GAO
Accountability•Integrity•Reliability

# Highlights

Highlights of GAO-04-157, a report to the House Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

## Why GAO Did This Study

The federal government is increasingly using online applications to provide access to information and services and to conduct internal business operations. In light of this trend, strong security assurances are needed to properly safeguard sensitive, personal, and financial data, in part by ensuring that the identities of those who use such applications are appropriately authenticated. When fully and properly implemented, public key infrastructure (PKI) offers many of these assurances. In 2001, GAO reported that the federal government faces a number of challenges in deploying PKI technology (GAO-01-277). GAO was requested to follow up this work by (1) determining the status of federal PKI activities, including initiatives planned or under way at 24 major federal departments and agencies, as well as the status and planned activities of the Federal Bridge Certification Authority (FBCA) and Access Certificates for Electronic Services (ACES) programs, and (2) identifying challenges encountered by the 24 agencies in implementing PKI initiatives since the 2001 report was issued.

In commenting on a draft of this report, GSA and OMB officials generally agreed with its content and conclusions. Technical comments provided by OMB have been addressed as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-04-157.

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

December 2003

# INFORMATION SECURITY

# Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies

## What GAO Found

PKI and its associated hardware, software, policies, and people can provide greater security assurances than simpler means of authenticating identity, such as passwords. In pursuit of these benefits, 20 of the 24 agencies reported that they are undertaking a total of 89 PKI initiatives. The 89 initiatives are at various stages of development, and collectively they represent a significant investment, estimated at about $1 billion. In addition, the governmentwide FBCA and ACES programs continue to promote the adoption and implementation of PKI, but these programs have seen mixed progress and results. The level of participation in the FBCA, which provides a means to link independent agency PKIs into a broader network, is the same as in 2001—four agencies have been certified as meeting technical and security requirements to interconnect through the network. Additional organizations are planning to participate in the future, including four federal agencies and some nonfederal organizations, such as the state of Illinois, the Canadian government, and educational consortiums. Similarly, the ACES program, which offers agencies various PKI services through a General Services Administration (GSA) contract, has seen lower than expected participation by federal agencies. GSA plans to revise the pricing structure associated with the ACES program to encourage participation.

PKI implementation continues to pose major challenges for agencies, which are shown in the table. Many of these challenges are similar to those identified in GAO's 2001 report. In that report, GAO recommended that the Office of Management and Budget (OMB), working with other key federal entities, take action to address these challenges, including establishing a governmentwide framework of policy and technical guidance and a program plan for the federal PKI. GAO also recommended that OMB take steps to ensure that agencies adhere to federal PKI guidance. OMB has not yet fully addressed the recommendations related to the construction of a PKI policy framework, but it issued a policy memorandum in July 2003 that lays out steps for consolidating investments related to authentication and identity management processes across government.

**Challenges to Implementation of PKI**

| Challenge | Description |
|---|---|
| Policy and guidance | These are lacking or ill-defined in a number of areas, including both technical standards and legal issues. |
| Funding | Besides the high costs associated with the technology, cost models are lacking that would aid budgeting, and cost is increased when systems must be designed to accommodate the uncertainty associated with undefined standards. |
| Interoperability | Integrating PKI systems with other systems (such as network, security, and operating systems) often requires significant changes or even replacement of existing systems. |
| Training and administration | Training is required for personnel to use and manage PKI, and basic PKI requirements and processes impose significant administrative burdens. |

Source: GAO.