require a more extensive use of biometric technologies in the federal government.

Access Control

Biometric systems have long been used to complement or replace badges and keys in controlling access to entire facilities or specific areas within a facility. The entrances to more than half the nuclear power plants in the United States employ biometric hand geometry systems. Figure 4 illustrates the use of fingerprint recognition for physical access.

As noted in our technology assessment, recent reductions in the price of biometric hardware have spurred logical access control applications. Fingerprint, iris, and speaker recognition are replacing passwords to authenticate individuals accessing computers and networks. The Office of Legislative Counsel of the U.S. House of Representatives, for example, is using an iris recognition system to protect confidential files and working documents. Other federal agencies, including the Department of Defense, Department of Energy, and Department of Justice, as well as the intelligence community, are adopting similar technologies.

Figure 4: Using Fingerprint Recognition for Physical Access

Source: National Coordination Office for Information Technology Research and Development.

The Department of Homeland Security's Transportation Security Administration (TSA) is working to establish a systemwide common credential to be used across all transportation modes for all personnel requiring unescorted physical and/or logical access to secure areas of the national transportation system, such as airports, seaports, and railroad terminals. Called the Transportation Worker Identification Credential (TWIC), the program was developed in response to recent laws and will include the use of smart cards and biometrics to provide a positive match of a credential to a person for 10-15 million transportation workers across the United States.[2]

Criminal Identification

Fingerprint identification has been used in law enforcement over the past 100 years and has become the de facto international standard for positively identifying individuals. The Federal Bureau of Investigation (FBI) has been using fingerprint identification since 1928. The first fingerprint recognition systems were used in law enforcement about 4 decades ago.

The FBI's Integrated Automated Fingerprint Identification System (IAFIS) is an automated 10-fingerprint matching system that stores rolled fingerprints. The more than 40 million records in its criminal master file are connected electronically with all 50 states and some federal agencies.

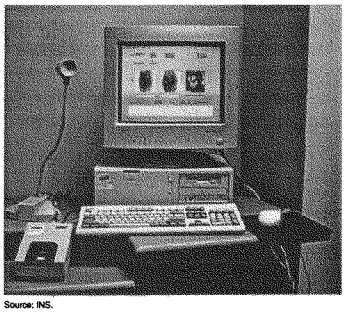
[2]See the *Aviation and Transportation Security Act* (Public Law 107-71, Nov. 19, 2001) and the *Maritime Transportation Security Act of 2002* (Public Law 107-295, Nov. 25, 2002).

IAFIS was designed to handle a large volume of fingerprint checks against a large database of fingerprints. Last year, we found that IAFIS processes, on average, approximately 48,000 fingerprints per day and has processed as many as 82,000 in a single day. IAFIS's target response time for criminal fingerprints submitted electronically is 2 hours; for civilian fingerprint background checks, 24 hours.

The Immigration and Naturalization Service (INS) began developing the Automated Biometric Fingerprint Identification System (IDENT) around 1990 to identify illegal aliens who are repeatedly apprehended trying to enter the United States illegally. INS's goal was to enroll virtually all apprehended aliens. IDENT can also identify aliens who have outstanding warrants or who have been deported. When such aliens are apprehended, a photograph and two index fingerprints are captured electronically and queried against three databases (see figure 5). IDENT has over 4.5 million entries. A fingerprint query of IDENT normally takes about 2 minutes. IDENT is also being used as a part of the National Security Entry-Exit Registration System (NSEERS) that was implemented last year.[3]

[3]Under NSEERS, certain nonimmigrants, who may pose a national security risk, are being registered, and are fingerprinted and photographed when they arrive in the United States. These nonimmigrants are required to periodically report and update, when changes occur, their registration information, and record their departure from the country.

Figure 5: An IDENT Workstation



Source: INS.

Border Security

INS Passenger Accelerated Service System (INSPASS), a pilot program in place since 1993, has more than 45,000 frequent fliers enrolled at nine airports, and has admitted more than 300,000 travelers. It is open to citizens of the United States, Canada, Bermuda, and visa waiver program countries who travel to the United States on business three or more times a year. INSPASS permits frequent travelers to circumvent customs procedures and immigration lines. To participate, users undergo a background screening and registration. Once enrolled, they can present their biometric at an airport kiosk for comparison against a template stored in a central database.

In a joint INS and State Department effort to comply with the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, every border crossing card issued after April 1, 1998, contains a biometric identifier and is machine-readable. The cards, also called laser visas, allow Mexican citizens to enter the United States for the purpose of business or pleasure without being issued further documentation and stay for 72 hours or less, going no farther than 25 miles from the border. Consular staff in Mexico photograph applicants and take prints of the two index fingers and then electronically forward applicants' data to INS. Both State and INS conduct checks on each applicant, and the fingerprints are compared with prints of previously enrolled individuals to ensure that the applicant is not

applying for multiple cards under different names. The cards store a holder's identifying information along with a digital image of his or her picture and the minutiae of the two index fingerprints. As of May 2002, State had issued more than 5 million cards.

The Department of State has been running pilots of facial recognition technology at 23 overseas consular posts for several years. As a visa applicant's information is entered into the local system at the posts and replicated in State's Consular Consolidated Database (CCD), the applicant's photograph is compared with the photographs of previous applicants stored in CCD to prevent fraudulent attempts to obtain visas. Some photographs are also being compared to a watch list.

Laws passed in the last 2 years require a more extensive use of biometrics for border control.[4] The Attorney General and the Secretary of State jointly, through the National Institute of Standards and Technology (NIST) are to develop a technology standard, including biometric identifier standards. When developed, this standard is to be used to verify the identity of persons applying for a U.S. visa for the purpose of conducting a background check, confirming identity, and ensuring that a person has not received a visa under a different name. By October 26, 2004, the Departments of State and Justice are to issue to aliens only machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers. At the same time, Justice is to install at all ports of entry equipment and software that allow the biometric comparison and authentication of all U.S. visas and other travel and entry documents issued to aliens and machine-readable passports. The Department of Homeland Security is developing the United States Visitor and Immigrant Status Indication Technology (US-VISIT) system to address this requirement.

Challenges and Issues in Using Biometrics

While biometric technology is currently available and used in a variety of applications, questions remain regarding the technical and operational effectiveness of biometric technologies in large-scale applications. We have found that a risk management approach can help define the need and use for biometrics for security. In addition, a decision to use biometrics

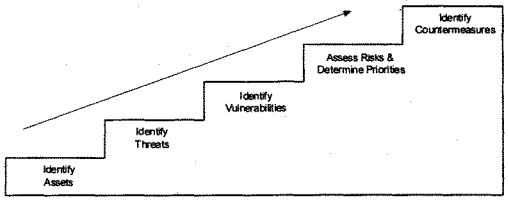
[4]See the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)* (Public Law 107-56, §403(c) and §414, Oct. 26, 2001) and the *Enhanced Border Security and Visa Entry Reform Act of 2002* (Public Law 107-173, May 14, 2002).

should consider the costs and benefits of such a system and its potential effect on convenience and privacy.

Risk Management Is the Foundation of Effective Strategy

The approach to good security is fundamentally similar, regardless of the assets being protected, whether information systems security, building security, or homeland security. As we have previously reported, these principles can be reduced to five basic steps that help to determine responses to five essential questions (see figure 6).[5]

Figure 6: Five Steps in the Risk Management Process



Source: GAO.

What Am I Protecting?

The first step in risk management is to identify assets that must be protected and the impact of their potential loss.

Who Are My Adversaries?

The second step is to identify and characterize the threat to these assets. The intent and capability of an adversary are the principal criteria for establishing the degree of threat to these assets.

[6]U.S. General Accounting Office, *National Preparedness: Technologies to Secure Federal Buildings*, GAO-02-687T (Washington, D.C.: Apr. 25, 2002).

How Am I Vulnerable?

Step three involves identifying and characterizing vulnerabilities that would allow identified threats to be realized. In other words, what weaknesses can allow a security breach?

What Are My Priorities?

In the fourth step, risk must be assessed and priorities determined for protecting assets. Risk assessment examines the potential for the loss or damage to an asset. Risk levels are established by assessing the impact of the loss or damage, threats to the asset, and vulnerabilities.

What Can I Do?

The final step is to identify countermeasures to reduce of eliminate risks. In doing so, the advantages and benefits of these countermeasures must also be weighed against their disadvantages and costs.

Protection, Detection, and Reaction Are Integral Security Concepts

Countermeasures identified through the risk management process support the three integral concepts of a holistic security program: protection, detection, and reaction. Protection provides countermeasures such as policies, procedures, and technical controls to defend against attacks on the assets being protected. Detection monitors for potential breakdowns in protective mechanisms that could result in security breaches. Reaction, which requires human involvement, responds to detected breaches to thwart attacks before damage can be done. Because absolute protection is impossible to achieve, a security program that does not incorporate detection and reaction is incomplete.

Biometrics can support the protection component of a security program. It is important to realize that deploying them will not automatically eliminate all security risks. Technology is not a solution in isolation. Effective security also entails having a well-trained staff to follow and enforce policies and procedures. Weaknesses in the security process or failures by people to operate the technology or implement the security process can diminish the effectiveness of technology.

Furthermore, there is a need for the security process to account for limitations in technology. Biometrics can help ensure that people can only enroll into a security system once and to ensure that a person presenting himself before the security system is the same person that enrolled into the system. However, biometrics cannot necessarily link a person to his or

her true identity. While biometrics would make it more difficult for people to establish multiple identities, if the one identity a person claimed were not his or her true identity, then the person would be linked to the false identity in the biometric system. The quality of the identifier presented during the enrollment process is key to the integrity of a biometrics system.

Procedures for exception processing would also need to be carefully planned. As we described, not all people can enroll in a biometrics system. Similarly, false matches and false nonmatches will also sometimes occur. Procedures need to be developed to handle these situations. Exception processing that is not as good as biometric-based primary processing could be exploited as a security hole.

Deciding to Use Biometric Technology

A decision to use biometrics in a security solution should also consider the benefits and costs of the system and the potential effects on convenience and privacy.

Weighing Costs and Benefits

Best practices for information technology investment dictate that prior to making any significant project investment, the benefit and cost information of the system should be analyzed and assessed in detail. A business case should be developed that identifies the organizational needs for the project and a clear statement of high-level system goals should be developed. The high-level goals should address the system's expected outcomes such as the binding of a biometric feature to an identity or the identification of undesirable individuals on a watch list. Certain performance parameters should also be specified such as the time required to verify a person's identity or the maximum population that the system must handle.

Once the system parameters are developed, a cost estimate can be developed. Not only must the costs of the technology be considered, but also the costs of the effects on people and processes. Both initial costs and recurring costs need to be estimated. Initial costs need to account for the engineering efforts to design, develop, test, and implement the system; training of personnel; hardware and software costs; network infrastructure improvements; and additional facilities required to enroll people into the biometric system. Recurring cost elements include program management costs, hardware and software maintenance, hardware replacement costs, training of personnel, additional personnel to enroll or verify the identities of people in the biometric system, and possibly the issuance of token cards for the storage of biometrics.

