September 2003

ELECTRONIC GOVERNMENT

Challenges to the Adoption of Smart Card Technology

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.

What GAO Found

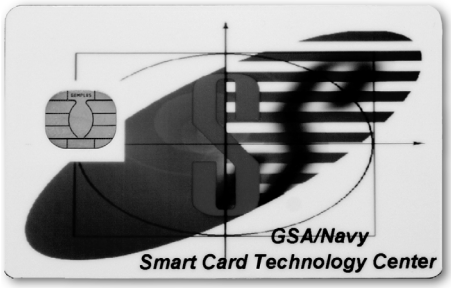
To successfully implement smart card systems, agency managers have faced a number of substantial challenges:

- 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