

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.

Technology Administration
BENJAMIN H. WU
DEPUTY UNDER SECRETARY OF
COMMERCE FOR TECHNOLOGY



Ben Wu was sworn in as Deputy Under Secretary for Technology at the U.S. Department of Commerce on November 6, 2001. In this capacity, he supervises policy development, direction, and management at the Technology Administration (TA), a bureau of over 4,000 employees that includes the Office of Technology Policy (OTP), the National Institute of Standards and Technology (NIST), and the National Technical Information Service (NTIS).

TA serves as the principal resource to support Commerce Secretary Don Evans in developing policies to maximize science and technology's contribution to America's economic growth. Some of Ben's priorities have included supporting entrepreneurship and innovation, strengthening U.S. technology cooperation with other countries, enhancing research and development in our nation's federal laboratory systems, and creating greater collaboration between government, industry, and universities. Ben also participates in activities with the National Science and Technology Council (NSTC), a Cabinet-level council established by the President to coordinate science, space, and technology policy within the Federal research and development enterprise, and is the Executive Secretary for the NSTC Committee on Technology.

Prior to joining Commerce, Ben held senior staff positions in the U.S. Congress where he led on issues affecting United States technology and competitiveness policy. He worked in Congress from 1988, having served as Counsel to Congresswoman Constance A. Morella of Maryland and on the Science Committee, first serving on the Investigations and Oversight Subcommittee staff in 1993 and then on the Technology Subcommittee from 1995 until his current appointment.

Ben has extensive experience focusing on information technology, biomedical technology, and technology transfer policy. He was the primary congressional staff on legislation affecting federal intellectual property and federal technology transfer. Additionally, Ben has worked on Technology Administration issues since TA's inception in 1989, with particular emphasis on NIST. Ben was also the most senior member and the lead Committee staff of the House Y2K Task Force that directed congressional efforts to correct the Year 2000 computer problem.

Ben received a Bachelor of Arts from New York University in 1985 and a Juris Doctor from the University of Pittsburgh in 1988.