Weighed against these costs are the security benefits that accrue from the system. Analyzing this cost-benefit trade-off is crucial when choosing specific biometrics-based solutions. The consequences of performance issues—for example, accuracy problems, and their effect on processes and people—are also important in selecting a biometrics solution.

Effects on Privacy and Convenience

The Privacy Act of 1974 limits federal agencies' collection, use, and disclosure of personal information, such as fingerprints and photographs.[6] Accordingly, the Privacy Act generally covers federal agency use of personal biometric information. However, the act includes exemptions for law enforcement and national security purposes. Representatives of civil liberties groups and privacy experts have expressed concerns regarding (1) the adequacy of protections for security, data sharing, identity theft, and other identified uses of biometric data and (2) secondary uses and "function creep." These concerns relate to the adequacy of protections under current law for large-scale data handling in a biometric system. Besides information security, concern was voiced about an absence of clear criteria for governing data sharing. The broad exemptions of the Privacy Act, for example, provide no guidance on the extent of the appropriate uses law enforcement may make of biometric information. Because there is no general agreement on the appropriate balance of security and privacy to build into a system using biometrics, further policy decisions are required. The range of unresolved policy issues suggests that questions surrounding the use of biometric technology center as much on management policies as on technical issues.

Finally, consideration must be given to the convenience and ease of using biometrics and their effect on the ability of the agency to complete its mission. For example, some people find biometric technologies difficult, if not impossible, to use. Still others resist biometrics because they believe them to be intrusive, inherently offensive, or just uncomfortable to use. Lack of cooperation or even resistance to using biometrics can affect a system's performance and widespread adoption.

Furthermore, if the processes to use biometrics are lengthy or erroneous, they could negatively affect the ability of the assets being protected to operate and fulfill its mission. For example, last year, we found that there are significant challenges in using biometrics for border security. The use of biometric technologies could potentially impact the length of the

[6]5 U.S.C. §552a.

inspection process. Any lengthening in the process of obtaining travel documents or entering the United States could affect travelers significantly. Delays inconvenience travelers and could result in fewer visits to the United States or lost business to the nation. Further studies could help determine whether the increased security from biometrics could result in fewer visits to the United States or lost business to the nation, potentially adversely affecting the American economy and, in particular, the border communities. These communities depend on trade with Canada and Mexico, which totaled $653 billion in 2000.

In conclusion, biometric technologies are available today that can be used in security systems to help protect assets. However, it is important to bear in mind that effective security cannot be achieved by relying on technology alone. Technology and people must work together as part of an overall security process. As we have pointed out, weaknesses in any of these areas diminishes the effectiveness of the security process. We have found that three key considerations need to be addressed before a decision is made to design, develop, and implement biometrics into a security system:

1. Decisions must be made on how the technology will be used.
2. A detailed cost-benefit analysis must be conducted to determine that the benefits gained from a system outweigh the costs.
3. A trade-off analysis must be conducted between the increased security, which the use of biometrics would provide, and the effect on areas such as privacy and convenience.

Security concerns need to be balanced with practical cost and operational considerations as well as political and economic interests. A risk management approach can help federal agencies identify and address security concerns. As federal agencies consider the development of security systems with biometrics, they need to define what the high-level goals of this system would be and develop the concept of operations that will embody the people, process, and technologies required to achieve these goals. With these answers, the proper role of biometric technologies in security can be determined. If these details are not resolved, the estimated cost and performance of the resulting system will be at risk.

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

Contacts

For further information, please contact Keith Rhodes at (202)-512-6412 or Richard Hung at (202)-512-8073.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

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

Order by Mail or Phone

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

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:

Voice:	(202) 512-6000
TDD:	(202) 512-2537
Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Public Affairs

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

Mr. PUTNAM. Our second witness is Mr. Christer Bergman. Mr. Bergman has been associated with Precise Biometrics since 2000 and has served as president and CEO for the company since June 2001. Prior to joining Precise Biometrics, Mr. Bergman has worked in the information technology industry for the last 20 years and has held managerial and executive positions in leading Fortune 500 companies. He also serves as an officer on the board of directors of the International Biometric Industry Association, a trade association dedicated to supporting and advancing the collective international interests of the biometric industry as a whole.

Welcome to the subcommittee. You're recognized for 5 minutes.

STATEMENT OF CHRISTER BERGMAN, CEO, PRECISE BIOMETRICS

Mr. BERGMAN. Good morning, Mr. Chairman, and thank you for the opportunity to be here today to represent the view of the industry regarding advancements in smart card and biometric technology in the Federal Government market. As you indicated, my role, roles, are living and breathing biometrics, an industry that is transitioning from emerging technologies into the necessary tool which is part of our daily lives.

The biometric industry today is recognized as very much in focus for governments, organizations, corporations, but it still needs a major sign of approval from government and corporations in order to grow into a mature industry. I'm delighted to have the opportunity to give the industry perspective of what is happening and what is needed in order for this to be a reality.

Let's talk biometrics. As we heard, simply speaking, biometrics is using the body, body parts, in order to identify, verify or authenticate yourself. It could be face, finger, voice, etc. It could be a combination or stand-alone. Biometric technologies could also be used in conjunction with another technology, such as a smart card.

When we talk about biometrics, it's also important to say where the biometric template—which is a digital stamp of your fingerprint or face—is compared? It's stored and compared in the process. This could be done on a network server, including a data base; that could be done on a workstation, or on device, or even on a smart card, as we talked today, and then we call that technology Match-on-Card. Same thing, smart card.

What is a smart card? A smart card is a credit-card-sized plastic card with a small computer on it. It could either be connected via the chip or contactless, as in the case with physical access, and waving the card in front of the reader. The smart ID card, as we call it, it's an intelligent badge; that can be used to access buildings, gain access to computer networks, and can also be the carrier and verifier of my personal biometric identifier. As Mr. Rhodes said before, that the combination of smart card and biometrics can provide a very secure infrastructure. To present something you have; which is a card, something you are; which is your finger or face, and combine it with the password, then you have a three-factor authentication, which represent a very secure ID credential.

However, in reality, in most systems there is a big security gap between what the system is designed for and how it is actually working. Therefore, there is a growing demand of biometrics in

combination with smart cards, so, in my statement, I'm referring to biometrics and now the smart card.

In the older configuration, you used a smart card purely to store information, e.g., a biometric template. In the newer, more preferred from a security point of view, preferred configuration, you use, in fact, the smart card as a computer and also do a comparison of the biometric template on the card, and I will come back to that in a few seconds. Clearly, that means that all the smart card functionality on that card can only be accessed by the person with the biometrics matching the one stored on the card.

We from the industry very much appreciate the committee holding this very important hearing today, because as we approach the second anniversary of September 11, it is crucial to be asking the questions as to why deployment of these secure items is not happening on a broader scale.

My full testimony is attached in response to many of the reasons for this. Let me take a moment to highlight just a couple of the challenges and misunderstandings.

Privacy. People think that a biometric application takes your fingerprint image and places it in a big data base where it can be used or misused. That is not correct. We are using a biometric template, a template from a fingerprint. It could be stored on a smart card, not in the data base, and also it can, in fact, be stored and computed on the card. That means that the only place where the biometric template exists is on the smart card both during storage and the comparison of the stored and captured new image.

Second, the cost. There are many elements that we heard before are building up the cost of any system in the infrastructure. If you combine the smart card and biometrics, you can optimize the cost to any system. For instance, if the application is only verification, there is no need for a big back-end data base and a costly infrastructure.

Coming back to overall leadership support, biometrics was considered a new technology a number of years ago. We from the biometric industry, we applaud President Bush, Secretary Ridge and others who frequently mention biometrics in speeches. That gives us a big boost about biometrics out in the industry.

However, there are other organizations that need to be applauded. They have shown national leadership in the government community, such as the U.S. Treasury, that implement the smart card and biometric system. DMDC and the CAC program, as we heard before, are looking into replacing the PIN code with biometrics, and we have the State Department, who was one of the first to implement the smart card.

My conclusion is that the biometric-enabled smart card is not only a concept, it is very much a proven reality. It could lower overall cost, minimize privacy issues, optimize the usability from a security and convenience point of view, and it could be used for physical and logical access. The industry is actively participating in the standardization work, but in order to create the de facto standard and implement a secure, cost-effective and convenient security system with minimum security gaps, there's a strong need for visionary leadership.

The combined smart card and biometric industries are ready and willing to work with the leaders of this community, the Congress and administration to make biometric-enabled smart cards a reality.

Thank you, Mr. Chairman, for your time and consideration.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Bergman follows:]

Testimony

Advancements in Smart Card and Biometric Technology

Christer Bergman
President and CEO
Precise Biometrics

Submitted to the
U.S. House of Representatives
Committee of Government Reform
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and Census

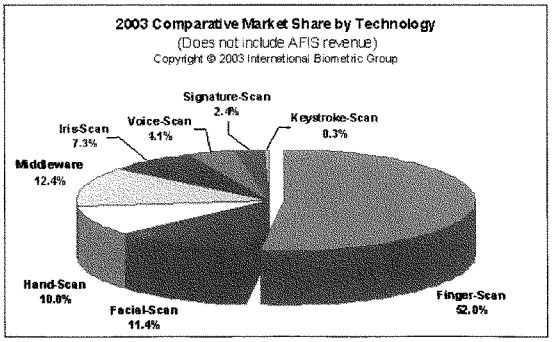
September 9, 2003

Good morning, Mr. Chairman, Ranking Member Mr. Clay and Members of the subcommittee. Thank you for the opportunity to be here today to represent the views of the industry regarding "Advancements in Smart Card and Biometric Technology" in the Federal government market.

I am Christer Bergman President and CEO of a small public company in the biometric industry, Precise Biometrics [1], our focus is fingerprint technology in combination with smart card technology. I also serve as an officer of the International Biometric Industry Association (IBIA) [2] Board of Directors. As my roles indicate, I am living and breathing "Biometrics", an industry that is transitioning from emerging technologies into the necessary tool, which is part of our daily lives. Sadly this is in large part due to the tragic events of the last couple of years. The biometric industry today is recognized as very much in focus for Governments, organizations, corporations and individuals. But, from an industry "insider" point of view, it still needs some major "sign of approval" from Government and corporations in order to grow to a mature industry. With the above, I am delighted to have the opportunity to give an industry perspective of what is happening, what the issues are and what impediments need to be overcome in order to advance the use of biometrics and smart cards for the Federal government.

