January 2003

GAO Highlights

Highlights of GAO-03-144, a report to the Chairman, Subcommittee on Technology and Procurement Policy, House of Representatives

ELECTRONIC GOVERNMENT

Progress in Promoting Adoption of Smart Card Technology

Why GAO Did This Study

Smart cards—credit-card-like devices that use integrated circuit chips to store and process data—offer a range of potential uses for the federal government, particularly in increasing security for its many physical and information assets. GAO was asked to review the use of smart cards across the federal government (including identifying potential challenges), as well as the effectiveness of the General Services Administration (GSA) in promoting government adoption of smart card technologies.

What GAO Recommends

GAO recommends, among other things, that GSA establish guidelines for federal building security that address smart card technology; that OMB establish policy on adoption of smart cards for physical and logical security; and that NIST continue to improve and update the government smart card interoperability specification.

In commenting on a draft of this report, agency officials generally agreed with its content and recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-03-144.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

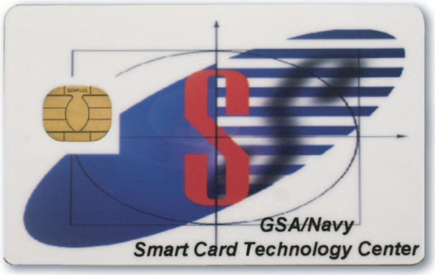
Progress has been made in implementing smart card technology across government. As of November 2002, 18 federal agencies had reported initiating a total of 62 smart card projects. These projects have provided a range of benefits and services, ranging from verifying the identity of people accessing buildings and computer systems to tracking immunization records.

To successfully implement such 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;
- maintaining the security of smart card systems and privacy of personal information.

In helping agencies to overcome these challenges, not only GSA but also the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have roles to play. As the federal government's designated promoter of smart card technology, GSA assists agencies in assessing the potential of smart cards and in implementation. Although GSA has helped agencies significantly by implementing a governmentwide, standards-based contracting vehicle, it has not kept guidance up to date and has not addressed important subjects, such as building security standards, in its guidance. Further, OMB, which is responsible for setting policies for ensuring the security of federal information and systems, has not issued governmentwide policy on adoption of smart cards. In its role of setting technical standards, NIST is responsible for the government smart card interoperability specification, which does not yet address significant emerging technologies. Updated guidance, policy, and standards would help agencies to take advantage of the potential of smart cards to enhance security and other agency operations.

A typical smart card (not to scale)



Source: GSA.

United States General Accounting Office