The Technologies

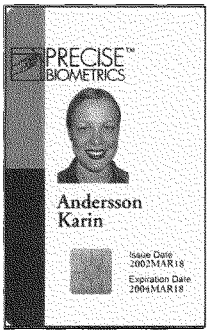
Let me start with a simple ***"Biometrics 101".*** Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. The characteristics measured include: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies can be used in order to identify, authenticate, or verify a person. Biometric technologies can be used as stand alone technology or integrated with other technologies such as smart cards, encryption keys, and digital signatures. The process of comparing a stored biometric template (i.e. a digital representation created from your biometric feature) with the actual captured biometric template can be done by a variety of means, computer network server, workstation, kiosk, access control terminal, embedded processor in a device, or even a processor on a smart card, known as Match-on-Card. For more detailed information about different biometric solutions, see "How secure is your biometric solution" [See Attachment].



Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. The most widely used and accepted biometric technology is fingerprint, which represents about 50% of the market today.

In the same fashion let me do a ***"Smart Card 101";*** a smart card could be defined as a credit card sized plastic card with an embedded secure and powerful computer chip. The chip can either be a microprocessor based device with its own secure Operating System and internal memory or historically a simple memory chip with non-programmable logic. The Smart Card's chip connection is either via direct physical contact or remotely via a contact-less electromagnetic interface. More and more, the smart card is being used as an intelligent ID badge, i.e. Smart ID Card. Today's Smart ID Cards demand the highest levels of computing and security. The Department of Defense's Common Access Card with now approximately 3Million Smart Cards deployed has been fully certified to the highest levels of security required by the US Government (NIST). The Smart ID Card can be used to access buildings, gain access to computer networks, serve as a loyalty card, a banking card and can certainly be the carrier and verifier of my personal biometric identifier(s). The microprocessor on the Smart Card can be used for many different purposes and should be viewed as a powerful and secure miniature computer with an input/output communications port, Operating System and non-volatile memory for storing information. It can also provide a secure data management system ensuring an on-board personal firewall to protect the private data maintained within the Smart ID Card from improper disclosure or usage.

The combination of smart card and biometrics can provide a very secure and convenient secure ID credential. Not only can you present something you have (the smart card), you can also present who you are (biometrics) and combined with a password (something you know); the secure ID credential then represents a very secure 3-factor authentication system. However, more often the preferred solution contains 2-factor authentication: what you have (smart card) and who you are (biometrics). The PIN code or password is becoming a human nightmare to maintain, if we are supposed to follow all the rules regarding selecting the PIN code/password. You are not allowed to have the same PIN code for more than one application, you cannot select a PIN code that could be tracked to yourself and you have to change the PIN code every 30 days - and by the way - you are not supposed to write it down anywhere. In reality most systems today, which are based on PIN code/password, have a huge hidden security gap, the difference between how the system was designed and the practical use of the PIN code/password. Hence, in a world with a growing demand for a convenient and secure system, a biometric enabled smart card offers the best solution.



What does ***a biometric enabled smart card*** mean and how does it work? In older configurations the smart card is used only as a storage device for your enrolled biometric template captured when the card is issued to the cardholder. Upon verification, the smart card would release the stored biometric information to the workstation (or the server) and the live captured biometric template is then compared in the workstation (or server). This configuration is referred to as Match-on-PC (or Match-on-Server). The benefit is that you carry your biometric information with you and can use the biometric enabled smart card

on multiple devices that each support the same mechanism to convert the live captured fingerprint image to the corresponding template. The drawback is that your complete enrolled biometric template once transmitted by the Smart Card is exposed during transfer and verification, creating security vulnerability and a direct concern regarding the privacy of your biometric information.

From a security aspect, the more preferred configuration is when you fully utilize the capabilities of the Smart Card and use the Smart Card not only as a secure storage device, but also use it as a powerful self contained secure computer. The actual comparison of the enrolled template to the live captured template is performed within the Smart Card chip itself. If there is a match, then the Smart Card will securely supply that information to the application. This configuration is referred to as ***Match-on-Card.*** The additional benefit is that both the security and privacy concern will be minimized – the template verification is done within a secure environment (inside the secure area of the Smart Card) and the enrolled biometric template information does not leave the card, hence the only place your biometric template exists is within the Smart Card – which you control and carry about. Clearly the Smart Card functionality is useless to anybody else other then the enrolled person who can prove their identity by presenting their biometric for the card to internally verify.

The first biometric technology for true Match-on-Card is fingerprint technology which was introduced to the market a couple of years ago and is now a standard product offering. It can be used with most Smart Cards today and companies such as Schlumberger, Datakey, Siemens and other Smart Card manufactures have already integrated the product in their product portfolio. However, the Match-on-Card concept could be used for other biometric technologies as well.

From an end user point of view, the ideal fit for Match-on-Card is with Identity Systems that incorporate Public Key Infrastructure Technology. Instead of using the Smart ID Card's PIN code to get access to the Private key's functionality, the live captured and computed biometric template is presented and if verified with the stored template - access is granted and minimum changes are needed to the overall application and project. Both the end user and Identity System provider will experience a secure, cost effective and importantly a convenient solution to ensuring strong cardholder verification.

The Issues

What is happening?

So it seems that the combination of Smart Card and biometrics could be the optimal solution to ensure a convenient way to increase the physical as well as computer security throughout the Federal government and corporations. Why is this not happening on a broader scale?

- "We don't know how secure the system is!"
- "Integrating physical and logical security will not work!"

- "It costs too much – we can't afford this!"
- "There is no standard – it is not approved!"
- "It is not interoperable with other biometrics systems!"
- "Privacy concerns - my fingerprint will be available to anyone!"

These are some of the comments that you will get from the market. Let me therefore explore some of these aspects further:

Privacy.

The first misunderstanding is that people think that using fingerprint biometrics means that the system captures the fingerprint and then sends it over the (open) network, where it can be intercepted and used for criminal purposes. (Some of the science fiction movies during the recent years are good for marketing biometrics – but it does not give the complete and accurate information about how biometric technology can be used in reality). People are also afraid of being recorded in a national database involuntarily, even if they do not have any criminal record. The reality is that the Identity System uses the fingerprint to create a digital biometric template that does not show your complete fingerprint, nor can it be use to recreate your fingerprint. It is also a reality that most biometric systems today use a secure network if the biometric template is being transmitted. With the use of Match-on-Card, the biometric template does not even leave the Smart Card and you decide yourself when you want to use a service that requires the use of your biometric enabled Smart Card.
An excellent Reference paper entitled "Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems" has been published by the Smart Card Alliance and is available on their web site [3].

It should also be noted that all the members of IBIA have accepted and adhere to the IBIA Privacy Principles [2].

Interoperability.

Certainly it would be very nice if there would be complete interoperability among all the different biometric technologies – but this is not realistic. But it should be mentioned that a number of biometric implementations today include multiple biometric technologies; fingerprint + face or fingerprint + iris. Many of the biometric solutions that support multiple applications also use PIN code and other legacy technologies in order to work with the installed base of infrastructure.
Even the interoperability between biometric vendors within one biometric technology (e.g. Fingerprint) is not there today. However, there has been significant progress made over the course of the last couple of years - one of the most important initiatives is The Biometric Consortium [4]. The biometric industry is now driving towards standards, both domestic and international. However, it takes time to agree on a technical standard and as most of the other new technologies that are changing our daily life; a de-facto standard is being created in parallel with the standardization work.

The above is valid for the biometric industry and to a lesser extent the Smart Card industry, which has made significant efforts to create open standards and specifications.

However in the combination of biometrics and Smart Cards, the progress is slower largely due to the relative recent maturity of Smart Cards and their ability to now perform Match-on-Card. Therefore there is a need for visionary leadership to help create the de-facto standard for biometric enabled Smart Card technologies by funding and directing some of the ongoing Smart Card projects to include Match-on-Card biometrics as a secure, cost effective, convenient solution to strong card holder authentication.

Security of the system.

In the biometric industry, the security is often measured with the terms False Acceptance Rate (FAR), and False Rejection Rate (FRR), and the combination of the two. A biometric system could be tailored to high security (very low FAR and moderate FRR) or it could be used more for convenience (moderate FAR and very low FRR). The problem arises when comparing the FAR/FRR from different systems, because there is no standard on how to perform the tests. Should the test be done on a human population or should it be performed on a database of fingerprints, and in this case on which database? Certainly the best performance test would mirror the practical use and involve real people for the testing. One such initiative is the "Comparative Biometric Testing", performed by International Biometric Group, IBG [5]. Another more recent development is the formation of the National Biometric Security Project, NBSP [6] whose mission includes facilitating the education, test and deployment of biometric security systems.

When it comes to comparing the security of a biometric system versus a PIN code based application, which is often the case when referring to a biometric enabled smart card - the picture becomes even more complicated. It is easy to measure the FAR for a 6 digit PIN code, where a quick calculation gives the answer 1:1,000,000. However, when the security gap (as referred to above) is taken into consideration, there is no real practical answer. On the opposite, it is only a theoretical and maximal security level. In a biometric system, it is real people in different situations who are using the system; therefore there will always be a difference in how the individual is applying the finger to the device during enrollment and verification. In conclusion, there is a need to develop test cases that mirror the real usage of a system. The results could then be used as one parameter in selecting a biometric system. Another more important parameter is installed systems and the end users feedback on the convenience aspect of the implementation.

Cost.

There are many elements that build up the cost of any system or infrastructure. Let me therefore only briefly highlight some of the considerations. If the system is a biometric only system, there is a cost per biometric device, for the biometric application and a cost for the infrastructure. Practical examples show that for a Single Sign On application, i.e. "replace my passwords with biometrics", the return on investment could be less than 6 months. This calculation is based on the downtime for both the end user and the help desk in order to solve password problems.

If the combination of the biometrics and Smart Card is fully utilized, then the cost can be further optimized for the system as well as satisfying the need for a fully scalable Identity System. If part of the application is a biometric verification only, there is no need to have

a costly infrastructure in place. The biometric matching application resides on the Smart Card. If the Identity Verification application could be built as a "kiosk" or mobile/portable application, then there are minimum needs for biometric devices and minimum needs for connectivity to any databases storing a collection of enrolled biometric templates.

By using a combination of biometrics, Smart Card and also another new revolutionary technology; Real Time Credential, the overall cost for a project like US-VISIT would be dramatically reduced.

Overall leadership support.

Biometrics was considered a new technology a number of years ago. Very few people knew about the existence. Today there is a totally different awareness of biometrics: even President Bush, Secretary of the Department of Homeland Security Ridge and Undersecretary of Borders and Transportation Security Hutchinson frequently mention biometrics in public speeches. When it comes to smart card technology the market awareness also in the US has increased quite dramatically during the last couple of years. For strong card holder verification the combination of biometric Match-on-Card, Smart ID Cards and Public Key Infrastructure represents an ideal way to protect our Nation's infrastructure from unauthorized access, attack or abuse.

The standardization of biometrics is on its way as well as the standardization of Smart Card technologies. However, there are very few initiatives that combine the technologies. Why is it so?

Any change of procedures, new technologies that change the way we should work or any other "disturbance" is not welcome in an organization or society. There has always been and there will always be a need for visionary leadership in order to change.

Any organization that is faced with changes has to be reviewed; this is also true for the Federal government when it comes to the combination of biometrics and smart card. The security community of the Federal government is used to the Smart Card's "PIN code security" – i.e. all biometric systems are welcome to replace the PIN code if it can be proven without doubt that the FAR is 1:1,000,000. After the explanation above, it is obviously a good and easy measurement, however is this reality? The Biometric community has been testing systems for the last couple of years – but where are the results or directives for the industry to change or adopt? Clearly Biometric Match-on-Card is ready, tested and proven and can be deployed with confidence that strong card holder verification is practical and cost effective.

However, there are a number of organizations that have shown visionary leadership both in the government and corporations. They are implementing Smart Card and biometric systems, but they are also crossing the organizational bridges between physical and logical (computer) security. US Treasury is one such organization that realized the importance of biometrics and Smart Card and has started to build an infrastructure that can be flexible for a biometric enabled Smart Card. The DMDC and the CAC project

have shown such leadership, and are planning to take the next step in order to optimize their system and to introduce biometric card holder verification in place of, or in addition to the CAC's PIN. The State Department was one of the first organizations to implement a Smart Card based Identity System and are also showing their visionary leadership. These are only a few, there are many more who test the concept with great success, but are waiting to deploy on a broader scale. They are all waiting for any of the large Federal projects to sponsor and pioneer the new technology: the overall PKI-initiative, CAC, TWIC and/or US-VISIT.

Conclusion

Finally let me once again, express my appreciation for the opportunity to share my view on the "Advancements in Smart Card and Biometric Technology". My conclusion is that the biometric enabled Smart Card is not only a concept; it is very much a proven reality. It should lower the overall cost of a system implementation by virtue of removing the heavy support costs of PIN management, it can minimize privacy concerns with respect to storing the biometric information in a central database and the potential exposure of the biometric information when using the system. It will also optimize the usability of the overall system with respect to security and the convenience of using the biometrics for both physical as well as logical access control. The industry is actively participating in the standardization work as well as driving towards a performance test that will show real, practical performance of a biometric enabled Smart Card Identity system. However, in order to create a de-facto standard and implement a secure, cost effective and convenient security system - with a minimum of hidden security gap – there is a strong need for visionary leadership. The combined Smart Card and Biometric industries are ready and we seek your help from within the Federal government to make biometrically enabled Smart ID Cards a reality.

Thank you for your time and consideration.

Reference list:

1. Precise Biometrics, www.precisebiometrics.com
2. International Biometric Industry Association, www.ibia.org
3. Smart Card Alliance: www.smartcardalliance.org
4. The Biometric Consortium, www.biometrics.org
5. International Biometrics Group, IBG, www.biometricsgroup.com
6. National Biometric Security Project, NBSP, www.nationalbiometric.org

Attachment:

1. "How secure is your biometric solution", Precise Biometrics White Paper

How secure is your biometric solution?

Magnus Pettersson, Mårten Öbrink

Precise Biometrics AB, Dag Hammarskjölds väg 2, SE 224 67 Lund, Sweden

26th February 2002

Abstract

Biometric solutions are installed frequently everywhere from airports to stock broker firms. There are various biometric solutions on the market, the question is: which biometric technology is best suited for my needs? This document is a security overview of different ways to use biometrics to secure computers, networks and digital information in general.

1 Introduction

What should the biometric device be used for? Is it only PC/network log-on? Is it to secure a signing key? Encrypt data? Enter a door? Sign a mobile transaction? These questions are important when choosing a solution. In this Whitepaper we will mainly address logical access, i.e. access to information. A basic application providing logical access is PC/Network logon using biometrics. For this purpose, storing the fingerprint at the local computer or server might be enough. Furthermore, in this case the fingerprint does not represent your digital identity on the Internet, only in your local environment. If the scope is PKI based applications (such as VPN, secure email etc) where a smart card is used for credential storage, that is also where the fingerprint template should be stored.

2 Computer security in general

To choose the appropriate level of security for a system is not an easy task. In most cases some kind of encryption is used, often using *PKI* (Public Key Infrastructure). This infrastructure relies upon digital certificates and the fact that each user has his or her own encryption key (called a private key), which must be protected. Via this key, access may granted to a network, a secure

email may be decrypted, a remote connection may be established to a company intranet etc. The private key is often stored on a smart card since this is a very secure storage medium and very hard, close to impossible, to tamper with. The smart card is protected by a secret, which traditionally is a PIN or sometimes a password. Instead of a PIN or a password, biometrics can be used to tie the identity to a physical person even stronger. However, this must be implemented in a secure way.

3 Different ways to implement biometrics

From a security aspect, the two important parts of a biometric system are

- Storing (on a server, in the PC, in the capturing device, in a smart card)
- Matching (on a server, in the PC, in the capturing device, in a smart card)

Depending on how these parts are combined, the security implications of the system are different. The table below is showing combinations of where the fingerprint is stored, and where it is matched. Some of these combinations are highly unlikely to ever exist in a commercial product and are therefore not discussed. These are marked with an X and will not be addressed further. (A server in this context is a hosted server accessed via the Internet).

Table 1: Combinations of where the biometric data is stored versus where it is matched.

	Store on server	Store in PC	Store in device	Store on card
Match on server	a	X	X	b
Match on PC	X	c	X	d
Match in device	X	X	e	f
Match on smart card	X	X	X	g

4 Security overview

a Match on server / Store on server

Matching on a server means matching in a protected environment. The administrator can monitor the security and detect attempted attacks on the system. The storage on the servers means that also the template is protected from tampering, at least from the outside. Getting users to store their fingerprint templates in a server out of their control may be hard; this requires that the party running the server is trusted. One security problem is the transfer of the template from the

capturing device to the server. This requires a secure Internet session or an intelligent way to solve the problem with cryptography. This solution also requires that a new infrastructure is built, which makes the solution difficult to deploy in large scale.

Conclusion

+ The administrator has full control of the fingerprint database
- The solution may be violating personal integrity
- The solution requires a whole new infrastructure to be built
- The fingerprints are transferred over an open network

b Match on server / store on card

In this case, the template remains with the user on a smart card, hence the problem with storing ones fingerprint template on a server out of your control is solved. The other problem with servers - the transfer of information across an untrusted network is augmented; now both the template and the input image must be transferred. In this case some kind of strong encryption should be applied to secure the transfer. This solution has drawbacks both with regards to security and due to the fact that a new infrastructure has to be built.

Conclusion

- The solution may be violating personal integrity
- The solution requires a whole new infrastructure to be built
- The fingerprints will be transferred over an open network unless an encrypted connection is used

c Match on PC / Store on PC

This is a common combination where the templates are stored on the users hard drive. This is also where the matching takes place. Since the PC is not a secure device there is an immediate threat that secrets such as templates or passwords may be stolen tampered with. Mobility may be a problem; the user can only log on to the computer where the template is stored.

Conclusion

+ The user has got control of his/hers own templates
- The PC is not a secure environment for template storage
- The solution is not scalable even on a local network

d Match in PC / store on smart card

Storing the template in a smart card but match in the PC eliminates some of the problems with variant (c). When a smart card is used it is often access to the protected area on the card that is critical. Access is granted if the correct PIN is sent to the card (the PIN is matched on the card). In this system, both the template and the PIN have to be transferred to the PC from the card, if the input image matches the template the PIN is sent back to the smart card to gain access. The template is not available for hacking at all time since it is stored on a card. But, the critical information (the template and the secret e.g. PIN) is sent to the PC from the card when matching. This means that both the template and the secret can be tampered with or stolen.

Conclusion

+ The user can carry his or her own template (stored in the smart card)
+ The user might use the fingerprint/smart card for accessing multiple devices
– The templates are exposed during verification
– The solution cannot be used for secure network transactions

e Match in device / store in device

In this scenario, no information is exposed in the PC since all information is stored in the device. This makes tampering with the template difficult. This means that the device is more or less personal since without it, I cannot reach my template.

Conclusion

+ The user has control over his or her own template
+ The template is never exposed (if the device is regarded as secure)
– Portability is limited since the template in the device itself and can not be accessed via another device

f Match in device, store on smart card

The roaming problem of (e) is solved here. The matching is also made in a safer place than the PC - the device itself. There is however still a PIN or password involved accessing the smart card. This means that this secret is stored somewhere - probably in the smart card. When the fingerprint matches, the secret is fed back to the card to gain access. Both the template and the secret can be

read from the card without restrictions, which means that the secret can be stolen.

Conclusion

+ The template can be accessed from any device
+ The user is in control of his/hers own template
– The template is exposed during verification (when transferred)
– There is a security hole when using the smart card for storage of certificates (PKI), as the secret to unlock the card is stored on the card and sent to the device before used to access the card

g Match on card / Store on card

Both matching and storing on the card mean that the sensitive data (the template) never leaves the card. There is also no secret to steal since a successful match enables the use of certificates on the card without the need of stored PINs or passwords. Even in the unlikely event that a card is tampered with; only limited damage is done since only that specific users credentials are hacked. An attack on multiple users means that the attacker must get hold of all users' cards This method is normally seen as the most secure way of biometrically securing computers, networks and digital information in general.

Conclusion

+ The smart card is made personal; it cannot be accessed without the appropriate biometric authentication
+ The templates are never exposed to a non-tamper proof environment
+ The user carries his/hers own templates
+ The solution works with a PKI (digital signatures, authentication over networks, encryption) without the need of new infrastructure

References

[1] Pettersson M., *Match-On-Card Whitepaper* 2000, Precise Biometrics external publication.

[2] Pettersson M., Öbrink M., *Ensuring integrity with fingerprint verification*2000, Precise Biometrics external publication.

[3] www.precisebiometrics.com

For Additional Information

www.precisebiometrics.com

Sweden, Lund

Precise Biometrics AB
Dag Hammarskjölds v.2
SE 224 64 Lund
Sweden

Tel: +46 46 311 100
Fax: +46 46 311 101
E-mail: info@precisebiometrics.com

Sweden, Stockholm

Precise Biometrics AB
Box 1223
SE 164 28 Kista
Sweden

Tel: +46 46 311 100
Fax: +46 46 311 101
E-mail: info@precisebiometrics.com

USA, Washington D.C.

Precise Biometrics Inc.
8300 Boone Boulevard, Suite 500
Vienna, VA 22182
USA

Tel: +1 703 848-9266
Fax: +1 703 832-0577
E-mail: infous@precisebiometrics.com

Mr. PUTNAM. Our final witness for this panel is Mr. Daniel Turissini. Mr. Turissini is president and COO and one of Operational Research Consultants' founding partners. For the past 10 years, he has focused the Operational Research Consultants in the field of information assurance and information security. Of note, ORC was certified as the first of three certificate authorities for the Department of Defense's External Certificate Authority program. The ORC is also certified by the General Services Administration to provide access certificates for electronic services. Under Mr. Turissini's leadership, ORC has been designated as the lead systems integrator for the DOD Public Key Infrastructure, a standard information assurance program being implemented across all branches of the DOD, which is a user community of approximately 36 million personnel, devices and applications.

Welcome to the subcommittee, Mr. Turissini. You're recognized for 5 minutes.

STATEMENT OF DANIEL E. TURISSINI, PRESIDENT, OPERATIONAL RESEARCH CONSULTANTS, INC.

Mr. TURISSINI. Thank you, Mr. Chairman.

Thank you for the opportunity to appear here to discuss advancements in smart card and biometric technology. The fact that this committee is holding these hearings reinforces an important focus on ensuring the integrity of sensitive and confidential information. The paper I provided, which I summarize here, highlights the complexity of this challenge.

I focus on digital security and authentication. We can talk to physical in the questioning. This includes maintaining an open environment for commerce, data exchange, collaboration and communication, but without sacrificing information security. To meet this challenge, we must first adopt a credential or a standard for credentials that will support confidentiality, data integrity, identification and authentication, privilege and authorization, and nonrepudiation.

Second, we must provision to protect those credentials. This is further complicated by our need in this country to be mobile.

And last, we must achieve these goals without encroaching upon civil liberties under which our country was founded.

The information fog preceding September 11 and the recent virus attacks in the headlines leave little time for invention and development, especially while we are not taking full advantage of significant advancements in the development of production and technologies like smart cards, biometrics, and asymmetric credentialing. We must certainly agree about the urgency to these requirements; yet, for over 5 years we are delayed implementing solutions that address many of these issues in favor of a more optimal solution that will soon be available or a single solution that will be everything to everybody.

Our target should be striving to attain the highest level of security currently attainable without sacrificing availability to authorized parties. To a large degree, the resistance to this technology has been due to fears of the loss of privacy and images of "big brother." Although not without merit, such fears do not have to be realized if the proper approaches, policies, procedures and edu-

cation are employed. We must embrace the technology available today and continue to evolve these technologies as advances emerge and technologies mature. Instead of reinventing the mouse trap, we must use the mouse trap we have and enhance that trap over time.

The technologies necessary to attain digital security in our open society are available. Asymmetric key technology fully supports nonrepudiation and ensures user privacy. Identity, represented by a key pair, can be managed so that key, the private key, is created and retained only by the owner, while the associated public key can be freely distributed, thus providing the requisite security needed to afford all parties a high level of confidence that the individuals attempting access into resources are who they claim to be, and that the actioning of a transaction can be identified and nonrepudiated, and this can be done without compromising or infringing upon the privacy of the individual. It has been by adhering to established standards, policies and procedures, and enforcing the proper use and integration of these technologies, and enforcing the laws to provide the requisite ramification for transgression.

The infrastructure to deploy this technology is currently fielded, capable and interoperable, but underutilized. Federal leadership is required for the implementation of meaningful and efficient security over the Internet to protect sensitive information and billions of dollars in transactions each day. With your support, the large investment already made in the GSA ACES program and the DOD PKI program can be embraced to avoid many of the problems that stand in the way of the President's e-government initiatives.

Equally as important is advancement of the technologies of smart cards and biometrics, and they can be focused on enhancing the existing security tools and ensuring the protection of these credentials that are available today. There is not currently one solution or technology that will attain the desired level of security without sacrificing availability and without encroaching on civil liberties; however, through proper integration and configuration of smart card, biometric and asymmetric key technology, security can be achieved and Constitutional rights protected. It is an achievable undertaking that will "provide for the common defense, promote the general Welfare, and secure the blessings of liberty to ourselves and our prosperity."

Thank you for your time and the opportunity to present our viewpoint.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Turissini follows:]

DANIEL E. TURISSINI
PRESIDENT
OPERATIONAL RESEARCH CONSULTANTS, INC.
TESTIMONY BEFORE
THE SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS
COMMITTEE ON GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

SEPTEMBER 9, 2003

Mr. Chairman and Members of the Subcommittee,

Thank you for this opportunity to appear before the Subcommittee to discuss issues relating to *Advancements in Smart Card and Biometric Technology.*

By the mere fact that this subcommittee is holding hearings on a topic such as Smart Cards and Biometrics, it stands to reason that the Government is truly focused on the requirement to ensure the integrity of sensitive or confidential information. As such, it is worth noting that this task is complicated by the fact that the same information to be protected must also be circulated among a limited, but frequently changing, audience of specifically named people. It must be provable who (by name, not simply office) the provider of a piece of information is and it must be provable that no one has modified the information subsequent to its issuance. There must be no question as to exactly when the information was published. There must be a means of reviewing the history of any particular document, in terms of who did what to it, and when, as it was developed and circulated. There must also be a means to archive all information securely as well as a means to recall the information from the secure archive at a later time. The systems and technology used to accomplish these objectives must be easy to use and suitable for senior executives, managers, and workers at all levels. Reliability must be very high. And there is a requirement for the system to support the mobility of some of its users. For speed and convenience, the system must be electronic, not paper. Taken individually, these are considerable tasks. Taken as a whole, they appear to require Herculean effort. However, appearances can often be misleading. This undertaking is achievable, the tools and technology currently exist, and some are already being leveraged by certain government agencies. Those available tools are Smart Cards for the storage of digital credentials (among other data) and Biometrics to achieve the highest certainty of credential protection.

With the events of today's society such as the information fog preceding September 11, 2001 and the recent virus attacks, there is an urgency to these requirements that permits little time for invention or development. The past several years have seen significant advancements in the development and production of smart card technology and biometrics has seen significant progress. Further, the integration of these technologies into legacy and current generation environments has grown correspondingly. Unfortunately, the policies and acceptance of these technologies have progressed at a

much slower pace. To a large degree, this resistance to smart cards and biometrics has been due to fears of the loss of privacy and images of "big brother." Such fears are not without merit. However, such fears do not have to be realized if the proper approach, polices, procedures and education is proliferated.

The Goal of Security

Security by definition is "*something which guarantees or safeguards.*"[1] With regard to Information Systems Security, it is defined as: "*The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.*"[2] That which is to be guaranteed or safeguarded is primarily the information asset residing within an enclave, enterprise, database, desktop, laptop, etc. Thus, Information Security applies to anyone using a computer, PDA, cell phone, and so on. In other words, it applies to most everyone in American society today.

There are numerous facets to Information Security that wage a continual tug-of-war, such as protection, privacy, availability, and so on. There are also a plethora of less than ethical individuals using malicious code to wreak havoc on their target du jour, as well as the unsuspecting. The news recently was once again filled with reports of viruses and worms spreading to businesses and households alike. To quote a September 1, 2003 article by Chris Taylor of Time magazine, "*worms spring from the minds of virus writers, who could be sitting at any computer in the world. Most spread because we do careless things like open e-mail attachments from strangers, but some have evolved to spread through computer networks on their own — like plague bacilli that have become airborne.* "[3]

The key piece of Mr. Taylor's article is the statement that "*we* (people in general) *do careless things like open e-mail attachments from strangers.*" This does not, and should not, have to be the case. The ease with which nefarious code writers proliferate malicious code is a travesty that does not have to be. Still, our Government has not taken advantage of the significant investment already made in digital certificate technology, a technology that can present an enormous roadblock to such worms and viruses as 'Blaster' and the 'I love you' virus, and the like. By embracing this existing infrastructure, transactions that do not originate from an entity authenticated with a credential from a known, trusted authority, can easily be discarded and we will all live to see another digital day.

The target we should all be striving for is to attain the highest level of security, without sacrificing availability to authorized parties, and without encroaching upon the civil liberties under which our country was founded and has operated for over two hundred years. Moreover, it is critical that we all understand that we cannot allow technology to

---

[1] New Concise Dictionary, Lexicon Publications, 1997
[2] Federal Information Security Awareness, *Definition of Information Systems Security*, Department of the Interior, National Business Center, Internet: http://www.doiu.nbc.gov/itsecurity/fissa/content/text_only/module1/topic2.htm
[3] Taylor, Chris, *Attack of the World Wide Worms*, TIME Magazine, September 1, 2003

be the driving force behind the policies governing their use. Instead, it must be common sense, sound policies and prudent laws that dictate how technology can complement and augment the safeguards and protections already in place. Too often, a new technology is devised and we make the mistake of compromising our processes and procedures so that the new technology can be used. This is analogous to building a brand new automobile in order to properly accommodate a newly invented radio. If the radio cannot be produced so that it can be integrated with an automobile, it must not be a *car* radio. If a technology or device requires the comprehensive reconfiguration and reconstruction of the existing resources, policies and procedures, it is not a proper fit.

Privacy issues

It is with good reason that most people in the today's society are skeptical of a universal identification card that contains vital personal information. Or, that they have fears of their personal data residing in a database somewhere that can potentially be 'hacked' into, causing their data to be compromised. Unfortunately, in the haste of the Internet boom vast amounts of personal data were willingly and/or unwittingly made available by individuals themselves, marketing groups, businesses, even some Government agencies, and a whole host of others. Now, we are left with trying to lock-down as much as possible while simultaneously reeling back in that which has escaped. Society's collective sense of being jaded by the Internet is quite well founded. However, the Internet was never intended to afford privacy to anyone. Quite to the contrary, the Internet was devised for the **open** sharing of information to anyone and everyone with a connection. Nonetheless, this is the state we are currently in, and some measure of privacy is still attainable.

Properly managed digital credentials can provide the additional security needed to afford all parties a high level of confidence that individuals attempting access to resources are who they claim to be or that the actionee of a transaction can be identified and non-repudiated. This can be achieved without compromising or infringing upon the privacy of the individual. It is simply a matter of adhering to established standards, policies and procedures to enforce the proper use and integration of the technologies, and laws to provide the requisite ramifications for transgression.

Smart cards and Biometrics

Smart cards afford an obvious benefit, mobility. By possessing a credential that can authenticate that an individual is who they claim to be, regardless of where they are, is highly beneficial. This un-tethers the individual from the desktop or laptop and frees them to move from station to station. And because there are such requirements within the Federal Government such as FIPS (Federal Information Processing Standard) to ensure such functionality as the token being tamper proof, for example, among other requirements, the level of assurance can remain consistent. However, with digital transactions smart cards are only as effective as the credential the card is protecting.

Biometrics provide a uniqueness of the persons identification, 'something you are.' Advancements have led to the ability to distinguish an individual by their fingerprint, voice, face, eye, entire body, and more. More importantly, devices are being developed that can use multiple biometric 'signatures' to exponentially increase the accuracy of identification and decrease the possibility of a 'false positive' or incorrect identification.

With both smart cards, as mentioned previously, and biometrics, legal non-repudiation is challenged because digitally there is no difference between the credential presented and the one stored for comparison. However secure, if the credential or the biometric 'signature' resides in a database, someone other than you has access to your credential. To extend this legal argument further, it is not necessary to prove that someone *did* or *did not* have access to your credential or biometric data. But rather, *could* someone, such as an administrator, have accessed your data? Or even the reverse of that argument, is it a categorical impossibility that no one other than the owner of the data had access to it? This is why the policies, guidelines and laws play such a critical role. Each piece of the equation, the card, the reader, the biometric, the credential, policies, the consequences, are all an equally important factor to the sum of the security solution.

For instance, with symmetric key generation the owner of the credential must know or have contact with all those in the community with which they are presenting their digital credential. This is because they must share their credential with that person and that person must subsequently 'recognize' that credential as being from its appropriate owner. This quickly becomes an arduous process when dealing with a community of any substantial size. To solve this issue, we must look beyond the physical and think in the "digital dimension."

Asymmetric key technology offers both identity assurance and privacy. An individual's identity is represented by a key pair. Properly managed, the private key is created and retained by the owner and only by the owner. The public key is then freely distributed to a public repository(s) where it can be accessed by anyone known or unknown. Despite being based on complex cryptographic technology and mathematics, the user experience is quite simple. To identify one's self, the individual applies an algorithm using their private key and presents the result, a 'hash.' At the other end of the transaction, an algorithm is applied using the individual's public key. If the resulting hash matches, the recipient can be assured of the identity of the initiator, and knows that the transaction was not altered or tampered with between the time it was created and the time it was received.

In a vast community of users such as the Internet it is much more feasible to leverage asymmetric key technology where distribution and retrieval of public keys can be readily achieved, and the protection of the private key can be managed to the level of assurance desired and that technology permits. The Internet can be used as it was designed, for the **open** sharing of information without the loss of protections or privacy.

Implementation

Federal agencies must lead the implementation of meaningful and efficient security into Internet/ Intranet operations to protect sensitive information and billions of dollars in transactions each day, as well as the privacy of its citizenry. A digital credential acquired from a certified "trusted third party" recognized and accepted both internally and externally as trustworthy is the front-runner to achieve these requirements. Once adopted, increasingly mature internal policies can be developed to ensure only those designated as authorized can gain access to resources while facilitating expedited secure communications with partners, vendors and citizens. And, equally important, the advancement of technologies such as smart cards and biometrics can be focused on enhancing existing security tools to ensure to a great degree that the individual presenting his or her self is, in fact, who they claim to be. Combined with asymmetric key technology, smart cards *and* biometrics provide 'three factor' protection of that digital credential.

- Something one knows, (pin or a password);
- Something one has, (smart card); and
- Something one is, (biometrics).

As the factors of the credential protection increase, so too does the assurance level that the individual is who they claim to be. Conversely, the probability that the individual is being 'spoofed' or mimicked by an intruder or interloper decreases.

The Department of Defense (DoD), as Mr. Scheflen has stated/will state, has been rapidly deploying the DoD Public Key Infrastructure (PKI) for the exchange of unclassified information leveraging smart card technology in the form of the Common Access Cards, and has piloted an external certificate authority (ECA) or trusted third party. Further, to meet the objectives of Federal-wide interoperability, the Defense Information Systems Agency has established a Federal Bridge Certificate Authority (FBCA) compliant commercial root which holds a non-agency specific Government OID (object identifier). This "Government commercial root CA" has been established to sign the subordinate ECAs. Additionally, the General Services Administration (GSA) has established the Access Certificates for Electronic Services (ACES) program, an infrastructure poised to provide digital certificates to the citizenry for use with various Government services such as Social Security Administration, Health and Human Services, etc. These infrastructures represent a prime example of best practices for ensuring authentication, confidentiality, data integrity and non-repudiation via digital certificates employing smart card technology.

Summation

The technologies necessary to attain digital security in our open society are available. Asymmetric credentials fully support non-repudiation and ensure user privacy coupled with multiple levels of credential protection based on the requisite security need. In more simple terms, providing each citizen the means by which they can authenticate themselves using something they know (password), something they have (smart card), and something they are (biometric) can begin today. Further, this does not have to be

done at the expense of anyone's civil liberties. However, to do so we must embrace the technology available today and continue to evolve these technologies as advancements emerge and technologies mature. The infrastructure to mitigate much of the risks associated with digital transactions is fielded. With your support, the ACES, DoD PKI, and DoD ECA programs can be embraced to avoid many of the problems that stand in the way of the President's eGov initiatives. Instead of continually reinventing the mousetrap, we need to use the mousetrap we have and continually enhance that trap to remain one step ahead of the mice. Through proper integration and configuration, security can be achieved and inalienable rights protected. Leveraging these technologies is not a panacea. It is an achievable undertaking that will "provide for the common defense, promote the general Welfare, and secure the blessings of liberty to ourselves and our posterity."[4]

Thank you for your time and the opportunity to present a viewpoint into this extremely important issue.

[4] The Constitution of the United States of America

Mr. PUTNAM. I appreciate the remarks of all of our witnesses.

I'd like to begin with questions from Mr. Rhodes. You opened up your remarks with a three-prong test, if you will: How will the technology be used, what is the cost-benefit analysis, and what are the tradeoffs.

Mr. RHODES. Yes, sir.

Mr. PUTNAM. I'd like you to answer, how does GAO envision smart-card technology being used; to what degree, what scale, what applications would be layered on? In other words, are we just talking about identity authentication, are we just talking about access, or would there be other applications which you all would envision?

Mr. RHODES. Well, there would be the primary function, of course, the authentication of you as who you are, and all that would be associated with your identity.

So that would be mainly in the areas of access, and that would be access to location as well as access to system and information, etc.; I mean, not unlike the token that you carry with you in order to vote. I can't use that token; that's yours. It's in your possession, but it gives you access in order to do something.

So in saying, "Is it just access to a facility or is it just access to a system," it's really the opener for you to be able to exercise your function as a Representative of the United States in your role of executing a vote. So that's defining it just as access to location or access to information. There is that part.

But then the other two legs, as it were, of detection as well as reaction in terms of holistic security approach, it would be used as a continual identifier of you wherever you were inside the system. You're inside a facility and then you log onto a computer and some incident occurs; we will be able to know where you are inside the system. So it's not just access for you as an individual, but it's also evidence collection. It's also forensic analysis from the law enforcement standpoint, and it's also reaction from either the computer emergency response team or law enforcement to be able to isolate the systems that are under attack or a location that's having a problem.

For example, in the release of the Blaster Worm that's gone on for the last few weeks, someone has been identified. There's a possibility that someone else is colluding with that individual. If people had better positive identification of themselves, of the system, and of the system to other systems involved—it's not just an access point, but it's also an identifier of action as well.

Mr. PUTNAM. So those are additional values that come from having positive ID. Does it pass your second test, which is the cost benefit?

Mr. RHODES. Depending on what you want to do. If you're talking about—I mean, once upon a time, for access to a particular system, when I worked prior to coming to GAO, I needed a retinal scan in order to actually control the system, because it was a high-value asset and it was a high-security clearance. I actually had several stages I had to go through before I got to that part of the system where I exercised the retinal scan. So in that scenario, the cost benefit is the function of what are you going to lose if the asset becomes compromised.

And that's really the primary high-level policy statement, not unlike the Smart Card discussion that my colleague Joel Willemssen talked about on the first panel. There has to be that policy established that says, "This is the hierarchy of value." What we're really talking about is operation security. You're looking at what are the critical assets. You're valuing them based on risk, and you're saying what needs to be applied.

Well, most people view a retinal scan as very intrusive, and they aren't willing to sit and go through that process; but everybody has their fingerprints, and that's less intrusive. So building that connection between value of asset and the multiple layers of authentication—something I have, something I know, something I am—that's the process for the cost benefit. So being able to say, are biometrics cost beneficial? Yes, they are.

Smart cards are cost beneficial as well, depending on how you apply them. I mean, the CAC program, as was discussed in the earlier panel, incorporates fingerprints. Obviously it's cost beneficial for their application, but you might not be able to use that to control a spacecraft on orbit.

Mr. PUTNAM. I think Mr. Willemssen's comments were right on, and his take-away point was that this credentialing standardization is the most important first step; and I think that was the key point. But at the higher levels, at the higher security clearances, if you want access to a silo or access to a sub, I think that people are pretty well in agreement and are willing to undergo the intrusive nature of the biometric scan. But we basically already have that.

Mr. RHODES. Absolutely.

Mr. PUTNAM. Since.

Mr. RHODES. Twenty years ago.

Mr. PUTNAM. But if our goal is a governmentwide smart card program or even a DOD-wide smart card program, is it still cost effective for someone who has no clearance, has no access to particularly sensitive material, and you're just using it as a nifty way to get around people having keys and people being able to get behind the counter at the Social Security Administration as opposed to just getting into the public building.

Is that cost benefit always worth it?

Mr. RHODES. Well, that's the—your point is—and the hierarchy you just went through is the true basis for it. If all you're wanting is for somebody to get access into a building in order to stand on the other side of the counter and talk to some government official you may not necessarily need that. However, for the person to get behind that counter in the environment we are in now, with the understanding of the threat that we have now, it certainly seems that something far beyond just my driver's license, which colleagues from our Special Investigations Office are testifying on today. We have forged credentials for them. At that point, the token at that moment, my driver's license, is pretty worthless.

Mr. PUTNAM. Especially in any good college town.

Mr. RHODES. Yes, especially in any good college town where they know that to be old enough to buy a beer, you need a photograph of the front of your face, not the profile of your face. I mean, these are the points that need to be made.

One other question, though, that needs to be asked is—and the other two panelists have alluded to this—the system behind the token has to be clearly designed and built from a security standpoint so that, for example, I have the correct token, but the system behind it is broken. So now I am authenticated into a system where either the enrollment piece isn't good enough or the system itself and who is maintaining the system behind it aren't good enough.

Mr. PUTNAM. This is not your first Technology Subcommittee hearing. You've heard stovepipes and interoperability and all this kind of stuff for a long, long time, a lot longer than I have. This is a question I posed to the first panel.

How do you juxtapose the goal of access management and identity authentication with the fact that there are so many thousands of different systems, even within agencies or within departments? Until we have interoperability there, will smart cards ever really work on a broad basis?

Mr. RHODES. Not on a broad basis. I mean, I have seven ID cards in my pocket right now, some of which—two of which are used for the exact same building. One is to get into the front door and one is to get onto a certain floor, because there are two different agencies in the building.

So if I'm talking about physical tokens with my picture on it, I think I'm in several hundred access systems around Washington and the United States and other government agencies.

So until you have that interoperability that you're talking about, I won't be able to have the "single sign-on" where I can do what you were asking on the first panel, take my token, plug it in. God forbid that my building has a—there's some accident that occurs in my building and I need to be evacuated. No, I will not be able to take that token and go to a remote location and log in unless the infrastructure is there or unless the stovepipes are broken, because it can't just be a matter of me being able to have complete, unfettered access and authentication to the system in front of me. I need to be able to go to other places.

Mr. PUTNAM. The point you made about the number of ID cards you have, you can go down to the Capital Hyatt or the Hilton or anywhere, and everybody gets a room card—hundreds of different room cards, two per room, 300 rooms in this big, tall hotel. All those cards get you in the front door after hours or the back door or the parking garage, all of them equally, but unequally get you into your discrete room that you have business being in. But GAO can't have the same technology.

Mr. RHODES. The GAO—I will say this. The GAO does have the same technology, but we're only 3,000 people. We're 3,000 people in 10 locations, and we have a Comptroller General who's a power user of technology.

If you want to have an organization, if you want to be able to take the entire Federal Government and say, standardize, well, who's the czar of the Federal Government? Who's going to use both carrot and stick to get that done? That's the modus operandi for the solution.

I mean, I report directly to the Comptroller General of the United States, and he believes that security is important, but con-

venience is also important. And we've struck a balance. So I have one ID for the General Accounting Office.

Mr. PUTNAM. Well, we're going to have a czarina now.

Mr. Bergman and Mr. Turissini, give us the private sector take on what you've heard this morning. Where are we headed? What is your vision for what the Federal Government's approach to smart card technology could be?

Just share that with us, if you would, please, beginning with Mr. Bergman.

Mr. BERGMAN. Do you want the pleasant answer or the truth?

Mr. PUTNAM. Well, you're under oath now. So you're stuck.

Mr. BERGMAN. Good point. I think it takes too long time to get started and deploy the technology.

The technology is there in different places, and we need to move forward. It was talked about that, we use more and more Web-enabled applications, and that's good and fair; but then we talk about the Web application having a smart card or smart ID credential interacting with the PIN code. So then we have two PIN codes talking with each other.

Where is the evidence that it is the person who is authenticated to that particular smart card?

The technology is here, and I think that it's been said a number of times today that we need to get moving and create a de facto standard. The technology is not the blockage, and I don't think that we have to be that complex in creating all the back-end systems, all interacting, because then we need to wait for another number of years.

Private organizations have similar problems. They don't have one back-end system even for a small corporation. They have hundreds maybe, and the technology still works there, as we speak, right now.

I do think that we have to decide, where we want to go, the strategy, the needs, and start to implement it. If we are sitting and trying to create the fantastic, unique system, then we'll never get there. I don't see any difference between the Federal Government versus the corporations in the market out there. Let's have the, "This is the direction we're going," and then let's move on.

Mr. PUTNAM. Mr. Turissini.

Mr. TURISSINI. Just to add to that, not only is the technology here, but the infrastructure has been invested in over the last 5 to 10 years within the DOD, with GSA to do the credentialing and to get people identity credentials, not only within the government but with our civil citizenry.

We have, again, neglected to go forth with this technology for fears, for stovepipes, for rice bowls maybe, but the bottom line is, we can currently credential almost everybody in the government and probably everybody in the country.

The DOD, under the program I'm working, is currently credentialing over 10,000 people a day on smart cards, giving unique credentials; and those credentials, in the form of digital certificates, can be accepted in your data bases, your Web-enabled data bases, tomorrow if you choose to do so. It's not a long process, nor is it a terribly expensive process.

We need to get on with the business of securing our information resources. You need what is the cost benefit.

There are very few pieces of information that anybody in this government deals with that in the aggregate can't be harmful to us outside of the United States, things like flight schedules, things like where people land and when they land and who's coming in and out of this country. We can't guarantee who the bad guys are, but we can guarantee who the good guys are. We can credential all the people we need to, so that if you don't have a credential, you're under suspicion and you've got to go get one or we've got to talk to you a little bit closer.

So the technology is here. We've invested 5 years, 7 years, and a lot of money with GSA and DOD to create the infrastructure to field this technology. I say, let's get on with the business of doing it; and I think the way that we do that is by—they called it "culture" earlier. I think it's just policy and direction. You need to be told, and you need to say, this is the way we're going.

We have policy that is set up in the forms of certificate policies and practice statements. They need to be in force. They need to be promulgated.

As far as the physical versus the virtual, this is my smart card CAC. This is my identification into a DOD building. Other than the color, I don't know what the culture shock is.

So physically don't tell the guys at smart card. I don't know. It's not that big a deal. But I do have a chip on my smart card, and that chip gives me digital capability.

And, again, the smart card is not my access. It's a protection of the credential. That's all it's doing. It's protecting the blob, the ones and zeros that are on there that identify me, the thing that I went to a work station, gave them my three or four forms of ID, gave them my fingerprint and guaranteed that I'm going to protect that credential. I can't give it to anybody else. It's not like a password that I can pass over to him, because it's on here, and I have it, and I'm the only one—and I'm responsible for that.

Mr. PUTNAM. One of the issues that always comes up in any congressional hearing when we're trying to push the Federal Government to do particular things is the considerable difficulty due to the sheer size of the government, and the different requirements based on job classifications and things like that.

To the best of your knowledge, who is the largest commercial user of smart card technology that might be a good firm for this subcommittee to pay a visit to and see how they've made it work?

Mr. TURISSINI. Actually, the banking industry is probably the best, and I don't know if it's a particular firm, maybe Chase Manhattan. But what we've got to be careful about is the definition of "smart card," and there are many definitions, everywhere from a stored value card to a card like the CAC, which is a cryptographic module card, a computer that actually protects a credential.

The biggest user of that kind of credentialing is the DOD. Nobody else is really doing that to the extent that the DOD is doing. Like I said, over 3 million users right now, and we're issuing 10,000 credentials a day. But from a credentialing point of view and a smart card in a less secure environment, although probably just as critical, the financial community is very involved in moving

transactions using digital credentials and protecting those credentials on some kind of a token, whether it's smart card or an IT or something like that.

Mr. PUTNAM. Mr. Bergman, do you want to add anything?

Mr. BERGMAN. No. The CAC program is definitely the biggest one.

I just want to add there are other projects on their way around the world right now, everywhere from Hong Kong to Malaysia, to Saudi, to Latvia, Turkey, a number of countries out there are doing the same thing right now. And those will maybe be bigger or larger deployment when they are deployed, but I don't know any bigger than the CAC program as deployed.

Mr. PUTNAM. A lot of pressure, Mr. Scheflen.

Mr. Rhodes, do you want to add anything to that?

Mr. RHODES. I would echo the distinction between a smart card, which actually has its cryptographic module on it and actually has the computer on the card, versus the stored value. There are larger implementations in industry that are stored value, but there isn't any larger implementation than the CAC of a truly smart—on-the-card, intelligent system.

Mr. PUTNAM. I may not be truly appreciating that distinction. It just seems that you get a little tag to hang on your key ring from your supermarket. They take 10 percent off every time, you use it and you earn points toward a new ball cap. And you get a little card to hang on your key ring that you wave in front of the gas pump, and you're allowed to get $50, $40 of gas at a time and head on, and they ask you if you want a receipt. You don't have to see anybody. You don't have to talk to anybody over those intercoms that never work.

It just seems like the rest of the world is figuring all this out reasonably well. I mean, we're buying gas, not getting access to missile silos. But still, tens, hundreds of millions of dollars' worth of transactions on a fairly frequent basis that ordinary citizens are becoming rather accustomed to and comfortable with, even though Giant knows that they prefer Cheer over Tide or that they buy 12 gallons of milk a month or whatever.

People are dealing with it so that they can get that 10 percent off. I mean, I think we're in this post-September 11 world, everybody is focused on ways to sell the government something based on security, but the idea that instead of there being a paper file that moves around with our 3 million military personnel every 2 years, you've got it on something the size of your VISA card and you swipe it when you go into whatever installation in whatever country on whatever base, and you deal with that; and then you perhaps could take that same card over to the PX and buy your groceries and you could take that same card over and, I mean, have dozens of applications on the same smart card above and beyond simple identity authentication and access.

And maybe I'm not appreciating the distinctions here, but even if you separate the zebra that is DOD from all the horses that are the rest of the government, there's a lot more that we can be doing with this, I think, for an awful lot of Federal Government employees, than we have.

Mr. Bergman, could you elaborate some on the match-on card technology?

Mr. BERGMAN. I would be happy to do that.

The match-on card technology that we're using, the chip on the smart card do the comparison of the template. That means that when I log onto my computer, I have my biometric template stored on that chip. I put it into my biometric and combined smart card reader, which is about a $100 piece of equipment. When I do the matching, the matching is done on the smart card. That means that my template will not be transformed over to a data base somewhere else. From a scalability point of view, that's very important. I don't need to have the infrastructure built up behind it.

For instance, take today's discussion about the U.S. VISIT program. Does it need to be an infrastructure to allow myself with my finger going into a data base somewhere in the world, or is it only when I issue a credential that I need to be connected back to the data base and say am I a good guy or bad guy. After that, once I've got my credential and it's secure enough to go around the world and say this is me, there's one piece missing in it. That's the validation of it. Is it valid? It's OK, it's me, but am I still valid? And there are technologies for that as well.

An example that happened to me last Saturday, returning back from Sweden, we were standing, myself and hundreds of other people, out in Dulles Airport waiting for INS because the back-end system was down. Is that the way we want to build the infrastructure? This was just to swipe my passport and my green card. Is this the way we protect our borders? That is a pretty effective way—"no one can enter." Nothing happened for 40 minutes because the back-end data base was down.

Those are the kinds of things that we need to think about when we deploy a large system. That's why I think you do DOD biometric authentication up front on your token, on a sticky product. A sticky product is something you have and that you use 10 times a day.

And you talk about convenience. It's convenience for me. You can't force people to use security. It's convenience that matters.

I can get into different places. The biometric comparison can be done on a card or a token, or it can be done back on a data base. And I think the data base is a legacy infrastructure and costly, and it's a pretty nonoptimized way of doing business today.

Mr. PUTNAM. To any of you who wish to answer, how far are we from being able to replace the paper passport with a smart-card type of identification, merged with biometrics?

Mr. Bergman.

Mr. BERGMAN. From a technology point of view, we're not far away, but I think along the same line, that we have been talking and listening today about the stovepipes.

If you talk about the passport which is one passport for the United States, another one for European countries, I think we need to discuss where we are heading. I think that biometrics should be on the road map, I think it's a good step forward to have my picture, my face on that smart card or token, in a readable format.

To have a smart card on the passports is probably a number of years, 5 years, 10 years away—if we decide upon the direction. I

don't know, but lots of people in this country don't even have a passport.

Those are the kinds of things that we have to sit down and decide about the strategy, go for it, and step by step we implement it.

Mr. PUTNAM. Mr. Rhodes.

Mr. RHODES. One point I would make is that INS and State—at the time of that report, INS and State had issued 5 million border crossing cards that included fingerprint or fingerprints—probably at about 6.5 million now. But just as you had the discussion this morning about the cards are issued, but are they application-enabled, well, the cards—you have 6.5 million cards out there, but they haven't bought enough readers. So now the cards are being treated just as any other travel document.

So as they're—how far away are we from this is my digital identity on this card and it's recognizable in the United States or it's recognizable inside the Federal Government. It's a matter of the implementation.

I can't stress enough what the other panelists, not just here but on the earlier panels, said. It is not a question of technology; it really isn't. The ID-on-card, match-on-card technology is one of the balancing factors for convenience as well as privacy concerns. It's a matter of deploying them, getting them out, getting people enrolled and making certain that the technology is in place.

Just as you were saying earlier for the earlier panel, when is it good enough?

It's not perfect. As somebody who tests the security of the Federal Government on behalf of the legislative branch, putting something in place better than a user ID and a password is a step in the right direction, even if it's not the greatest thing in the world, if it's not the best technology, because user IDs and passwords are folly. And you give me 7 days, I can break any one of them, and I don't care what it is, because we do it.

So trying to get a token and trying to get some smart card combination with biometric technology is superior to what we have now, and that's really the question that everyone needs to ask, "Is what we're trying to put in place better than what we have now," and the answer is, "Yes."

Mr. PUTNAM. You mentioned face, hand, iris and finger. Are they the key biometric features?

Mr. RHODES. Those are the four that are most mature.

Mr. PUTNAM. Right. So you mentioned that retinal scan is probably what most people would consider the most intrusive.

Mr. RHODES. No doubt.

Mr. PUTNAM. Fingerprint, probably less intrusive.

Mr. RHODES. Yes, sir.

Mr. PUTNAM. The least intrusive.

What is the most appropriate biometric characteristic to adopt for widespread usage for things like air travel, access to unclassified-type facilities and things of that sort that would be widely used perhaps on a passport?

Mr. RHODES. At least in the technology we've looked at, since fingerprint recognition is the most mature, that's probably the most

appropriate. You'd want to have a fingerprint photograph on a card.

Talking about a single token, you're actually talking about multiple identifiers on the token. There's the design of the token, the color of the token. There's a shield on it. There's probably a magnetic strip on the back as well as an on-board chip, and there would be some template inside there for a fingerprint.

Now the question becomes, "Do you want just a thumb, just an index finger? Do you want 10 fingers?" But the fingerprint recognition is the longest lived. I mean, that's the most mature technology at the moment, although retinal scan is very mature, but you have to sit for a long time, and you have to have this thing paint the back of your eye. And people usually don't want to take an afternoon and enjoy that. The more invasive it is, the more concerns there are.

Facial recognition is probably the least invasive, but it's extremely unstable, because you can do it with a CCTV. You can do it with closed circuit television at a stadium or something like that; but depending on how the lighting is, how the face is turned, the expression on the face, the identification points shift, and then they don't necessarily connect properly. There's a high false-positive rate. And there's a high false-negative rate, as well, with facial recognition, facial pattern.

Mr. PUTNAM. Mr. Turissini, talk a little bit about the privacy issues, please. You've raised that in your testimony, and understandably there are widespread concerns in the populace about privacy issues.

How do we strike the proper balance?

Mr. TURISSINI. Well, as I state in the paper, what you need to look at are multiple technologies, not just a single technology. Using smart cards with the biometric, with the asymmetric credential, allows the personal data, that fingerprint or the scan of the face or retina, to be owned and carried only by the owner of the fingerprint or the credential.

What I would be afraid of in a public venue would be to have my fingerprint or even a representation of my fingerprint to be in a data base to be compared to; and then that would be distributed. Because it's not going to be on one data base; it's going to go to the next data base. It's kind of like when you send an e-mail to eBay and you get 100 junk mails. Well, you use your fingerprint on one place, and then your fingerprint is all over the world.

But the big distinction—and I want to bring this back to the earlier question, the distinction between the cryptographic smart card, the cryptographic function versus just the stored value; and that's the same issue, there is this nonrepudiation. When you go to a gas station, even when you use your credit card, they're not checking to see if Mr. Putnam is swiping that card. They're checking to see that Mr. Putnam has money in that checking account or that credit card account or something like that. They really don't care who you are. They just care that you have money to pay the bill.

In the transactions we're dealing with in the government and the protections we're involved with, we not only want to know who's touching this data. We want to know what they're doing, and we want them to leave a trace of nonrepudiation. We don't want peo-

ple coming into our enclaves and doing something and then later being able to say, I didn't do it.

These viruses are a good example. We have the technology today to use digital credentialing, whether in the form of digital certificates or in combination with the smart cards and the biometrics, so that every e-mail I receive into my enclave is identified with the person sending it.

Now, if I have to go out and get a credential, show three forms of ID and sign that I'm going to protect that credential and I'm going to put it on a smart card, and then when I send you an e-mail, I have to apply that credential to it so that you know it came from me, I'm not going to send you a virus, certainly not on purpose. I'm not going to create a worm and send it to you with my signature on it.

So the distinction in just stored value versus this cryptographic or this strong smart card is really the assurance that the person doing the transaction is that person by name, rank, Social Security or serial number and not just a bank account or not just somebody from Federal Building No. 12 or something like that. It really brings every transaction to a personal level, not only from a signature, not only from an authentication, but also from an auditing point of view. And that's why it doesn't matter the level of security from the back-end point of view.

The only thing the credential cares about is your identity. Now, what you do with that identity in your back end is your choice.

Now, if you are—and we'll put numbers on it. If you're 99.9 percent sure that this credential is going to be correct because it comes from a trusted third party, and it's protected by a biometric or a smart card environment and you're going to do a financial transaction, maybe that's all you want is authentication by that credential. And if you're going to blow missiles up, maybe you want that person and somebody else's credential statement. So there's the back end.

How you react to that identity is kind of a separate question. It's not a completely different issue, but it is a separate question.

We have not only the technology but the infrastructure to credential, to make that credential available so that you can decide what to do with that credential; so that the FAA and TSA can say, you know, I've got this card and it's Dan Turissini, and Dan Turissini is allowed access in and out of the airports, and he's a good guy and he doesn't have a criminal record. And the guy that shows up with no ID and no credential, well, we've got to take a closer look at that. They're the people that should be taking off their shoes and checking their—the heels of their shoes and stuff like that.

So that's the distinction. It's the nonreputable authentication of that person and the auditing capability of those transactions, rather than to a bank account or to a location; it's directly to the person's identity.

Mr. PUTNAM. Any other comments from the other panelists?

Mr. BERGMAN. From a privacy point of view?

Mr. PUTNAM. Yes.

Mr. BERGMAN. I fully agree with my panelists here.

When you demo on a trade show, you demo biometrics. The worst you could joke about is saying, "What's happening right now is tak-

ing your fingerprint and sending it back to a data base." The people get really scared.

The biggest educational problem we have is, Mrs. So-and-So, we are not taking your fingerprint. You're using your fingerprint to create the digital representation. It's called a biometric template. And it's not stored in the data base. And it's not a unique concern. Thousands of people have discussed that kind of thing, I don't want to have my fingerprint in the data base.

And also, by the way, Minority Report and other interesting movies the last years haven't helped because, it's the fingerprint, I put the fingerprint somewhere else, and you're nailed.

So I think that the privacy, as you said here before, is that the template is one step; and the second step is, I have it right here. I control my template. I control my own data base, so to speak. That's why I'm concerned about the overall infrastructure that's being proposed for the U.S. VISIT and TWIC program right now. That's counterproductive to the biometric industries from an image template and the storage.

The privacy is a big concern. And you, Mr. Chairman, said before about passport, it's going to be even bigger, because we don't deal with only DOD people.

Mr. PUTNAM. Elaborate some on the TWIC concern.

Mr. BERGMAN. My understanding is that TWIC is proposing to have the image going back to a data base and to have 450 point of entries fully equipped with biometric devices that could capture fingerprints, send that fingerprint back to a data base and check if you are a good guy. Otherwise, we don't let you over the bridge, so to speak.

That's the big concern, to have the image back and forth to a data base, because as Mr. Turissini said before, it's not one data base. It's replicated in different data bases.

I've been working 5 years for a data base company, so I know that. Replication of data base is a special thing. It's easier to say, not so easily done.

Mr. PUTNAM. That's something we can look into.

Mr. Rhodes, do you have any final comments?

Mr. RHODES. The one point that I would make regarding either data base or sending information back is that is at the heart of the privacy concern. The question is how—the question from a citizen's point of view is, what are you going to do with this information, because we've now moved away from, you've stolen my identity because you've got my Social Security number.

Now you move into that realm of absolute nonrepudiation, because this is the double whorl on my thumb, and this is the single whorl on my left index finger, and two of them brought together give great authentication of who I am and leave me no margin for saying, "I wasn't there or I'm not this individual."

The more that information gets passed and the more that it becomes replicated, it becomes difficult to synchronize data bases, and it becomes difficult to make certain that they're all up to date. So the more that it is tied into on-card validation as opposed to a larger system where the information is being passed, the more it's going to be convenient; and ultimately, that's one of the factors that needs to be brought in.

We all know what it was like to try to move through Washington, DC, right after September 11th. We couldn't get into buildings. Even if you worked there, it was difficult to get into a building, and you had the right credentials.

Trying to get on an airplane during a high-threat period is very difficult. Trying to get on an airplane under any conditions is difficult these days, but during high threat it's very difficult.

So as more of this technology is applied, if it's convenient, if it makes it easier for people to move through portals and to get to the services that they need—your point about having my medical records on a smart card that's biometrically validated back to me, etc., all the conveniences, that's great, because the card can speak for me when I can't. But I have to make certain that the information on that card isn't then able to be used by someone else or that the information on that card isn't going to be corrupted or unusable because the system I plug into is getting creamed by Blaster at that moment. So these are all those balances that have to be worked out on the tradeoffs.

Mr. PUTNAM. Very good.

I want to thank this panel for their contributions and thank the first panel, as well, particularly those who stayed—Mr. Willemssen, Mr. Scheflen—and I appreciate your remaining and hearing the issues raised by the private sector and Mr. Rhodes.

We obviously have a lot of work to do on this issue, and this subcommittee will continue to follow the progress of the executive branch's move toward implementing this.

So, with that, we appreciate all the contributions, and just to make sure I'm not forgetting something. If there may be additional questions we did not have time for today, the record will remain open for 2 weeks for submitted questions an answers. With that, we stand adjourned.

[Whereupon, at 12:35 p.m., the subcommittee was adjourned.]